

Д.К. ФАДДЕЕВ

# ЛЕКЦИИ ПО АЛГЕБРЕ

*Допущено Министерством высшего  
и среднего специального образования СССР  
в качестве учебного пособия  
для студентов университетов  
и педагогических институтов*



МОСКВА «НАУКА»  
ГЛАВНАЯ РЕДАКЦИЯ  
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ  
1984

22.14  
Ф 15  
УДК 512.8

Фаддеев Д. К. Лекции по алгебре: Учебное пособие для вузов.— М.: Наука. Главная редакция физико-математической литературы, 1984.— 416 с.

Книга представляет собой изложение курса лекций по алгебре, читавшегося автором в Ленинградском университете на протяжении ряда лет. Этот курс рассчитан на 3 семестра. Большим достоинством книги является то, что абстрактные понятия вводятся в ней как результаты обобщения конкретного математического материала.

Для студентов университетов и пединститутков.

Рецензенты:  
кафедра высшей алгебры Московского государственного университета;  
доктор физико-математических наук Л. Я. Куликов

*Дмитрий Константинович Фаддеев*

## ЛЕКЦИИ ПО АЛГЕБРЕ

---

Редактор Ф. И. Кизнер

Техн. редакторы Е. В. Морозова, С. Я. Шкляр

Корректоры Т. Г. Егорова, Е. В. Сидоркина

ИБ № 12076

Сдано в набор 12.01.84. Подписано к печати 10.11.84. Формат 60×90<sup>1</sup>/<sub>16</sub>. Бумага книжно-журнальная. Усл. печ. л. 26. Усл. кр.-отт. 26,25. Уч.-изд. л. 28,35. Тираж 26 000 экз. Заказ № 26. Цена 1 р. 10 к.

Издательство «Наука»

Главная редакция физико-математической литературы  
117071 Москва В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли.  
198052, г. Ленинград, Л-52, Измайловский проспект, 29.

© Издательство «Наука».  
Главная редакция  
физико-математической литературы,  
1984

Ф  $\frac{1702030000-183}{053(02)-84}$  59—84

# ОГЛАВЛЕНИЕ

Предисловие . . . . .	6
-----------------------	---

## Глава I

### ЦЕЛЫЕ ЧИСЛА

§ 1. Теория делимости целых чисел . . . . .	7
§ 2. Теория сравнений . . . . .	15
§ 3. Некоторые общие понятия алгебры . . . . .	21

## Глава II

### КОМПЛЕКСНЫЕ ЧИСЛА

§ 1. Обоснование комплексных чисел . . . . .	26
§ 2. Тригонометрическая форма комплексного числа . . . . .	31
§ 3. Извлечение корня из комплексного числа . . . . .	39
§ 4. Корни из единицы . . . . .	43
§ 5. Показательная и логарифмическая функции комплексной переменной . . . . .	49

## Глава III

### ПРОСТЕЙШИЕ СВЕДЕНИЯ ОБ АЛГЕБРЕ ПОЛИНОМОВ

§ 1. Полиномы от одной буквы . . . . .	53
§ 2. Алгебраическое решение уравнений третьей и четвертой степени . . . . .	61
§ 3. Полиномы от нескольких букв . . . . .	69

## Глава IV

### МАТРИЦЫ И ОПРЕДЕЛИТЕЛИ

§ 1. Матрицы и действия над ними . . . . .	72
§ 2. Теория определителей . . . . .	82
§ 3. Линейная зависимость и линейная независимость строк (столбцов) . . . . .	108
§ 4. Системы линейных уравнений общего вида . . . . .	117
§ 5. Дальнейшие свойства определителей . . . . .	121
§ 6. Обращение квадратных матриц . . . . .	134
§ 7. Характеристический полином матрицы . . . . .	141

## Глава V

### КВАДРАТИЧНЫЕ ФОРМЫ

§ 1. Преобразование квадратичной формы к каноническому виду линейной подстановкой букв . . . . .	143
§ 2. Закон инерции квадратичных форм . . . . .	152
§ 3. Ортогональное преобразование квадратичной формы к каноническому виду . . . . .	156
§ 4. Эрмитовы формы . . . . .	164

## Глава VI

**ПОЛИНОМЫ И ДРОБИ**

§ 1. Теория делимости для полиномов от одной буквы . . . . .	167
§ 2. Производная . . . . .	175
§ 3. Рациональные дроби . . . . .	180
§ 4. Интерполяция . . . . .	191

## Глава VII

**СРАВНЕНИЯ В КОЛЬЦЕ ПОЛИНОМОВ И РАСШИРЕНИЯ ПОЛЕЙ**

§ 1. Сравнения в кольце полиномов над полем . . . . .	197
§ 2. Расширение полей . . . . .	198

## Глава VIII

**ПОЛИНОМЫ С ЦЕЛЫМИ КОЭФФИЦИЕНТАМИ. ПОЛИНОМЫ НАД ФАКТОРИАЛЬНЫМИ КОЛЬЦАМИ**

§ 1. Полиномы с целыми коэффициентами . . . . .	203
§ 2. Полиномы от одной буквы над факториальным кольцом . . . . .	208

## Глава IX

**РАСПРЕДЕЛЕНИЕ КОРНЕЙ ПОЛИНОМА**

§ 1. Существование корней в $\mathbb{C}$ . . . . .	214
§ 2. Распределение корней на плоскости комплексной переменной . . . . .	218
§ 3. Распределение вещественных корней полинома с вещественными коэффициентами . . . . .	223
§ 4. Обобщенная теорема Штурма . . . . .	229
§ 5. Приближенное вычисление корней полинома . . . . .	234

## Глава X

**ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП**

§ 1. Простейшие сведения . . . . .	242
§ 2. Нормальные подгруппы и факторгруппы . . . . .	247
§ 3. Гомоморфизм . . . . .	249
§ 4. Прямое произведение групп . . . . .	257
§ 5. Группы преобразований . . . . .	259
§ 6. Свободная группа . . . . .	269
§ 7. Свободные произведения групп . . . . .	273
§ 8. Конечные абелевы группы . . . . .	275
§ 9. Конечно порожденные абелевы группы . . . . .	278

## Глава XI

**СИММЕТРИЧЕСКИЕ ПОЛИНОМЫ**

§ 1. Выражение симметрических полиномов через основные . . . . .	284
§ 2. Значения симметрических полиномов от корней полинома . . . . .	288
§ 3. Результант . . . . .	294

## Глава XII

**ВЕКТОРНЫЕ ПРОСТРАНСТВА**

§ 1. Определения и простейшие свойства . . . . .	301
§ 2. Подпространства . . . . .	307
§ 3. Линейные функции . . . . .	312
§ 4. Линейные отображения векторных пространств . . . . .	314

§ 5. Линейные операторы в векторном пространстве . . . . .	317
§ 6. Операторы в векторных пространствах над полем $\mathbb{C}$ комплексных чисел . . . . .	333
§ 7. Операторы в векторных пространствах над полем $\mathbb{R}$ вещественных чисел . . . . .	341

## Глава XIII

## ЕВКЛИДОВО И УНИТАРНОЕ ПРОСТРАНСТВА

§ 1. Определения и простейшие свойства . . . . .	345
§ 2. Подпространства унитарного (или евклидова) пространства . . . . .	352
§ 3. Пространства, сопряженные с евклидовым и унитарным пространствами . . . . .	354
§ 4. Операторы в унитарном пространстве . . . . .	355
§ 5. Операторы в евклидовом пространстве . . . . .	362
§ 6. Преобразование уравнения гиперповерхности второго порядка к каноническому виду . . . . .	366
§ 7. Линейные отображения унитарного пространства в унитарное . . . . .	371
§ 8. Объем параллелепипеда в евклидовом пространстве . . . . .	374

## Глава XIV

## ЭЛЕМЕНТЫ АЛГЕБРЫ ТЕНЗОРОВ

§ 1. Основные понятия . . . . .	377
§ 2. Действия над тензорами . . . . .	380
§ 3. Симметричные и антисимметричные тензоры . . . . .	382
§ 4. Тензорные произведения векторных пространств . . . . .	383

## Глава XV

## АЛГЕБРЫ

§ 1. Общие сведения . . . . .	388
§ 2. Алгебра кватернионов . . . . .	394
§ 3. Внешняя алгебра . . . . .	401

Список литературы . . . . .	416
-----------------------------	-----

## ПРЕДИСЛОВИЕ

Настоящая книга представляет собой обработку лекций по алгебре, читавшихся мной на математико-механическом факультете Ленинградского государственного университета на протяжении нескольких десятилетий для математиков всех специальностей.

От года к году содержание лекций несколько менялось. Здесь собрано теоретико-множественное объединение материала, читавшегося в разные годы.

В основу книги положены лекции, которые я читал в последний раз в 1977—1978 гг. Лекции были старательно записаны Л. Ю. Колотилиной, за что я приношу ей глубокую благодарность.

В ЛГУ линейная алгебра не отделена от общего курса алгебры и читается на третьем семестре. В соответствии с этим последние главы, начиная с главы XII, посвящены линейной алгебре. Элементарно-калькулятивная часть линейной алгебры, состоящая из теории матриц, определителей и квадратичных форм, занимает главы IV и V; этот материал излагается в ЛГУ на первом семестре.

Язык книги несколько архаичен из-за того, что я не тороплюсь вводить абстрактные понятия во избежание формализма при их восприятии. Я считаю, что их следует вводить по мере того, как удастся возбудить в учащихся потребность в обобщении или, по крайней мере, если имеется возможность достаточно иллюстрировать общие понятия более конкретным материалом.

Оформление рукописи было бы для меня невозможным, если бы не энергичная помощь моих товарищей по работе в ЛОМИ. Всем им моя глубокая благодарность!

*Д. К. Фаддеев*

## ЦЕЛЫЕ ЧИСЛА

Изучение свойств целых чисел составляет содержание раздела математики, имеющего название «арифметика» или «теория чисел». Обычно первый термин относится к кругу самых элементарных вопросов, в основном, к правилам вычислений с целыми числами, а второй — к установлению более глубоких и нетривиальных свойств целых чисел. Цель этого раздела курса — познакомить читателя с самыми простыми идеями и фактами теории чисел.

### § 1. Теория делимости целых чисел

**1. Определение делимости и простейшие свойства этого отношения.** Множество всех целых чисел принято обозначать  $\mathbb{Z}$ . Множество  $\mathbb{Z}$  состоит из натуральных, т. е. целых положительных чисел 1, 2, 3, ..., числа 0 и целых отрицательных чисел  $-1, -2, -3, \dots$ . Ясно, что сумма, разность и произведение двух целых чисел суть снова целые числа. Частное же от деления двух целых чисел может и не быть целым числом. Говорят, что целое число  $a$  *делится* на целое число  $b$ , если существует такое целое число  $c$ , что  $a = bc$ . Другими словами,  $a$  делится на  $b$ , если их частное  $c$  снова есть целое число. То же отношение делимости  $a$  на  $b$  может быть выражено другими равнозначными терминами:  $b$  *делит*  $a$ ;  $b$  — *делитель*  $a$ ;  $a$  есть *кратное* для  $b$ . Из определения делимости ясно, что число 0 делится на любое целое число, в том числе и на 0, но ни одно целое число, отличное от нуля, на нуль не делится. Ясно также, что любое целое число  $a$  делится на  $a, -a, 1$  и  $-1$ . Эти числа называются *несобственными*, или *тривиальными*, делителями числа  $a$ . Остальные же делители, если они есть, называются *собственными*, или *нетривиальными*.

Запишем теперь в виде предложений (слово «предложение» значит то же, что слово «теорема», — это высказывание, которое должно быть доказано; мы будем пользоваться словом «теорема» только тогда, когда нужно подчеркнуть важность содержания) некоторые простейшие свойства делимости.

**Предложение 1.** Если два целых числа  $a$  и  $b$  делятся на целое число  $c$ , то их сумма и разность тоже делятся на  $c$ .

**Доказательство.** Имеем  $a = cg, b = ch$ , где  $g$  и  $h$  — целые числа, ибо  $a$  и  $b$  делятся на  $c$ . Тогда  $a \pm b = cg \pm ch = c(g \pm h)$ . Числа  $g \pm h$  целые. Следовательно, числа  $a \pm b$  делятся на  $c$ .

**Предложение 2.** Если целое число  $a$  делится на целое число  $b$  и  $k$  — целое число, то  $ak$  делится на  $b$ .

**Доказательство.** Имеем  $a = bt$  при целом  $t$ , ибо  $a$  делится на  $b$ . Тогда  $ak = btk$ . Число  $tk$  целое. Следовательно,  $ak$  делится на  $b$ , что и требовалось доказать.

Это предложение можно сформулировать и так: если  $c$  делится на  $a$  и  $a$  делится на  $b$ , то  $c$  делится на  $b$ . Действительно, « $c$  делится на  $a$ » значит то же самое, что  $c = ak$  при целом  $k$ .

**2. Деление с остатком.** Всем хорошо известно, что если деление целых чисел не выполняется «нацело», то возможно деление «с остатком». Придадим этому высказыванию точный смысл в виде следующей теоремы.

**Теорема 3.** Пусть  $a, b \in \mathbb{Z}$  (т. е.  $a$  и  $b$  являются целыми числами) и  $b \neq 0$ . Существуют целые числа  $q$  (неполное частное) и  $r$  (остаток) такие, что  $a = bq + r$  и  $0 \leq r \leq |b| - 1$ . Эти требования однозначно определяют  $q$  и  $r$ .

**Доказательство.** Положим сначала, что  $b > 0$ . Рассмотрим рациональное (не обязательно целое) число  $\alpha = \frac{a}{b}$ . Если оно целое, то положим  $q = \alpha$ . Если же  $\alpha$  не целое, то найдутся два соседних целых числа, в промежуток между которыми попадает  $\alpha$ . Меньшее из них обозначим через  $q$ . Тогда  $q < \alpha < q + 1$ . Итак, в обоих случаях мы нашли целое число  $q$  такое, что  $q \leq \frac{a}{b} < q + 1$ . Умножим все три части этого двойного неравенства на  $b$ . Так как  $b > 0$ , знаки неравенства должны сохранить:

$$bq \leq a < bq + b,$$

откуда  $0 \leq a - bq < b$ . Положим  $a - bq = r$ . Это целое число, и, так как  $r < b$ , а числа  $r$  и  $b$  оба целые, должно выполняться более сильное неравенство  $r \leq b - 1$ . Итак,  $a = bq + r$  и  $0 \leq r \leq b - 1$ .

Пусть теперь  $b < 0$ . Тогда  $b = -|b|$ . Применив предыдущее построение к числам  $a$  и  $|b|$ , найдем целые числа  $q'$  и  $r$  такие, что  $a = q'|b| + r$ ,  $0 \leq r \leq |b| - 1$ . Полагая  $q' = -q$ , получим  $a = q(-|b|) + r = qb + r$ ,  $0 \leq r \leq |b| - 1$ . Тем самым существование  $q$  и  $r$  доказано как для положительных, так и для отрицательных  $b$ .

Остается доказать единственность чисел  $q$  и  $r$ . Пусть  $a = bq_1 + r_1$ ,  $0 \leq r_1 \leq |b| - 1$ , и  $a = bq_2 + r_2$ ,  $0 \leq r_2 \leq |b| - 1$ , причем, разумеется, числа  $a, b, q_1, q_2, r_1, r_2$  — все целые. Тогда  $bq_1 + r_1 = bq_2 + r_2$ ,  $b(q_1 - q_2) = r_2 - r_1$ . Положим, что  $q_1 \neq q_2$ . Тогда  $|r_2 - r_1| = |b| \cdot |q_1 - q_2| \geq |b|$ , ибо  $|q_1 - q_2| \geq 1$ . С другой стороны, самое большее возможное значение для  $r_2 - r_1$  есть  $|b| - 1 - 0 = |b| - 1$ , самое меньшее:  $0 - (|b| - 1) = -(|b| - 1)$ . Таким образом,  $-(|b| - 1) \leq r_2 - r_1 \leq |b| - 1$ , откуда  $|r_2 - r_1| \leq |b| - 1$ , что противоречит установленному ранее  $|r_2 - r_1| \geq |b|$ . Мы пришли к противоречию, доказывающему неверность сделан-

ного предположения  $q_1 \neq q_2$ . Следовательно,  $q_1 = q_2$ , а тогда и  $r_1 = r_2$ . Теорема доказана.

**З а м е ч а н и е.** По ходу доказательства мы использовали то обстоятельство, что для любого вещественного  $\alpha$  (у нас  $\alpha$  было рациональным) найдется целое  $q$  такое, что  $q \leq \alpha < q + 1$ . Такое число  $q$  называется *целой частью*  $\alpha$  и обозначается  $[\alpha]$ . Например,  $[5] = 5$ ,  $[\pi] = 3$ ,  $[-2, 7] = -3$ .

**3. Наибольший общий делитель.** Пусть  $a$  и  $b$  — два целых числа, из которых по крайней мере одно отлично от нуля. *Наибольшим общим делителем* чисел  $a$  и  $b$  называется наибольшее натуральное число  $d$ , являющееся делителем как для  $a$ , так и для  $b$ .

Например, наибольший общий делитель чисел  $-6$  и  $10$  равен  $2$ , наибольший общий делитель чисел  $-6$  и  $0$  есть  $6$ , наибольший общий делитель чисел  $-6$  и  $5$  равен  $1$ .

Наибольший общий делитель чисел  $a$  и  $b$  обозначается н. о. д.  $(a, b)$  или просто  $(a, b)$ ; последнее обозначение применяется только в случае, если в том же контексте символ  $(a, b)$  не используется в каком-либо другом смысле (например, координаты точки на плоскости или скалярное произведение векторов  $a$  и  $b$  и т. д.).

Важное свойство наибольшего общего делителя сформулировано в следующей теореме.

**Теорема 4.** Пусть  $a, b$  — целые числа, одно из которых отлично от  $0$ , и пусть  $d$  — их наибольший общий делитель. Тогда

(1) существуют целые числа  $u_0, v_0$  такие, что  $d = au_0 + bv_0$ ;

(2) если  $d'$  — какой-либо общий делитель чисел  $a$  и  $b$ , то  $d$  делится на  $d'$ .

**Доказательство.** Рассмотрим бесконечное множество  $M$  целых чисел, состоящее из чисел  $au + bv$ , где  $u$  и  $v$  независимо друг от друга пробегает все целые числа:  $M = \{au + bv \mid u, v \in \mathbb{Z}\}$ .

Множество  $M$  содержит число  $a$ , оно получается при  $u = 1, v = 0$ ;  $M$  содержит  $b$  (при  $u = 0, v = 1$ );  $M$  содержит  $0$  (при  $u = 0, v = 0$ ) и бесконечно много других целых чисел.

Установим, что если два числа  $x$  и  $y$  принадлежат  $M$  и  $y \neq 0$ , то остаток при делении  $x$  на  $y$  тоже принадлежит  $M$ . Действительно,  $x \in M$  и  $y \in M$  значит, что  $x = au_1 + bv_1, y = au_2 + bv_2$  при некоторых целых  $u_1, v_1, u_2, v_2$ . Пусть  $x = yq + r, q, r \in \mathbb{Z}$  и  $0 \leq r < |y| - 1$ , так что  $r$  есть остаток при делении  $x$  на  $y$ . Тогда  $r = x - yq = au_1 + bv_1 - q(au_2 + bv_2) = a(u_1 - qu_2) + b(v_1 - qv_2)$ . Числа  $u_1 - qu_2$  и  $v_1 - qv_2$  целые, следовательно,  $r \in M$ .

Выберем теперь в множестве  $M$  наименьшее положительное число  $d$ . Покажем, что  $a$  и  $b$  делятся на  $d$ . Пусть  $r_1$  — остаток при делении  $a$  на  $d$ . Так как  $a$  и  $d$  принадлежат  $M$ , то, в силу только что сказанного,  $r_1$  принадлежит  $M$ . Но  $0 \leq r_1 < d$ , а  $d$  — наименьшее положительное число, содержащееся в  $M$ . Следова-

тельно,  $r_1$  не может быть положительным числом, так что  $r_1 = 0$ . Это значит, что  $a$  делится на  $d$ . Те же соображения приводят к выводу, что  $b$  делится на  $d$ . Таким образом,  $d$  есть общий делитель  $a$  и  $b$ . Далее, так как  $d \in M$ , существуют целые  $u_0$  и  $v_0$  такие, что  $d = au_0 + bv_0$ . Пусть теперь  $d'$  — какой-либо общий делитель для  $a$  и  $b$ . Из равенства  $d = au_0 + bv_0$  заключаем, что  $d$  делится на  $d'$ , ибо оба слагаемых правой части равенства делятся на  $d'$ . Поэтому  $d \geq d'$ , так что  $d$  есть наибольший общий делитель. По ходу рассуждения оказались доказанными оба утверждения теоремы.

**4. Алгоритм Евклида.** Метод доказательства теоремы 2 очень быстро приводит к цели, но он не дает средства для фактического вычисления  $d$ . Предлагаемый способ — найти наименьшее натуральное число в бесконечном множестве чисел  $M$  — совершенно не эффективен. Однако деление с остатком позволяет быстро «спускаться» внутри  $M$  к наименьшему натуральному числу, содержащемуся в  $M$ , т. е. к наибольшему общему делителю. Именно, поделим с остатком  $a$  на  $b$  (считаем, что  $b \neq 0$ ), затем  $b$  на первый остаток, затем первый на второй и т. д. Получим цепочку равенств и неравенств:

$$a = bq_1 + r_1, \quad 0 < r_1 \leq |b| - 1, \quad b = r_1q_2 + r_2, \quad 0 < r_2 \leq r_1 - 1 \text{ и т. д.}$$

Каждый последующий остаток есть натуральное число, строго меньшее предыдущего. Поэтому процесс не может продолжаться без конца. Но закончиться он может только на том, что на каком-то шагу деление выполнится без остатка. Таким образом,

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 &\leq |b| - 1; \\ b &= r_1q_2 + r_2, & 0 < r_2 &\leq r_1 - 1; \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 &\leq r_2 - 1; \\ &\dots\dots\dots & & \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 < r_k &\leq r_{k-1} - 1; \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

Покажем, что последний отличный от нуля остаток  $r_k$  равен н. о. д. ( $a, b$ ). Для этого сначала пересмотрим все равенства снизу вверх:  $r_{k-1}$  делится на  $r_k$ ,  $r_{k-2}$ , как сумма двух чисел, делящихся на  $r_k$ , тоже делится на  $r_k$  и т. д. К третьему сверху равенству мы придем, зная, что  $r_2$  и  $r_3$  делятся на  $r_k$ , и заключим отсюда, что  $r_1$  делится на  $r_k$ . Из второго заключим, что  $b$  делится на  $r_k$ , из первого — что  $a$  делится на  $r_k$ . Таким образом,  $a$  и  $b$  делятся на  $r_k$ .

Пусть теперь  $d'$  — какой-либо общий делитель для  $a$  и  $b$ . Пересмотрим равенства сверху вниз с точки зрения делимости на  $d'$ . Из первого равенства заключаем, что  $r_1$  как разность двух чисел, делящихся на  $d'$ , делится на  $d'$ . Из второго — что  $r_2$  делится на  $d'$  по той же причине, и т. д. Из предпоследнего заключим, что

$r_k$  делится на  $d'$  и, следовательно,  $r_k \geq d'$ . Итак,  $r_k$  оказывается общим делителем, причем наибольшим.

Изложенный способ отыскания н. о. д. называется *алгоритмом Евклида*, он известен уже более 2000 лет. В процессе доказательства мы вновь установили свойство (2) н. о. д. Далее, из сказанного ранее ясно, что все остатки  $r_1, r_2, \dots, r_k$  принадлежат множеству  $M$ , что дает доказательство и свойства (1), причем представление остатков в виде  $au + bv$  легко осуществляется шаг за шагом. Таким образом, алгоритм Евклида дает не только способ вычисления н. о. д. чисел  $a$  и  $b$ , но и его линейное представление в виде  $au_0 + bv_0$ .

**Пример.** Пусть  $a = 959$ ,  $b = 343$ . Найти их н. о. д. и найти его линейное представление.

Решение:  $959 = 343 \cdot 2 + 273$ ;  $343 = 273 \cdot 1 + 70$ ;  $273 = 70 \cdot 3 + 63$ ;  $70 = 63 \cdot 1 + 7$ ;  $63 = 7 \cdot 9 + 0$ . Таким образом,  $d = 7$ .  
Далее,  $273 = 959 - 343 \cdot 2$ ;  $70 = 343 - 273 \cdot 1 = 343 - (959 - 343 \cdot 2) \cdot 1 = 343 \cdot 3 - 959$ ;  $63 = 273 - 70 \cdot 3 = 959 - 343 \cdot 2 - (343 \cdot 3 - 959) \cdot 3 = 959 \cdot 4 - 343 \cdot 11$ ;  $7 = 70 - 63 = 343 \cdot 3 - 959 - (959 \cdot 4 - 343 \cdot 11) = 343 \cdot 14 - 959 \cdot 5$ . Таким образом,  $7 = 959 \cdot u_0 + 343 \cdot v_0$  при  $u_0 = -5$ ;  $v_0 = 14$ .

**5. Взаимно простые числа.** Два целых числа называются *взаимно простыми*, если их н. о. д. равен 1.

Ясно, что если  $d$  есть наибольший общий делитель целых чисел  $a$  и  $b$ , то  $\frac{a}{d}$  и  $\frac{b}{d}$  суть целые взаимно простые числа. Действительно, то, что эти числа целые, следует из того, что  $d$  — общий делитель для  $a$  и  $b$ . Если  $\delta$  — наибольший общий делитель  $\frac{a}{d}$  и  $\frac{b}{d}$ , то  $a$  и  $b$  делятся на  $d\delta$ , откуда следует, что  $\delta = 1$ , иначе  $d$  не был бы наибольшим общим делителем для  $a$  и  $b$ .

**Предложение 5.** Для того чтобы целые числа  $a$  и  $b$  были взаимно простыми, необходимо и достаточно существование целых чисел  $u_0, v_0$  таких, что  $au_0 + bv_0 = 1$ .

Предложение 5 можно сформулировать и в других терминах: для того чтобы неопределенное уравнение  $au + bv = 1$  имело решение  $u_0, v_0$  в целых числах, необходимо и достаточно, чтобы  $a$  и  $b$  были взаимно просты.

**Доказательство.** Пусть  $a$  и  $b$  взаимно просты. Тогда их н. о. д., равный 1, имеет линейное представление:  $1 = au_0 + bv_0$ . Пусть теперь существуют  $u_0$  и  $v_0$  такие, что  $au_0 + bv_0 = 1$ . Тогда н. о. д.  $(a, b)$  делит  $au_0$  и  $bv_0$ , а следовательно, и их сумму, равную 1. Но 1 не имеет натуральных делителей, кроме 1, так что н. о. д.  $(a, b)$  равен 1. Предложение доказано полностью.

**Предложение 6.** Если целые числа  $a_1, a_2$  взаимно просты с целым числом  $b$ , то их произведение  $a_1 a_2$  тоже взаимно просто с  $b$ .

**Доказательство.** Существуют целые  $u_1, v_1, u_2, v_2$  такие, что  $a_1u_1 + bv_1 = 1$ ,  $a_2u_2 + bv_2 = 1$  в силу предложения 5. Перемножая эти равенства, получим после очевидных преобразований

$$a_1a_2u_1u_2 + b(a_1u_1v_2 + a_2u_2v_1 + bv_1v_2) = 1,$$

откуда, в силу того же предложения, числа  $a_1a_2$  и  $b$  взаимно просты, ибо  $u_1u_2$  и  $a_1u_1v_2 + a_2u_2v_1 + bv_1v_2$  — целые числа.

**Предложение 7.** Если целые числа  $a_1, a_2, \dots, a_k$  все взаимно просты с  $b$ , то произведение  $a_1a_2 \dots a_k$  тоже взаимно просто с  $b$ .

**Доказательство.** Применим метод математической индукции. При  $k = 2$  предложение верно в силу предложения 6. Допустим, что оно верно для произведения  $k - 1$  множителей, и в этом предположении докажем его для  $k$  множителей. Запишем  $a_1a_2 \dots a_k$  как  $a_1(a_2 \dots a_k)$ . Первый множитель  $a_1$  взаимно прост с  $b$  по условию. Второй  $a_2 \dots a_k$  взаимно прост с  $b$  в силу индуктивного предположения. Следовательно, мы можем применить предложение 6 и заключить, что  $a_1a_2 \dots a_k$  взаимно просто с  $b$ , что и требовалось доказать.

**Предложение 8.** Если целые числа  $a_1, \dots, a_k$  и  $b_1, \dots, b_m$  таковы, что каждое число  $a_i, i = 1, \dots, k$ , взаимно просто с каждым числом  $b_j, j = 1, \dots, m$ , то их произведения  $a_1 \dots a_k$  и  $b_1 \dots b_m$  взаимно просты.

**Доказательство.** Применив  $m$  раз предложение 7 к числам  $a_1, \dots, a_k$  и  $b_j, j = 1, \dots, m$ , получим, что числа  $b_1, \dots, b_m$  взаимно просты с числом  $a_1 \dots a_k$ . Применяя еще раз предложение 7, получим, что  $b_1 \dots b_m$  взаимно просто с  $a_1 \dots a_k$ , что и требовалось доказать.

**Предложение 9.** Если целые числа  $a$  и  $b$  взаимно просты, то при натуральных  $k$  и  $m$  числа  $a^k$  и  $b^m$  тоже взаимно просты.

Для доказательства достаточно в предложении 8 положить  $a_1 = \dots = a_k = a, b_1 = \dots = b_m = b$ .

**Предложение 10.** Если произведение  $ab$  двух целых чисел  $a$  и  $b$  делится на целое число  $c$  и первый множитель  $a$  взаимно прост с  $c$ , то  $b$  делится на  $c$ .

**Доказательство.** По условию  $a$  и  $c$  взаимно просты, так что существуют целые  $u_0$  и  $v_0$  такие, что  $au_0 + cv_0 = 1$ . Умножив это равенство на  $b$ , получим  $abu_0 + cbv_0 = b$ . Первое слагаемое левой части делится на  $c$  по условию, второе делится на  $c$  тривиальным образом. Следовательно, и их сумма  $b$  делится на  $c$ , что и требовалось доказать.

**Предложение 11.** Если целое число  $a$  делится на целые взаимно простые числа  $b_1$  и  $b_2$ , то  $a$  делится и на их произведение.

**Доказательство.** Пусть  $a = b_1c$  при целом  $c$ . По условию  $a$  делится на  $b_2$ , а  $b_1$  взаимно просто с  $b_2$ . Следовательно, согласно предложению 8 число  $c$  делится на  $b_2$ , т. е.  $c = b_2t$  при целом  $t$ . Поэтому  $a = (b_1b_2)t$ , что и требовалось доказать.

Установленные предложения очень просты и кажутся почти тривиальными. Тем не менее из них можно вывести некоторые не совсем тривиальные следствия.

Выведем, например, что степень с натуральным показателем дробного рационального положительного числа не может быть целым числом.

Действительно, пусть  $a/b$  — дробное рациональное число с целым положительным знаменателем  $b$  и с целым числителем  $a$ . Без нарушения общности можно считать, что числитель и знаменатель взаимно просты, этого можно добиться за счет сокращения на наибольший общий делитель. Пусть это выполнено. Ясно, что  $b > 1$ , иначе  $a/b$  было бы целым. Пусть  $m$  — натуральное число. Тогда  $(a/b)^m = a^m/b^m$ . В силу предложения 7  $a^m$  и  $b^m$  взаимно просты. Поэтому  $a^m$  не может делиться на  $b^m$ , так что  $a^m/b^m$  не является целым числом.

Из доказанного следует далее, что если целое положительное число  $c$  не является  $m$ -й степенью целого числа (при натуральном  $m$ ), то оно не является  $m$ -й степенью дробного рационального

числа. Поэтому  $\sqrt[m]{c}$  есть либо целое число, либо иррациональное. Так, числа  $\sqrt{2}$ ,  $\sqrt{3}$ ,  $\sqrt{5}$ ,  $\sqrt{6}$ ,  $\sqrt{7}$ ,  $\sqrt{8}$ ,  $\sqrt{10}$ , ... (пропускаются целые  $\sqrt{4}$ ,  $\sqrt{9}$ , ...) все иррациональны, также иррациональны и числа  $\sqrt[3]{2}$ ,  $\sqrt[3]{3}$ ,  $\sqrt[3]{4}$ ,  $\sqrt[3]{5}$ ,  $\sqrt[3]{6}$ ,  $\sqrt[3]{7}$ ,  $\sqrt[3]{9}$ ,  $\sqrt[3]{10}$ , ... (пропускаются целые  $\sqrt[3]{8}$ ,  $\sqrt[3]{27}$ , ...) и т. д.

**6. Простые числа.** Целое положительное число, большее единицы, называется *простым*, если оно не имеет целых положительных делителей кроме себя и единицы. Так, числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 простые, а числа 4, 6, 8, 9, 10, 12, 14, ... нет. Непростые числа 4, 6, ... называются также *составными*. Число 1 не относится ни к простым, ни к составным числам.

**Предложение 12.** *Всякое целое число, большее 1, делится по крайней мере на одно простое число.*

**Доказательство.** Пусть  $n > 1$  — целое положительное число. Если оно простое, предложение верно, ибо  $n$  всегда делится на себя. Если оно составное, то оно делится на число  $n_1 > 1$ , меньшее чем  $n$ . Если  $n_1$  простое, предложение доказано:  $n$  делится на  $n_1$ . Если нет, то оно делится на меньшее чем  $n_1$  число  $n_2$  и т. д.

Процесс выделения делителей  $n > n_1 > n_2 > \dots$  оборвется через конечное число шагов, а оборваться он может только на том, что мы придем к простому делителю  $n_k$ . Предложение доказано.

Простых чисел существует бесконечно много. Это непосредственно вытекает из следующего предложения.

**Предложение 13.** *Каково бы ни было конечное множество простых чисел  $\{p_1, p_2, \dots, p_k\}$ , всегда найдется простое число, не принадлежащее этому множеству.*

**Доказательство.** Рассмотрим число  $n = p_1 p_2 \dots p_k + 1$ . В силу предложения 12 оно делится по крайней мере на одно простое число  $p$ . Это число  $p$  не может совпадать ни с одним из чисел  $p_1, p_2, \dots, p_k$ . Действительно, если  $p = p_i$ , то 1 делится на  $p_i$  как разность двух чисел, делящихся на  $p_i$ , что невозможно.

Это рассуждение было известно еще Евклиду.

**Предложение 14.** *Если целое число  $n$  не делится на простое число  $p$ , то  $n$  и  $p$  взаимно просты.*

**Доказательство.** Пусть  $d = (n, p)$ . Так как  $p$  делится на  $d$  и  $p$  простое, для  $d$  имеются только две возможности:  $d = p$  или  $d = 1$ . В первом случае  $n$  делится на  $p$ , во втором  $n$  и  $p$  взаимно просты, что и требовалось доказать.

Из предложения 14 вытекает следующее утверждение.

**Предложение 15.** *Если  $p_1$  и  $p_2$  — два различных простых числа, то они взаимно просты.*

Действительно, меньшее из них не делится на большее, и, следовательно, они взаимно просты.

**Предложение 16.** *Если произведение двух целых чисел делится на простое число, то по крайней мере один из сомножителей делится на это простое число.*

Действительно, пусть  $ab$  делится на  $p$ , где  $a, b \in \mathbb{Z}$ ,  $p$  — простое. Если  $a$  делится на  $p$ , то предложение справедливо. Если  $a$  не делится на  $p$ , то  $a$  и  $p$  взаимно просты, а тогда, согласно предложению 10,  $b$  делится на  $p$ .

Это предложение легко обобщается.

**Предложение 17.** *Если произведение нескольких целых чисел делится на простое число, то на него делится хотя бы один из сомножителей.*

**Доказательство.** Применим метод математической индукции по числу сомножителей. База есть — предложение верно для двух сомножителей. Допустим, что оно верно для произведения  $k - 1$  сомножителей. Пусть теперь  $a_1 a_2 \dots a_k$  делится на простое число  $p$ . Так как  $a_1 a_2 \dots a_k = a_1 (a_2 \dots a_k)$ , заключаем на основании предложения 14, что либо  $a_1$  делится на  $p$ , либо произведение  $a_2 \dots a_k$  делится на  $p$ . Во втором случае, в силу индуктивного предположения, один из сомножителей  $a_2, \dots, a_k$  делится на  $p$ , а в первом  $a_1$  делится на  $p$ . Тем самым предложение доказано.

Теперь мы в состоянии доказать основную теорему теории делимости целых чисел.

**Теорема 18.** *Каждое натуральное число, большее единицы, может быть представлено в виде произведения простых сомножителей, и два таких разложения могут отличаться только порядком следования сомножителей.*

**Доказательство.** Применим метод индукции. Для числа 2 утверждение теоремы тривиально (так же, как и для всякого простого числа). Допустим, что теорема верна для всех натуральных

чисел, меньших  $n$ , и в этом предположении докажем ее для числа  $n$ .

В силу предложения 12 число  $n$  делится на некоторое простое число  $p_1$ , так что  $n = p_1 n_1$ , причем  $n_1 < n$ . Если  $n_1 = 1$ , то  $n$  есть «произведение» одного сомножителя  $p_1$ . Если  $n_1 > 1$ , то в силу индуктивного предположения  $n_1$  допускает разложение на простые сомножители:  $n_1 = p_2 \dots p_k$ , и тогда  $n = p_1 p_2 \dots p_k$ . Возможность разложения доказана.

Докажем однозначность разложения с точностью до порядка следования сомножителей. Пусть  $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ , где все числа  $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$  простые. Из этого равенства следует, что произведение  $q_1 q_2 \dots q_l$  делится на  $p_1$ . В силу предложения 15 один из сомножителей  $q_1, q_2, \dots, q_l$  должен делиться на  $p_1$  и в силу простоты  $q_1, q_2, \dots, q_l$  совпадать с  $p_1$ . Без нарушения общности, за счет изменения нумерации сомножителей второго разложения, мы можем принять, что  $q_1 = p_1$ , так что  $p_1 p_2 \dots p_k = p_1 q_2 \dots q_l$ , откуда  $p_2 \dots p_k = q_2 \dots q_l$ . Но  $p_2 \dots p_k = n/p_1 < n$ . Поэтому можно применить индуктивное предположение, так что  $l = k$ , и простые числа  $q_2, \dots, q_k$  отличаются от  $p_2, \dots, p_k$  только порядком следования. Теорема доказана.

Среди сомножителей в разложении  $n = p_1 p_2 \dots p_k$  могут быть равные. Их принято объединять в виде степеней. Разложение в форме  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  при попарно различных  $p_1, p_2, \dots, p_m$  называется *каноническим разложением* натурального числа  $n$ . Каноническое разложение распространяется на все целые числа, кроме 0, в форме

$$n = (-1)^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m},$$

где  $\alpha_0$  принимает значения 0, 1.

Далее, каноническое разложение может быть распространено на дробные рациональные числа, если допустить отрицательные значения для  $\alpha_1, \dots, \alpha_m$ . Чтобы получить каноническое разложение для дробного рационального числа, нужно написать разложение для числителя и знаменателя и выполнить деление одного на другое, употребляя, в случае надобности, отрицательные показатели. Так,  $\frac{63}{10} = 2^{-1} 3^2 5^{-1} 7$ ,  $-\frac{125}{54} = (-1) 2^{-1} 3^{-3} 5^3$ .

Теорема об однозначном разложении целых чисел на простые множители играет исключительно большую роль в теории чисел.

## § 2. Теория сравнений

Пусть  $m$  — данное натуральное число. Все целые числа по отношению к числу  $m$  естественно разбиваются на  $m$  классов, если отнести к одному классу числа, дающие один и тот же остаток при делении на  $m$ . Так, если  $m = 2$ , целые числа разбиваются на

классы четных и нечетных чисел. Если  $m = 3$ , классы в этом смысле составляют числа вида  $3k, 3k + 1, 3k + 2$  при целых  $k$  и т. д. Числа, относящиеся к одному классу, называются *сравнимыми*, и изучение свойств классов носит название теории сравнений. Переходим к точным определениям относящихся сюда понятий.

**1. Определение и простейшие свойства.** Пусть  $m$  — натуральное число. Два целых числа  $a$  и  $b$  называются *сравнимыми по модулю  $m$* , если их разность  $a - b$  делится на  $m$ . Высказывание « $a$  и  $b$  сравнимы по модулю  $m$ » записывается в виде  $a \equiv b \pmod{m}$ .

Предложение 1.  $a \equiv a \pmod{m}$ ; далее, если  $a \equiv b \pmod{m}$ , то  $b \equiv a \pmod{m}$ ; если  $a \equiv b \pmod{m}$  и  $b \equiv c \pmod{m}$ , то  $a \equiv c \pmod{m}$ .

Действительно,  $a - a = 0$  делится на любое число; если  $a - b$  делится на  $m$ , то и  $b - a$  делится на  $m$ ; если  $a - b$  и  $b - c$  делятся на  $m$ , то  $a - c = (a - b) + (b - c)$  тоже делится на  $m$ .

Именно эти свойства сравнений позволяют заключить, что каждое целое число попадает в один и только один класс попарно сравнимых между собой целых чисел. Эти классы называются *классами вычетов по модулю  $m$*  или просто *классами по модулю  $m$* .

Предложение 2. Каждое целое число сравнимо по модулю  $m$  с одним и только одним из чисел ряда  $0, 1, \dots, m - 1$ .

Действительно, пусть  $a$  — некоторое целое число. Поделим его на  $m$  с остатком:  $a = mq + r$ ,  $0 \leq r \leq m - 1$ . Ясно, что  $a \equiv r \pmod{m}$ , ибо  $a - r = mq$  делится на  $m$ . Итак, каждое целое число  $a$  сравнимо со своим остатком при делении на  $m$ . Остается показать, что среди чисел  $0, 1, \dots, m - 1$  нет сравнимых по модулю  $m$ . Но это ясно — если взять два различных целых числа этого ряда и вычесть из большего меньшее, мы получим в качестве разности положительное число, меньшее чем  $m$ , и, следовательно, эта разность не делится на  $m$ . Предложение доказано.

В процессе доказательства мы убедились, что каждый класс по модулю  $m$  действительно состоит из чисел, дающих один и тот же остаток при делении на  $m$ .

Любая совокупность чисел, взятых по одному из каждого класса по модулю  $m$ , называется *полной системой вычетов по модулю  $m$* . Например, числа  $0, 1, \dots, m - 1$  образуют полную систему вычетов. Полной же системой вычетов будет  $1, 2, \dots, m$ ; при нечетном  $m = 2k + 1$  полной системой вычетов будет  $-k, \dots, -1, 0, 1, \dots, k$ , и т. д.

Предложение 3. Если  $a_1 \equiv a_2 \pmod{m}$  и  $b_1 \equiv b_2 \pmod{m}$ , то  $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$ .

Доказательство. Если  $a_1 \equiv a_2 \pmod{m}$  и  $b_1 \equiv b_2 \pmod{m}$ , то  $a_1 - a_2$  и  $b_1 - b_2$  делятся на  $m$ , а следовательно, и  $a_1 \pm b_1 - (a_2 \pm b_2) = (a_1 - a_2) \pm (b_1 - b_2)$  тоже делится на  $m$ , т. е.  $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$ .

Предложение 4. Если  $a_1 \equiv a_2 \pmod{m}$  и  $b_1 \equiv b_2 \pmod{m}$ , то  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$ .

**Доказательство.**  $a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$ . Если  $a_1 \equiv a_2$  и  $b_1 \equiv b_2 \pmod{m}$ , то оба слагаемых делятся на  $m$ , а с ними и их сумма  $a_1b_1 - a_2b_2$ . Следовательно,  $a_1b_1 \equiv a_2b_2 \pmod{m}$ , что и требовалось доказать.

В частности, если  $a_1 \equiv a_2 \pmod{m}$  и  $c$  — любое целое число, то  $a_1c \equiv a_2c \pmod{m}$ .

**Предложение 5.** Если  $ca_1 \equiv ca_2 \pmod{m}$  и число  $c$  взаимно просто с  $m$ , то  $a_1 \equiv a_2 \pmod{m}$ .

Действительно, если  $ca_1 \equiv ca_2 \pmod{m}$ , то  $ca_1 - ca_2 = c(a_1 - a_2)$  делится на  $m$ ,  $c$  взаимно просто с  $m$  и согласно предложению 8  $a_1 - a_2$  делится на  $m$ , что и требовалось доказать.

Таким образом, обе части сравнения можно сократить на множитель, взаимно простой с модулем. Без предположения о взаимной простоте это, вообще говоря, делать нельзя. Так,  $2 \equiv 6 \pmod{4}$ , но  $1 \not\equiv 3 \pmod{4}$ .

**2. Действия над классами.** Пусть  $m = 6$ . Представим себе, что числа, сравнимые с нулем, мы записываем черными цифрами, сравнимые с единицей — красными, сравнимые с 2 — желтыми, сравнимые с 3 — фиолетовыми, сравнимые с 4 — зелеными и сравнимые с 5 — синими. Тогда предложения 3 и 4 можно переформулировать так: цвет суммы двух чисел зависит только от цветов слагаемых, но не от того, как выбраны эти слагаемые внутри своих классов. То же относится к разности и к произведению. Например, складывая «желтое» число с «синим», мы всегда получим «красное». Умножая «синее» на «фиолетовое», мы всегда получим «фиолетовое», и т. д. Сокращенно это можно записать:  $ж + с = к$ ;  $с \cdot ф = ф$  и т. д. Для шести символов: ч, к, ж, ф, з, с мы можем записать «суммы», «разности» и «произведения», руководствуясь сложением, вычитанием и умножением чисел (все равно каких), взятых из соответствующих классов.

То же самое имеет место при любом  $m$ . Для того чтобы указать класс, к которому принадлежит сумма, разность или произведение двух чисел, нам достаточно знать классы, к которым эти числа принадлежат, а как они выбраны внутри классов — на результате не сказывается. Это обстоятельство делает естественными следующие определения.

**Суммой** двух классов по модулю  $m$  называется класс по модулю  $m$ , к которому принадлежит сумма каких-либо чисел из слагаемых классов.

**Произведением** двух классов по модулю  $m$  называется класс по модулю  $m$ , к которому принадлежит произведение каких-либо чисел из перемножаемых классов.

В силу предложений 3, 4 эти определения корректны — какие бы числа из двух данных классов мы ни выбрали, их сумма и их произведение будут принадлежать вполне определенным классам, не зависящим от выбора чисел внутри данных классов.

**Пример.** Приведем «таблицы умножения» для классов по модулю 7 и 8.

Таблица 1

$m=7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Таблица 2

$m=8$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Символы  $\bar{0}$ ,  $\bar{1}$ ,  $\bar{2}$ ,  $\bar{3}$ ,  $\bar{4}$ ,  $\bar{5}$ ,  $\bar{6}$  в табл. 1 обозначают классы по модулю 7, которым принадлежат числа 0, 1, 2, 3, 4, 5, 6. Значение символов в табл. 2 — аналогично. Такими обозначениями мы будем пользоваться и впредь — символ  $\bar{a}$  будет обозначать класс по модулю (который предполагается заданным), содержащий число  $a$ .

Рассмотрение классов по модулю как объектов, над которыми совершаются действия, часто вызывает у начинающих некоторое затруднение. Иногда оно вызывается тем, что класс это не число, а бесконечное множество чисел, и сама мысль о том, что действие над классами суть действия сразу над бесконечными множествами чисел, кажется противоестественной. Для преодоления этого психологического барьера следует мыслить вместо класса одно из чисел этого класса, но безразлично какое, как бы отказываясь различать их одно от другого, как бы «склеивая» их в один объект. Собственно говоря, это обычный и привычный в обыденной жизни путь формирования абстрактного понятия. Говоря слово «яблоко», мы отвлекаемся от особенностей конкретных представителей этого класса предметов и подразумеваем некоторое яблоко, все равно какое. Нам привычно, говоря «яблоко», не вызывать в воображении множество всех имеющихся на земле в данный момент яблок. Так же надо относиться к понятию «класс по модулю  $m$ ».

Отметим некоторые очевидные свойства действий над классами по модулю.

1.  $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$  (ассоциативность сложения).

Действительно,  $(\bar{a} + \bar{b}) + \bar{c}$  есть класс, содержащий  $(a + b) + c$ , а  $\bar{a} + (\bar{b} + \bar{c})$  есть класс, содержащий  $a + (b + c)$ . Но  $(a + b) + c = a + (b + c)$ , откуда и следует требуемое.

2.  $\bar{a} + \bar{b} = \bar{b} + \bar{a}$  (коммутативность сложения).

3. Класс  $\bar{0}$  играет роль нуля при сложении:  $\bar{a} + \bar{0} = \bar{a}$  при любом  $\bar{a}$ .

4. Класс  $\overline{-a}$  играет роль класса, противоположного классу  $\bar{a}$ , именно,  $\bar{a} + (\overline{-a}) = \bar{0}$ .

$$5. \bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c};$$

$$5'. (\bar{b} + \bar{c})\bar{a} = \bar{b}\bar{a} + \bar{c}\bar{a} \text{ (дистрибутивность).}$$

$$6. \bar{a}(\bar{b}\bar{c}) = (\bar{a}\bar{b})\bar{c} \text{ (ассоциативность умножения).}$$

$$7. \bar{a}\bar{b} = \bar{b}\bar{a} \text{ (коммутативность умножения).}$$

Свойства 3 и 4 очевидны. Свойства 2, 5, 6, 7 доказываются точно так же, как свойство 1, посредством перехода от классов к любым числам из этих классов, для которых соответствующие свойства действий имеют место.

8. Класс  $\bar{1}$  играет роль единицы при умножении классов, именно,  $\bar{a} \cdot \bar{1} = \bar{a}$  при любом  $\bar{a}$ .

**3. Приведенная система вычетов и примитивные классы.**

Предложение 6. Пусть  $d = \text{н.о.д.}(a, m)$  и  $a_1 \equiv a \pmod{m}$ . Тогда н.о.д.  $(a_1, m) = d$ .

Доказательство. Имеем  $a_1 = a + mq$  при некотором  $q \in \mathbb{Z}$ , так что  $d$  есть общий делитель для  $a_1$  и  $m$ , и потому  $d \leq d_1$ , где  $d_1 = \text{н.о.д.}(a_1, m)$ . С другой стороны,  $a = a_1 - mq$ , откуда следует, что  $d_1$  является общим делителем для  $a$  и  $m$ , так что  $d_1 \leq d$ . Отсюда заключаем, что  $d_1 = d$ .

В частности, если одно из чисел класса по модулю  $m$  взаимно просто с  $m$ , то и все числа этого класса взаимно просты с  $m$ .

Классы, состоящие из чисел, взаимно простых с модулем, называются *примитивными классами*. Для любого модуля примитивные классы существуют; такими будут, в частности, классы  $\bar{1}$  и  $\overline{m-1}$ .

Предложение 7. Для того чтобы сравнение  $ax \equiv 1 \pmod{m}$  имело решение, необходимо и достаточно, чтобы  $a$  было взаимно просто с  $m$ .

Доказательство. Необходимость. Пусть существует целое число  $x_0$  такое, что  $ax_0 \equiv 1 \pmod{m}$ . Число 1 взаимно просто с  $m$ , значит (предложение 6), число  $ax_0$  взаимно просто с  $m$ , откуда  $a$  взаимно просто с  $m$ , что и требовалось доказать.

Достаточность. Пусть  $a$  взаимно просто с  $m$ . Тогда, согласно предложению 5 § 1, существуют целые числа  $u$  и  $v$  такие, что  $au + mv = 1$ . Ясно, что  $au \equiv 1 \pmod{m}$ , так что  $u$  есть решение сравнения  $ax \equiv 1 \pmod{m}$ .

Предложение 7 можно в терминах классов сформулировать так: для того чтобы класс  $\bar{a}$  имел обратный  $\bar{a}^{-1}$ , т. е. такой, что  $\bar{a}\bar{a}^{-1} = \bar{1}$ , необходимо и достаточно, чтобы класс  $\bar{a}$  был примитивным.

Ясно, что если  $x_0$  — решение сравнения  $ax \equiv 1 \pmod{m}$ , то все сравнимые с  $x_0$  числа тоже доставляют решения, так что решение «приводит за собой» весь класс, его содержащий. В этом смысле

решений бесконечно много. Однако класс решений существует только один. Действительно, если  $ax_0 \equiv 1 \pmod{m}$  и  $ax_1 \equiv 1 \pmod{m}$ , то  $ax_0 \equiv ax_1 \pmod{m}$ , и в силу взаимной простоты  $a$  и  $m$ ,  $x_0 \equiv x_1 \pmod{m}$ . В терминах классов: обратный класс  $\bar{a}^{-1}$  к примитивному классу  $\bar{a}$  существует только один.

Число примитивных классов по модулю  $m$  обозначается  $\varphi(m)$ . Так определенная функция называется *функцией Эйлера*. Ясно, что  $\varphi(1) = 1$ . Для  $m > 1$   $\varphi(m)$  равно, очевидно, числу взаимно простых с  $m$  чисел ряда  $0, 1, \dots, m-1$ . Так,  $\varphi(2) = 1$ ,  $\varphi(3) = 2$ ,  $\varphi(4) = 2$ ,  $\varphi(5) = 4$ ,  $\varphi(6) = 2$ ,  $\varphi(7) = 6$ ,  $\varphi(8) = 4$  и т. д.

Если модуль есть простое число  $p$ , то все классы, кроме нулевого, примитивны, так что  $\varphi(p) = p - 1$ .

**Предложение 8.** Сравнение  $ax \equiv b \pmod{m}$ , если  $a$  взаимно просто с  $m$ , имеет единственный класс решений.

**Доказательство.** Пусть  $a'$  — решение сравнения  $ax \equiv 1 \pmod{m}$ . Ясно, что  $a'b$  есть решение сравнения  $ax \equiv b \pmod{m}$ , ибо  $a(a'b) = aa' \cdot b \equiv 1 \cdot b \pmod{m}$ . Если  $x_0$  — какое-либо решение сравнения  $ax \equiv b \pmod{m}$ , т. е.  $ax_0 \equiv b \pmod{m}$ , то  $a'ax_0 \equiv a'b \pmod{m}$ , откуда  $x_0 \equiv a'b \pmod{m}$ , ибо  $a'a \equiv 1 \pmod{m}$ .

В терминах классов предложение 8 означает, что возможное деление на примитивный класс: уравнение  $\bar{a}\bar{x} = \bar{b}$  имеет единственное решение  $\bar{x} = \bar{a}^{-1}\bar{b}$ .

Если модуль  $m$  есть простое число, то все классы, кроме нулевого, примитивны, так что в этом случае возможно деление на любой класс, кроме нулевого.

Имеет место следующая теорема, носящая имя Эйлера.

**Теорема Эйлера.** Если  $a$  и  $m$  взаимно просты, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

**Доказательство.** Пусть  $a_1, a_2, \dots, a_k$  — числа, взятые по одному из каждого примитивного класса, так что  $k = \varphi(m)$ . Пусть  $a$  взаимно просто с  $m$ . Тогда числа  $aa_1, aa_2, \dots, aa_k$  тоже взаимно просты с  $m$ , т. е. принадлежат примитивным классам. Все они попарно несравнимы между собой. Действительно, если  $aa_i \equiv aa_j \pmod{m}$ , то в силу предложения 5  $a_i \equiv a_j \pmod{m}$ , что возможно только если  $a_i$  и  $a_j$  равны. Итак, числа  $aa_1, aa_2, \dots, aa_k$  лежат в разных классах и, так как их число равно числу классов, среди них имеется по одному из всех классов («10 человек в 10 комнатах, ни в одной нет двоих, следовательно, все комнаты заняты»). Поэтому числа  $aa_1, aa_2, \dots, aa_k$  сравнимы с  $a_1, a_2, \dots, a_k$ , расположенными, быть может, в другом порядке. Запишем это:

$$\begin{aligned} aa_1 &\equiv a_{i_1}, \\ aa_2 &\equiv a_{i_2}, \\ &\dots \\ aa_k &\equiv a_{i_k}. \end{aligned} \quad (\text{mod } m)$$

Здесь  $i_1, i_2, \dots, i_k$  — те же числа  $1, 2, \dots, k$ , но в другом порядке. Перемножив эти сравнения, получим

$$a^k a_{i_1} a_{i_2} \dots a_k \equiv a_{i_1} a_{i_2} \dots a_{i_k} \pmod{m}.$$

Но  $a_{i_1} a_{i_2} \dots a_{i_k} = a_1 a_2 \dots a_k$ , так как сомножители различаются только порядком. Итак,

$$a^k a_1 a_2 \dots a_k \equiv a_1 a_2 \dots a_k \pmod{m}.$$

Число  $a_1 a_2 \dots a_k$  взаимно просто с  $m$ , и на него можно сократить обе части последнего сравнения. Поэтому  $a^k \equiv 1 \pmod{m}$ , и остается вспомнить, что  $k = \varphi(m)$ .

В терминах классов теорема Эйлера выглядит так: если  $\bar{a}$  — примитивный класс по модулю  $m$ , то  $\bar{a}^{\varphi(m)} = \bar{1}$ .

Важным частным случаем теоремы Эйлера является теорема Ферма: если  $p$  — простое число и  $a$  не делится на  $p$ , то  $a^{p-1} \equiv 1 \pmod{p}$ . Она непосредственно следует из теоремы Эйлера, ибо  $\varphi(p) = p - 1$ . Теорему Ферма часто записывают в равносильной форме  $a^p \equiv a \pmod{p}$ . В этой записи предположение о том, что  $a$  не делится на  $p$ , становится излишним.

Теорема Эйлера дает возможность в явном виде записывать класс, обратный к данному примитивному классу. Именно,  $\bar{a}^{-1} = \bar{a}^{\varphi(m)-1}$ .

### § 3. Некоторые общие понятия алгебры

**1. Группы.** В теории сравнений мы встретились с новым явлением, имеющим большую принципиальную важность. Мы обнаружили математические объекты, именно, классы по модулю, не являющиеся числами, но над которыми мы имеем возможность совершать алгебраические действия. Свойства этих действий напоминают свойства действий над числами. Подобного рода системы объектов возникают в математике в разнообразных ситуациях, и это делает естественной и необходимой формализацию возникающих на этом пути более общих понятий.

*Полугруппой* называется множество, в котором определено действие, сопоставляющее каждой упорядоченной паре элементов третий — результат действия. Действие предполагается ассоциативным. Полугруппами являются: множество целых неотрицательных чисел относительно действия сложения, то же множество относительно действия умножения (это совсем другая полугруппа), множество классов по модулю относительно умножения. Во всех этих примерах действие коммутативно.

Полугруппа называется *группой*, если в ней существует *нейтральный элемент*  $e$  такой, что при всех  $a$  из группы  $a * e = e * a = a$  (через  $*$  обозначен знак действия), и для каждого элемента  $a$  существует *обратный*  $a^{-1}$  такой, что  $a * a^{-1} = a^{-1} * a = e$ .

Примерами групп могут служить: группа всех целых чисел относительно сложения, группа положительных рациональных чисел относительно умножения, группа классов по модулю относительно сложения, группа примитивных классов по модулю относительно умножения. Все эти группы коммутативны. В качестве примера некоммутативной группы рассмотрим множество непрерывных строго возрастающих функций на  $[0, 1]$ , со значениями  $\varphi(0) = 0$ ,  $\varphi(1) = 1$ , т. е. функций, осуществляющих взаимно однозначные отображения промежутка  $[0, 1]$  на себя, по отношению к действию суперпозиции, т. е. подстановки функции в функцию, так что  $(\varphi * \psi)(x) = \varphi(\psi(x))$ . Нейтральным элементом здесь является функция  $\varphi(x) = x$ , осуществляющая отображение каждой точки промежутка на себя. Обратным элементом является обратная функция, ассоциативность очевидна. Рассмотрим функции  $\varphi_1 = x_2$  и  $\varphi_2 = \sin \frac{\pi x}{2}$ . Обе они принадлежат рассматриваемому множеству. Далее,  $(\varphi_1 * \varphi_2)(x) = \left(\sin \frac{\pi x}{2}\right)^2$ , а  $(\varphi_2 * \varphi_1)(x) = \sin \frac{\pi x^2}{2}$ . Это разные функции, так что данная группа некоммутативна.

Коммутативные группы называются также *абелевыми*.

Действие в группе обозначается обычно как умножение (мультипликативная запись), иногда как сложение (аддитивная запись). Аддитивная запись применяется только для абелевых групп. Нейтральный элемент при мультипликативной записи обозначается 1, при аддитивной записи 0. Соответственно, обратный к  $a$  элемент в мультипликативной записи обозначается  $a^{-1}$ , в аддитивной — через  $-a$  (и называется *противоположным* элементом).

**2. Кольца и поля.** *Кольцом* называется множество математических объектов, в котором определены два действия — «сложение» и «умножение», сопоставляющие упорядоченным парам элементов их «сумму» и «произведение», являющиеся элементами того же множества. Предполагается, что действия удовлетворяют следующим требованиям:

1.  $(a + b) + c = a + (b + c)$  (ассоциативность сложения).
2.  $a + b = b + a$  (коммутативность сложения).
3. Существует нулевой элемент 0 такой, что  $a + 0 = a$  при любом  $a$ .
4. Для каждого  $a$  существует противоположный  $-a$  такой, что  $a + (-a) = 0$ .
5.  $(a + b)c = ac + bc$ ;
- 5'.  $c(a + b) = ca + cb$

(левая и правая дистрибутивность).

Первые четыре требования обозначают, что элементы кольца образуют абелеву группу относительно сложения, которая называется *аддитивной группой* кольца.

Выведем простейшие следствия из поставленных требований.

**Предложение 1.** Если  $a + x = a + y$ , то  $x = y$ .

Действительно, пусть  $a + x = a + y$ . Тогда  $(-a) + (a + x) = (-a) + (a + y)$ . Воспользовавшись ассоциативностью, получим  $((-a) + a) + x = ((-a) + a) + y$ ,  $0 + x = 0 + y$ , и, следовательно,  $x = y$ .

**Предложение 2.** При данных  $a$  и  $b$  уравнение  $a + x = b$  имеет единственное решение  $(-a) + b$ .

Действительно, если  $a + x = b$ , то  $(-a) + (a + x) = (-a) + b$ ,  $0 + x = (-a) + b$  и  $x = (-a) + b$ . Обратно, если  $x = (-a) + b$ , то  $a + x = a + ((-a) + b) = 0 + b = b$ .

Из предложения 2 следует единственность нуля и противоположного элемента, ибо  $0$  есть решение уравнения  $a + x = a$ , а  $-a$  есть решение уравнения  $a + x = 0$ .

Предложения 1 и 2 верны для любой абелевой группы, а не только для аддитивной группы кольца.

**Предложение 3.**  $a \cdot 0 = 0 \cdot a = 0$  при любом  $a$ .

Действительно,  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ , и, в силу предложения 2,  $a \cdot 0 = 0$ .

В общем определении кольца на действие умножения не накладывается никаких ограничений кроме дистрибутивности со сложением. Однако чаще всего возникает необходимость рассматривать кольца, в которых умножение удовлетворяет тем или другим дополнительным естественным требованиям.

Наиболее употребимыми являются:

6.  $(ab)c = a(bc)$  (ассоциативность умножения).

При выполнении этого требования элементы кольца образуют подгруппу относительно умножения.

7.  $ab = ba$  (коммутативность умножения).

8. Существование единичного элемента  $1$  (т. е. такого, что  $a \cdot 1 = 1 \cdot a = a$  для любого элемента  $a$ ).

9. Существование обратного элемента  $a^{-1}$  для любого элемента  $a$ , отличного от  $0$ .

В конкретных кольцах эти требования могут выполняться как порознь, так и вместе в различных комбинациях. Кольцо называется *ассоциативным*, если в нем выполнено условие 6, *коммутативным*, если выполнено условие 7, *коммутативным и ассоциативным*, если выполнены условия 6 и 7. Если выполнено условие 8, говорят о *кольце с единицей*, снабжая слово «кольцо» прилагательным в зависимости от выполнения условий 6 и 7.

Если в кольце есть единица, то она единственна. Действительно, если  $1$  и  $1'$  — две единицы, то  $1 \cdot 1' = 1$ , так как  $1'$  — единица, и  $1 \cdot 1' = 1'$ , так как  $1$  — единица, поэтому  $1 = 1'$ .

Кольцо называется *областью целостности*, если из равенства  $ab = 0$  следует, что хотя бы один из сомножителей  $a$  или  $b$  равен  $0$ .

*Поле* называется коммутативное ассоциативное кольцо с единицей, в котором каждый отличный от нуля элемент  $a$  имеет

обратный  $a^{-1}$ . Иными словами, поле есть кольцо, в котором отличные от нуля элементы образуют коммутативную группу. Эта группа носит название *мультипликативной группы* поля.

Любое поле есть область целостности. Действительно, если  $ab = 0$  и  $a \neq 0$ , то  $a^{-1}(ab) = a^{-1}0 = 0$ , и, следовательно,  $b = 0$ .

Существуют поля, в которых некоторое целое кратное 1, т. е.  $m \cdot 1 = \underbrace{1 + 1 + \dots + 1}_m$ , равно нулю. Наименьшее натуральное

число, обладающее этим свойством, называется *характеристикой* поля. Характеристика поля всегда равна простому числу. Действительно, если  $m \cdot 1 = 0$  и  $m = m_1 m_2$  при  $1 < m_1 < m$ , то  $(m_1 \cdot 1)(m_2 \cdot 1) = 0$ , откуда  $m_1 \cdot 1 = 0$  или  $m_2 \cdot 1 = 0$ , так что  $m$  — не наименьшее натуральное. Поле вычетов по простому модулю  $p$  имеет, очевидно, характеристику  $p$ .

Если же любое кратное единицы отлично от нуля, то говорят, что характеристика поля равна 0.

Приведем теперь примеры. Множество  $\mathbb{Z}$  всех целых чисел образует кольцо, коммутативное, ассоциативное и с единицей. Оно является областью целостности, но не полем. Полями являются множество  $\mathbb{Q}$  всех рациональных чисел и множество  $\mathbb{R}$  всех вещественных чисел.

Классы по модулю  $m$  образуют коммутативное ассоциативное кольцо с единицей. Оно называется *кольцом вычетов по модулю  $m$* . Если  $m$  — составное число, то это кольцо не будет областью целостности. Действительно, если  $m = m_1 m_2$ ,  $1 < m_1 < m$ , то  $m_1 \neq 0$ ,  $m_2 \neq 0$ , но  $m_1 m_2 = m = 0$ . Если же  $m = p$  есть простое число, то кольцо вычетов по нему есть не только область целостности, но даже поле. Действительно, предложение 7 § 2 утверждает, что все классы по модулю  $p$ , кроме нулевого, обратимы. В частности, кольцо вычетов по модулю 2, состоящее всего-навсего из двух элементов  $\bar{0}$  и  $\bar{1}$  (классы четных и нечетных чисел), является полем. Это поле, несмотря на свою крайнюю простоту, оказывается важным для некоторых приложений.

Все правила и формулы элементарной алгебры, включая теорию уравнений, полностью сохраняются, если под буквами понимать элементы любого поля, так как в основе этих правил и формул лежат свойства действий и возможность деления, кроме деления на нуль.

Пример. Решить уравнение  $\bar{2}x^2 + \bar{5}x + \bar{4} = \bar{0}$  в поле вычетов по модулю 11.

Применим обычную формулу решения квадратного уравнения:

$$x = \frac{-\bar{5} \pm \sqrt{\bar{5}^2 - 4 \cdot \bar{2} \cdot \bar{4}}}{2 \cdot \bar{2}} = \frac{-\bar{5} \pm \sqrt{-\bar{7}}}{4} = \frac{\bar{6} \pm \sqrt{\bar{4}}}{4} = \frac{\bar{6} \pm \bar{2}}{4},$$

т. е.  $x = \bar{2}$  или  $x = \bar{1}$ .

В этом примере квадратный корень благополучно извлекается. Могло бы случиться и так, что элемент, находящийся под знаком квадратного корня, не является квадратом какого-либо элемента поля. Это означало бы, что данное квадратное уравнение не имеет корней в исходном поле.

**3. Изоморфизм.** Часто оказывается, что группы, возникающие в различных областях математики или ее приложений, оказываются совершенно одинаковыми по своим свойствам, хотя элементы, из которых они составлены, различны по своей природе. Это явление носит название изоморфизма групп.

Дадим точное определение. Взаимно однозначное отображение группы  $G_1$  на группу  $G_2$  называется *изоморфизмом*, если образом результата групповой операции над двумя элементами из  $G_1$  является результат применения групповой операции в  $G_2$  над образами исходных элементов.

В символьной записи, если отображение обозначено через  $\varphi$ , нужно (кроме взаимной однозначности), чтобы  $\varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2)$  (мы прибегаем к мультипликативной записи группового действия). Группы называются *изоморфными*, если для них существует изоморфное отображение. Например, группа классов по модулю 2 относительно сложения изоморфна группе, элементами которой служат числа  $\pm 1$ , а операцией — обычное умножение. Изоморфизм дается сопоставлением классу четных чисел числа 1, а классу нечетных чисел — числа  $-1$ .

Менее тривиальный пример изоморфизма имеется для группы всех вещественных чисел относительно сложения и группы положительных чисел относительно умножения. Изоморфизм дается сопоставлением любому вещественному числу  $x$  значения показательной функции  $a^x$ . Действительно, оно взаимно однозначно (обратное отображение дается логарифмом) и  $a^{x_1} \cdot a^{x_2} = a^{x_1 + x_2}$ .

Аналогично изоморфизму групп дается определение изоморфизма колец. Именно, взаимно однозначное отображение  $\varphi$  кольца  $A_1$  на кольцо  $A_2$  называется *изоморфным*, если оно сохраняется при операциях сложения и умножения, т. е. если  $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$  и  $\varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2)$ . Ясно, что если кольцо  $A_1$  есть область целостности или поле, то его изоморфный образ есть область целостности или поле.

## ГЛАВА II

---

### КОМПЛЕКСНЫЕ ЧИСЛА

Как известно, комплексными числами называются выражения вида  $a + bi$ , где  $a$  и  $b$  — вещественные числа,  $i$  — некоторый символ, удовлетворяющий соотношению  $i^2 = -1$ . Первые попытки введения в математику комплексных чисел были сделаны итальянскими математиками 16 в. Кардано и Бомбелли в связи с решением уравнений 3-й и 4-й степеней. Однако признание комплексных чисел как ценного орудия исследования происходило очень медленно. Недоверие вызывал сам символ  $i$  («мнимая единица»), заведомо не существующий среди вещественных чисел. Это недоверие усугублялось тем, что некритическое перенесение некоторых формул обычной алгебры на комплексные числа порождало неприятные парадоксы (например,  $i^2 = -1$ , но вместе с тем, используя формальное выражение  $i = \sqrt{-1}$  и обычные правила действий с квадратными корнями, получим  $i^2 = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1)^2} = \sqrt{1} = 1$ ). Лишь в 19 в. Гауссу удалось дать достаточно убедительное обоснование понятия комплексного числа. Построенная в 19 в. на основе комплексных чисел теория функций комплексного переменного обогатила математический анализ новыми результатами, придала значительной части математического анализа чрезвычайную стройность и простоту, а в дальнейшем оказалась могущественным средством исследования в важных разделах механики и физики. Таким образом, «невозможные», «мнимые» числа явились ценнейшим средством исследования, и тем самым их введение в науку оказалось оправданным не только их непротиворечивостью, но и практической важностью.

#### § 1. Обоснование комплексных чисел

**1. Наводящие соображения.** Задание комплексного числа  $a + bi$  вполне определяется заданием двух обыкновенных вещественных чисел  $a$  и  $b$ , называемых его *компонентами*.

Вводя комплексные числа, необходимо ввести и арифметические действия над ними, по возможности с сохранением обычных правил действий, но с обязательством заменять символ  $i^2$  на  $-1$ . Постараемся охарактеризовать правила этих действий в терминах компонент, без упоминания о «сомнительном» символе  $i$ . Так, если по обычным правилам элементарной алгебры «сложить» два комплексных числа  $a + bi$  и  $c + di$ , то мы получим комплексное число

$(a + c) + (b + d)i$ , и при этом компоненты суммы двух комплексных чисел будут равны суммам соответствующих компонент слагаемых.

Далее,  $(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$ , т. е. первая компонента произведения двух комплексных чисел равна разности произведений первых и вторых компонент, а вторая компонента равна сумме произведений первой компоненты одного из сомножителей на вторую компоненту другого.

Наконец, положив  $b = 0$  (и считая, что  $0i = 0$ ), получим  $a + 0i = a$ , т. е. комплексное число с нулевой второй компонентой отождествляется с вещественным числом, именно, с первой компонентой.

Разумеется, все эти соображения имеют лишь наводящий характер — мы сформулировали в терминах компонент правила действий над комплексными числами, как будто мы уже каким-то образом убедились в закономерности введения этих странных математических объектов. Но то, что нам это удалось сделать, естественно наводит на мысль дать само определение комплексных чисел и действий над ними в терминах компонент, т. е. вещественных чисел.

**2. Определение комплексных чисел.** *Комплексными числами* называются упорядоченные пары вещественных чисел (компонент), для которых понятия равенства, суммы, произведения и отождествления некоторых пар с вещественными числами вводятся согласно следующим определениям (аксиомам).

I. Пары  $(a, b)$  и  $(c, d)$  считаются *равными* в том и только в том случае, когда равны их соответствующие компоненты.

В символической записи:

$$(a, b) \stackrel{\text{def}}{=} (c, d) \Leftrightarrow \begin{cases} a = c, \\ b = d. \end{cases}$$

II. *Суммой* пар  $(a, b)$  и  $(c, d)$  называется пара  $(a + c, b + d)$ , т. е.

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d).$$

III. *Произведением* пар  $(a, b)$  и  $(c, d)$  называется пара  $(ac - bd, ad + bc)$ , т. е.

$$(a, b)(c, d) \stackrel{\text{def}}{=} (ac - bd, ad + bc).$$

IV. Пара  $(a, 0)$  отождествляется с вещественным числом  $a$ , т. е.  $(a, 0) \stackrel{\text{def}}{=} a$ .

Таким образом, в данном определении комплексных чисел, составными частями которого являются определения их равенства, суммы, произведения, нет речи о каком-либо извлечении квадрат-

ного корня из отрицательных чисел. Все определения формулируются в терминах вещественных чисел и действий над ними.

В первых трех аксиомах речь идет об определении разных понятий. Поэтому их сопоставление не может привести к каким-либо противоречиям. Единственное, чего можно опасаться, это нарушения обычных законов действий, которое априори могло бы произойти. Несколько в другом положении находится аксиома IV. Дело в том, что понятия равенства, суммы и произведения для вещественных чисел имеют определенный смысл, и если бы оказалось, что эти понятия расходятся с теми, которые возникают в силу аксиом I, II, III при рассмотрении вещественных чисел как пар специального вида, то это привело бы к такой путанице (пришлось бы отличать сумму вещественных чисел как таковых, от их суммы как пар, и т. д.), что следовало бы от аксиомы IV отказаться.

Поэтому прежде всего нужно сопоставить аксиому IV с аксиомами I, II, III.

I и IV. Пусть вещественные числа  $a$  и  $b$  равны, как отождествленные с ними пары  $(a, 0)$  и  $(b, 0)$ . Это будет, согласно аксиоме I, в том и только в том случае, когда  $a = b$ , т. е. если они равны в обычном смысле.

II и IV. Сумма вещественных чисел  $a$  и  $b$ , рассматриваемых как пары  $(a, 0)$  и  $(b, 0)$ , равна, согласно аксиоме II, паре  $(a + b, 0)$ , отождествленной с числом  $a + b$ , т. е. с суммой  $a$  и  $b$  в обычном смысле.

III и IV. Произведение вещественных чисел  $a$  и  $b$ , рассматриваемых как пары  $(a, 0)$  и  $(b, 0)$ , равно согласно аксиоме III паре  $(ab - 0 \cdot 0, a0 + 0b) = (ab, 0)$ , отождествленной с числом  $ab$ , т. е. с произведением  $a$  и  $b$  в обычном смысле. Таким образом, аксиома IV хорошо согласована с аксиомами I, II, III и не приводит к путанице, которой можно было бы опасаться.

Обратим внимание еще на одну формулу, непосредственно вытекающую из аксиом III, IV, именно,

$$m(a, b) = (ma, mb),$$

если  $m$  — какое угодно вещественное число. Действительно,  $m(a, b) = (m, 0)(a, b) = (ma - 0b, mb + 0a) = (ma, mb)$ . Допустим теперь, что  $m$  — натуральное число. В силу аксиомы II  $(a, b) + (a, b) = (2a, 2b)$ ,  $(2a, 2b) + (a, b) = (3a, 3b)$  и т. д., так что  $(ma, mb)$  есть результат последовательного сложения  $m$  слагаемых, равных  $(a, b)$ , что хорошо согласуется с привычным представлением о том, что умножение на натуральное число  $m$  равносильно сложению  $m$  равных слагаемых. Это еще раз свидетельствует о хорошем согласовании аксиом.

**3. Свойства действий.** Теперь нам нужно проверить, что аксиомы II и III согласованы в себе и друг с другом так, что привычные нам свойства действий над числами сохраняются при пе-

реходе к комплексным числам. Именно, мы установим, что комплексные числа образуют поле. При описании свойств действий мы будем придерживаться принятой в § 3 гл. I нумерации аксиом кольца и поля, но при проверке будем несколько отступать от последовательности, предписываемой этой нумерацией.

2.  $(a, b) + (c, d) = (c, d) + (a, b)$  (коммутативность сложения). Действительно, левая часть равна  $(a + c, b + d)$ , правая равна  $(c + a, d + b)$ . Они равны в силу коммутативности сложения вещественных чисел.

1.  $((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f))$  (ассоциативность сложения). Действительно, в силу ассоциативности сложения вещественных чисел правая и левая части равны  $(a + c + e, b + d + f)$ .

3.  $(a, b) + (0, 0) = (a, b)$ , так что пара  $(0, 0)$  (отождествляемая с вещественным числом 0) играет роль нуля и при сложении пар.

4.  $(a, b) + (-a, -b) = (0, 0)$ . Поэтому для каждой пары  $(a, b)$  существует противоположная, именно,  $(-a, -b)$ .

7.  $(a, b)(c, d) = (c, d)(a, b)$  (коммутативность умножения). Действительно, левая часть равна  $(ac - bd, ad + bc)$ , правая равна  $(ca - db, da + cb)$ . Они равны.

5.  $((a, b) + (c, d))(e, f) = (a, b)(e, f) + (c, d)(e, f)$ ;

5'.  $(e, f)((a, b) + (c, d)) = (e, f)(a, b) + (e, f)(c, d)$

(левая и правая дистрибутивность).

В силу коммутативности умножения достаточно проверить первую из формул 5. Левая часть равна

$$(a + c, b + d)(e, f) = ((a + c)e - (b + d)f, (a + c)f + (b + d)e) = \\ = (ae + ce - bf - df, af + cf + be + de).$$

Правая часть равна

$$(ae - bf, af + be) + (ce - df, cf + de) = \\ = (ae - bf + ce - df, af + be + cf + de),$$

т. е. равна левой части.

6.  $((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$  (ассоциативность умножения). Действительно, левая часть равна

$$(ac - bd, ad + bc)(e, f) = ((ac - bd)e - (ad + bc)f, (ac - bd)f + \\ + (ad + bc)e) = (ace - bde - adf - bcf, acf - bdf + ade + bce).$$

Правая часть равна

$$(a, b)(ce - df, cf + de) = (a(ce - df) - b(cf + de), b(ce - df) + \\ + a(cf + de)) = (ace - adf - bcf - bde, bce - bdf + acf + ade),$$

т. е. правая часть равна левой.

8.  $(a, b)(1, 0) = (a, b)$ .

Таким образом, пара  $(1, 0)$  (отождествляемая с вещественным числом 1) играет роль 1 и при умножении пар.

Итак, комплексные числа составляют коммутативное ассоциативное кольцо с единицей.

Введем теперь понятие сопряженных комплексных чисел. Пары  $(a, b)$  и  $(a, -b)$ , отличающиеся знаком второй компоненты, называются *сопряженными*. Умножив сопряженные пары

$$(a, b)(a, -b) = (aa - b(-b), a(-b) + ba) = (a^2 + b^2, 0) = a^2 + b^2,$$

получим, что их произведение равно неотрицательному числу  $a^2 + b^2$ , которое равно нулю только если  $a = 0$ ,  $b = 0$ , т. е. если  $(a, b) = 0$ . Если  $(a, b) \neq 0$ , то, умножив сопряженную пару  $(a, -b)$  на вещественное число  $\frac{1}{a^2 + b^2}$ , мы получим обратную к паре  $(a, b)$  пару, т. е. такую, которая при умножении на  $(a, b)$  дает число 1. Таким образом, верно:

9. Для любой пары  $(a, b)$ , отличной от 0, существует обратная  $(a, b)^{-1}$ , именно,  $\frac{1}{a^2 + b^2}(a, -b) = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right)$ .

Итак, мы доказали, что комплексные числа составляют поле.

4. **Возвращение к обычной форме записи.** Ясно, что  $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$ , где буквой  $i$  обозначена пара  $(0, 1)$ . Из аксиомы III следует, что

$$i^2 = (0, 1)(0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -1.$$

Таким образом, мы вернулись к обычной записи комплексного числа в виде  $a + bi$ , но «мнимая» единица  $i$  получила реальное истолкование как одна из пар, действия над которыми определены аксиомами I, II, III, IV, именно, пара  $(0, 1)$ . Если угодно, множитель  $i$  при вещественном числе  $b$  можно истолковать как указание на то, что  $b$  является второй компонентой пары  $(a, b)$ .

Первая компонента комплексного числа  $\alpha = a + bi$  называется *вещественной частью* этого числа и обозначается  $\text{Re } \alpha$ , а вторая компонента называется его *мнимой частью* и обозначается  $\text{Im } \alpha$ . Подчеркнем, что мнимая часть (так же, как и вещественная часть) комплексного числа есть число вещественное.

В дальнейшем, говоря о комплексных числах, мы должны помнить, что вещественные числа мы рассматриваем как частный случай комплексных (с нулевой второй компонентой), так что фраза « $\alpha$  есть комплексное число» отнюдь не исключает того, что  $\alpha$  может быть и вещественным.

5. **Вычитание и деление комплексных чисел.** Действия вычитания и деления определяются как действия, обратные к действиям сложения и умножения, т. е. вычитание — как действие, восстанавливающее одно из слагаемых по данной сумме и второму слагаемому, а деление — как отыскание одного из сомножителей по данному произведению и второму сомножителю. Их возможность и единственность обосновывается следующими предложениями.

**Предложение 1.** Пусть  $\alpha$  и  $\beta$  — данные комплексные числа. Тогда существует одно и только одно комплексное число  $x$  такое, что  $\alpha + x = \beta$ , именно,  $x = (-\alpha) + \beta$ .

**Доказательство.** Имеем  $\alpha + ((-\alpha) + \beta) = \alpha + (-\alpha) + \beta = \beta$ , так что  $x = (-\alpha) + \beta$  удовлетворяет поставленному требованию. Обратное, если  $\alpha + x = \beta$ , то  $(-\alpha) + \alpha + x = (-\alpha) + \beta$ , откуда  $x = (-\alpha) + \beta$ , так что всякое число, отличное от  $(-\alpha) + \beta$ , не удовлетворяет поставленному требованию. Число  $(-\alpha) + \beta$  есть, таким образом, разность чисел  $\beta$  и  $\alpha$ . Она обозначается обычным образом:  $\beta - \alpha$ .

**Предложение 2.** Пусть  $\alpha$  и  $\beta$  — данные комплексные числа, причем  $\alpha \neq 0$ . Тогда существует одно и только одно комплексное число  $x$  такое, что  $\alpha x = \beta$ , именно,  $x = \alpha^{-1}\beta$ .

**Доказательство.** Если  $x = \alpha^{-1}\beta$ , то  $\alpha x = \alpha \alpha^{-1}\beta = \beta$ . Если  $\alpha x = \beta$ , то  $\alpha^{-1}\alpha x = \alpha^{-1}\beta$ ,  $x = \alpha^{-1}\beta$ , что и требовалось доказать.

Число  $\alpha^{-1}\beta$  есть, таким образом, частное от деления  $\beta$  на  $\alpha$ . Частное обычно записывается в форме дроби  $\frac{\beta}{\alpha}$ . Ясно, что если

$\gamma \alpha x = \beta$ , то при любом  $\gamma \neq 0$  будет  $\gamma \alpha x = \gamma \beta$ , откуда  $x = \frac{\gamma \beta}{\gamma \alpha}$ , таким образом, числитель и знаменатель дроби можно умножать на одно и то же число, отличное от 0.

Удобно фактически вычислять частное  $\frac{\beta}{\alpha}$ , умножая числитель и знаменатель на число, сопряженное со знаменателем:  $\frac{\beta}{\alpha} = \frac{\beta \bar{\alpha}}{\alpha \bar{\alpha}}$ , так как  $\alpha \bar{\alpha}$  есть вещественное число. Например,

$$\frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = \frac{4+2i}{2} = 2+i.$$

Конечно, этот способ равносителен представлению числа  $\alpha^{-1}$  в виде  $\frac{1}{\alpha \bar{\alpha}} \bar{\alpha}$ , указанном выше для  $\alpha = a + bi$ .

## § 2. Тригонометрическая форма комплексного числа

**1. Геометрическое изображение.** Комплексное число  $\alpha = a + bi$  естественно изобразить точкой на плоскости, приняв числа  $a$  и  $b$  за координаты точки, изображающей число  $\alpha$ . При этом каждому комплексному числу соответствует точка и каждой точке плоскости соответствует некоторое комплексное число. Вещественные числа изображаются точками с равными нулю ординатами, т. е. точками, лежащими на оси абсцисс. На оси ординат располагаются изображения «чисто мнимых» чисел  $bi$ . Началу координат соответствует число 0.

Плоскость, на которой изображаются комплексные числа, называется *плоскостью комплексной переменной*. Ее ось абсцисс называется *вещественной осью*, ось ординат — *мнимой осью* в соот-

ветствии с наименованиями чисел, изображения которых лежат на этих осях.

Наряду с изображением комплексных чисел точками на плоскости удобно с каждым комплексным числом связывать вектор, исходящий из начала координат в точку, изображающую это число (т. е. радиус-вектор этой точки). Компоненты  $a$  и  $b$  комплексного числа  $a + bi$  являются, очевидно, проекциями (алгебраическими, с учетом знаков) этого вектора на оси координат. Как известно, проекция суммы векторов (в смысле векторного сложения)

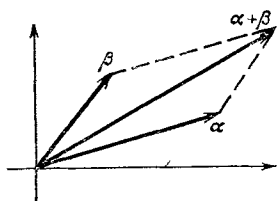


Рис. 1.

на любую ось равна сумме проекций слагаемых. Поэтому сумма векторов, изображающих комплексные числа  $\alpha$  и  $\beta$ , есть вектор, изображающий сумму  $\alpha + \beta$  этих чисел, так как компоненты числа  $\alpha + \beta$  равны суммам соответствующих компонент слагаемых (рис. 1).

**2. Модуль и аргумент комплексного числа.** Введем в рассмотрение полярные координаты точки, изображающей комплексное

число  $\alpha$ , принимая начало координат за полюс и вещественную ось за полярную ось (рис. 2). Как известно, полярными координатами точки являются длина ее радиус-вектора, равная расстоянию от точки до полюса, и величина ее полярного угла, образованного положительным направлением полярной оси и радиус-вектором рассматриваемой точки. Длина радиус-вектора точки, изображающей комплексное число  $\alpha$ , называется *модулем* этого числа и обозначается  $|\alpha|$ . Ясно, что  $|\alpha| \geq 0$ , причем  $|\alpha| = 0$  только, если  $\alpha = 0$ . Величина полярного угла точки, изображающей комплексное число  $\alpha$ , называется *аргументом* этого числа и обозначается  $\arg \alpha$ . Заметим, что  $\arg \alpha$  имеет смысл лишь при  $\alpha \neq 0$ , аргумент числа 0 смысла не имеет.

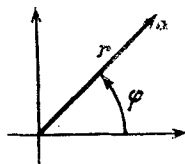


Рис. 2.

Положительным направлением отсчета аргумента комплексного числа считается направление от положительной полуоси вещественной оси к положительной полуоси мнимой оси, т. е. против часовой стрелки при обычном расположении осей.

Аргумент комплексного числа определен не однозначно, так как угол между двумя направлениями (даже если выбрано положительное направление отсчета) можно отсчитывать многими способами. Уточним характер многозначности аргумента. Пусть  $\varphi_0$  — наименьшее значение аргумента, отсчитанное в положительном направлении. Сделав при отсчете несколько полных оборотов в положительном направлении, мы придем к значению аргумента  $\varphi_0 + k \cdot 2\pi$ , где  $k$  — число полных оборотов, т. е. целое неотрицательное число. Простейший отсчет в отрицательном направлении дает,

очевидно, значение аргумента  $-(2\pi - \varphi_0) = \varphi_0 - 2\pi$  (рис. 3). Если же сделать еще  $s$  полных оборотов в отрицательном направлении, мы придем к значению  $\varphi_0 - (s+1)2\pi$ ,  $s \geq 0$ . Тем самым все возможные значения аргумента даются формулой:  $\varphi = \varphi_0 + 2k\pi$ , где  $k$  — любое целое число, положительное, отрицательное или 0. Таким образом, данному комплексному числу, не равному 0, можно соотнести в качестве аргумента бесконечное множество чисел, правда, очень просто связанных между собой, именно, любые два значения аргумента отличаются на целое кратное  $2\pi$ .

Разумеется, многозначности аргумента можно было бы избежать, наложив на аргумент какие-либо требования, выделяющие одно значение из всех возможных, например,  $0 \leq \varphi < 2\pi$  или  $-\pi < \varphi \leq \pi$ . Однако это оказывается неудобным, особенно при изучении функций от комплексной переменной. Пусть, например, комплексное число  $x + yi$  изменяется так, что его изображение описывает в положительном направлении окружность с центром в начале координат, начиная, например, с точки  $i$  и возвращаясь в ту же точку (рис. 4). Если бы мы наложили ограничения на аргумент:  $0 \leq \varphi < 2\pi$ , нам пришлось бы считать, что при подходе к точке 1 аргумент скачком переходит от значений, сколь угодно близких к  $2\pi$ , к значению 0, и это неестественно. Естественнее считать, что аргумент изменяется непрерывно, но когда  $x + yi$  возвращается в исходную точку, его аргумент получает приращение, равное  $2\pi$ .

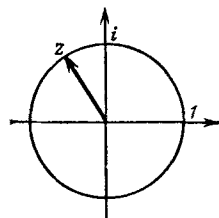


Рис. 4.

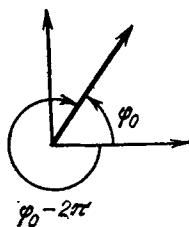


Рис. 3.

Впредь, говоря об аргументе комплексного числа, мы будем подразумевать какое-либо его значение, безразлично какое. Если же возникает необходимость выбирать определенное значение, это приходится делать при помощи надлежащего описания (например, «возьмем наименьшее неотрицательное значение аргумента»).

**3. Тригонометрическая запись комплексного числа.** Модуль  $r = |\alpha|$  и аргумент  $\varphi = \arg \alpha$  комплексного числа  $\alpha = a + bi$  связаны с его компонентами при помощи формул

$$a = r \cos \varphi, \quad b = r \sin \varphi.$$

Эти формулы непосредственно следуют из определения функций  $\cos$  и  $\sin$  любого угла. Ясно, что  $r = \sqrt{a^2 + b^2}$ ,  $\cos \varphi = \frac{a}{r}$ ,  $\sin \varphi = \frac{b}{r}$ . Эти формулы определяют модуль и аргумент по данным  $a$  и  $b$ . Для определения аргумента можно пользоваться формулой  $\operatorname{tg} \varphi = \frac{b}{a}$  при  $a \neq 0$ . Однако эта формула задает  $\varphi$  лишь с точно-

стью до целого кратного  $\pi$  (т. е. полуоборота), а не до целого кратного  $2\pi$ . Это заставляет дополнительно выбирать из двух значений  $\varphi$  в противоположных четвертях одно, по знаку  $\cos \varphi$  (или  $\sin \varphi$ ), совпадающему со знаком  $a$  (соответственно  $b$ ).

Подставляя вместо компонент комплексного числа  $\alpha = a + bi$  их выражения через модуль и аргумент, получаем

$$\alpha = r(\cos \varphi + i \sin \varphi).$$

Такая форма записи комплексного числа называется *тригонометрической*.

Примеры:

$$1 = 1(\cos 0 + i \sin 0),$$

$$-1 = 1(\cos \pi + i \sin \pi),$$

$$i = 1\left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}\right),$$

$$1 - i = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i \sin\left(-\frac{\pi}{4}\right)\right),$$

$$3 + 4i = 5(\cos \varphi + i \sin \varphi),$$

где  $\varphi$  — угол первой четверти, косинус которого равен  $\frac{3}{5}$ .

**4. Неравенства для модуля суммы и модуля разности двух комплексных чисел.** Имеют место следующие неравенства:

$$a) \quad |\alpha + \beta| \leq |\alpha| + |\beta|,$$

$$b) \quad |\alpha - \beta| \leq |\alpha| + |\beta|,$$

$$c) \quad |\alpha + \beta| \geq |\alpha| - |\beta|,$$

$$d) \quad |\alpha - \beta| \geq |\alpha| - |\beta|.$$

Эти неравенства удобны для оценивания модуля суммы и модуля разности комплексных чисел, т. е. для указания границ их изменения, если известны границы для модулей слагаемых. Неравенства а) и б) применяются для оценивания сверху, неравенства с) и d) дают оценки снизу.

Докажем прежде всего неравенство а).

Пусть  $\alpha = r_1(\cos \varphi_1 + i \sin \varphi_1)$ ,  $\beta = r_2(\cos \varphi_2 + i \sin \varphi_2)$  (здесь  $r_1 = |\alpha|$ ,  $r_2 = |\beta|$ ). Тогда  $\alpha + \beta = r_1 \cos \varphi_1 + r_2 \cos \varphi_2 + i(r_1 \sin \varphi_1 + r_2 \sin \varphi_2)$ , откуда

$$\begin{aligned} |\alpha + \beta|^2 &= (r_1 \cos \varphi_1 + r_2 \cos \varphi_2)^2 + (r_1 \sin \varphi_1 + r_2 \sin \varphi_2)^2 = \\ &= r_1^2 \cos^2 \varphi_1 + 2r_1 r_2 \cos \varphi_1 \cos \varphi_2 + r_2^2 \cos^2 \varphi_2 + r_1^2 \sin^2 \varphi_1 + \\ &\quad + 2r_1 r_2 \sin \varphi_1 \sin \varphi_2 + r_2^2 \sin^2 \varphi_2 = r_1^2 (\cos^2 \varphi_1 + \sin^2 \varphi_1) + \\ &\quad + 2r_1 r_2 (\cos \varphi_1 \cos \varphi_2 + \sin \varphi_1 \sin \varphi_2) + r_2^2 (\cos^2 \varphi_2 + \sin^2 \varphi_2) = \\ &= r_1^2 + 2r_1 r_2 \cos(\varphi_1 - \varphi_2) + r_2^2. \end{aligned}$$

Но  $\cos(\varphi_1 - \varphi_2) \leq 1$ . Поэтому  $|\alpha + \beta|^2 \leq r_1^2 + 2r_1r_2 + r_2^2 = (r_1 + r_2)^2$ , откуда в силу положительности  $|\alpha + \beta|$  и  $r_1 + r_2$  заключаем, что  $|\alpha + \beta| \leq r_1 + r_2 = |\alpha| + |\beta|$ , что и требовалось доказать.

Для доказательства неравенства б) заметим прежде всего, что  $|\beta| = |-\beta|$ . Действительно, компоненты чисел  $\beta$  и  $-\beta$  отличаются только знаками, и суммы квадратов компонент одинаковы. Далее,  $|\alpha - \beta| = |\alpha + (-\beta)| \leq |\alpha| + |-\beta| = |\alpha| + |\beta|$ , что и требовалось доказать.

Для доказательства неравенства с) применим неравенство б) к  $\alpha = (\alpha + \beta) - \beta$ . Получим:  $|\alpha| \leq |\alpha + \beta| + |\beta|$ , откуда  $|\alpha + \beta| \geq |\alpha| - |\beta|$ .

Наконец,  $|\alpha - \beta| = |\alpha + (-\beta)| \geq |\alpha| - |\beta|$ , чем доказано неравенство д).

Все доказанные неравенства имеют ясное геометрическое истолкование (рис. 5). Если точки, изображающие  $0$ ,  $\alpha$ ,  $\beta$ , не лежат на одной прямой, то треугольник с вершинами  $0$ ,  $\alpha$ ,  $\alpha + \beta$  имеет длины сторон  $|\alpha|$ ,  $|\beta|$  и  $|\alpha + \beta|$ . Из известных «неравенств треугольника» — сторона треугольника меньше суммы двух других сторон и больше их разности — получаем неравенства а) и б) (даже без включения равенства, что обеспечивается сделанным предположением о невырожденности треугольника  $0$ ,  $\alpha$ ,  $\alpha + \beta$ ). Неравенства с) и д) становятся очевидными при взгляде на треугольник с вершинами в точках  $0$ ,  $\alpha$ ,  $\beta$ . Длины двух его сторон равны  $|\alpha|$  и  $|\beta|$ , длина третьей стороны равна длине радиус-вектора точки  $\alpha - \beta$ , т. е. равна  $|\alpha - \beta|$ . Применение неравенства треугольника приводит к неравенствам с) и д), снова без знаков равенства, которые могут появиться в случае вырождения треугольника в отрезок. При доказательстве неравенств с) и д) мы отметили одно обстоятельство, интересное само по себе: модуль разности двух комплексных чисел равен расстоянию между точками, изображающими эти комплексные числа.

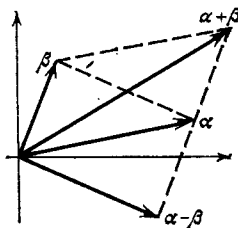


Рис. 5.

Неравенства с) и д) иногда полезны в слегка усиленной формулировке

$$с') \quad |\alpha + \beta| \geq ||\alpha| - |\beta||,$$

$$д') \quad |\alpha - \beta| \geq ||\alpha| - |\beta||.$$

Их справедливость почти очевидна. Действительно,  $|\alpha + \beta| \geq ||\alpha| - |\beta||$  и  $|\alpha + \beta| \geq |\beta| - |\alpha|$ . Правые части отличаются знаком и, выбрав из них положительную, придем к неравенству с'). Неравенство д') следует из с') после замены  $\beta$  на  $-\beta$ .

Неравенство а) очевидным образом обобщается на сумму нескольких слагаемых:  $|\alpha_1 + \alpha_2 + \dots + \alpha_k| \leq |\alpha_1| + |\alpha_2| + \dots + |\alpha_k|$ .

Из неравенства б) и обобщенного неравенства а) следует

$$|\alpha_1 + \alpha_2 + \dots + \alpha_k| \geq |\alpha_1| - |\alpha_2 + \dots + \alpha_k| \geq \geq |\alpha_1| - |\alpha_2| - \dots - |\alpha_k|.$$

Это неравенство можно рассматривать как обобщение неравенства б). Оно удобно для оценивания снизу суммы, в которой модуль одного слагаемого больше суммы модулей остальных.

### 5. Умножение комплексных чисел в тригонометрической записи.

Пусть  $\alpha_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$  и  $\alpha_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$ . Тогда  $\alpha_1 \alpha_2 = r_1 r_2 (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 + i (\sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2)) = r_1 r_2 (\cos (\varphi_1 + \varphi_2) + i \sin (\varphi_1 + \varphi_2))$ .

Таким образом,  $\alpha_1 \alpha_2$  легко преобразуется к тригонометрической записи числа, модуль которого равен  $r_1 r_2$  и аргумент равен  $\varphi_1 + \varphi_2$ . Следовательно, модуль произведения двух комплексных чисел равен произведению модулей сомножителей и аргумент произведения (точнее, одно из значений аргумента) равен сумме аргументов сомножителей. В буквенной записи

$$|\alpha_1 \alpha_2| = |\alpha_1| \cdot |\alpha_2|, \quad \arg(\alpha_1 \alpha_2) = \arg \alpha_1 + \arg \alpha_2.$$

Эти правила распространяются на произведение любого числа сомножителей. Именно,

$$|\alpha_1 \alpha_2 \dots \alpha_k| = |\alpha_1| \cdot |\alpha_2| \dots |\alpha_k|,$$

$$\arg(\alpha_1 \alpha_2 \dots \alpha_k) = \arg \alpha_1 + \arg \alpha_2 + \dots + \arg \alpha_k.$$

Действительно, эти формулы верны для  $k = 2$ . Допустив, что они верны для произведения из  $k - 1$  сомножителей, мы получим

$$|\alpha_1 \alpha_2 \dots \alpha_k| = |\alpha_1| \cdot |\alpha_2 \dots \alpha_k| = |\alpha_1| \cdot |\alpha_2| \dots |\alpha_k|,$$

$$\arg(\alpha_1 \alpha_2 \dots \alpha_k) =$$

$$= \arg \alpha_1 + \arg(\alpha_2 \dots \alpha_k) = \arg \alpha_1 + \arg \alpha_2 + \dots + \arg \alpha_k.$$

В обеих цепочках равенств последний переход обеспечивается индуктивным предположением.

### 6. Возведение комплексного числа в степень с целым показателем и формула Муавра. Положим в формуле

$$r_1(\cos \varphi_1 + i \sin \varphi_1) r_2(\cos \varphi_2 + i \sin \varphi_2) \dots r_k(\cos \varphi_k + i \sin \varphi_k) = r_1 r_2 \dots r_k (\cos (\varphi_1 + \varphi_2 + \dots + \varphi_k) + i \sin (\varphi_1 + \varphi_2 + \dots + \varphi_k)),$$

что все сомножители равны, так что  $r_1 = r_2 = \dots = r_k = r$ ,  $\varphi_1 = \varphi_2 = \dots = \varphi_k = \varphi$ . Получим

$$(r(\cos \varphi + i \sin \varphi))^k = r^k (\cos k\varphi + i \sin k\varphi).$$

При  $r = 1$  получается знаменитая формула Муавра:

$$(\cos \varphi + i \sin \varphi)^k = \cos k\varphi + i \sin k\varphi.$$

Мы вывели эту формулу в предположении, что  $k$  — целое положительное число. Покажем, что она остается верной и при  $k = 0$  и при целом отрицательном  $k$ , считая для комплексных чисел, так же как для вещественных,  $\alpha^0 = 1$  и  $\alpha^{-m} = \frac{1}{\alpha^m}$ . При  $k = 0$  формула превращается в верное равенство:

$$(\cos \varphi + i \sin \varphi)^0 = \cos 0 + i \sin 0 = 1.$$

Положим теперь  $k = -m$ , считая  $m$  целым положительным. Тогда

$$\begin{aligned} (\cos \varphi + i \sin \varphi)^k &= (\cos \varphi + i \sin \varphi)^{-m} = \frac{1}{(\cos \varphi + i \sin \varphi)^m} = \\ &= \frac{1}{\cos m\varphi + i \sin m\varphi} = \frac{\cos m\varphi - i \sin m\varphi}{\cos^2 m\varphi + \sin^2 m\varphi} = \cos(-m)\varphi + i \sin(-m)\varphi = \\ &= \cos k\varphi + i \sin k\varphi. \end{aligned}$$

Таким образом, формула Муавра оказывается верной при всех целых значениях  $k$ .

**7. Применения формулы Муавра к преобразованиям тригонометрических выражений.** Формула Муавра оказывается удобным средством для преобразования некоторых выражений, содержащих тригонометрические функции. Рассмотрим несколько примеров.

**Пример 1.** Выразить  $\operatorname{tg} 5\varphi$  через  $\operatorname{tg} \varphi$ .

Имеем соотношение  $\cos 5\varphi + i \sin 5\varphi = (\cos \varphi + i \sin \varphi)^5$ . Приравняв бином Ньютона, получим

$$\begin{aligned} \cos 5\varphi + i \sin 5\varphi &= \cos^5 \varphi + 5i \cos^4 \varphi \sin \varphi - 10 \cos^3 \varphi \sin^2 \varphi - \\ &\quad - 10i \cos^2 \varphi \sin^3 \varphi + 5 \cos \varphi \sin^4 \varphi + i \sin^5 \varphi \end{aligned}$$

(пользуемся тем, что  $i^2 = -1$ ,  $i^3 = -i$ ,  $i^4 = 1$ ,  $i^5 = i$ ). Приравнявая компоненты, получим

$$\begin{aligned} \cos 5\varphi &= \cos^5 \varphi - 10 \cos^3 \varphi \sin^2 \varphi + 5 \cos \varphi \sin^4 \varphi, \\ \sin 5\varphi &= 5 \cos^4 \varphi \sin \varphi - 10 \cos^2 \varphi \sin^3 \varphi + \sin^5 \varphi, \end{aligned}$$

откуда

$$\operatorname{tg} 5\varphi = \frac{5 \cos^4 \varphi \sin \varphi - 10 \cos^2 \varphi \sin^3 \varphi + \sin^5 \varphi}{\cos^5 \varphi - 10 \cos^3 \varphi \sin^2 \varphi + 5 \cos \varphi \sin^4 \varphi} = \frac{5 \operatorname{tg} \varphi - 10 \operatorname{tg}^3 \varphi + \operatorname{tg}^5 \varphi}{1 - 10 \operatorname{tg}^2 \varphi + 5 \operatorname{tg}^4 \varphi}.$$

(Мы поделили числитель и знаменатель на  $\cos^5 \varphi$ .)

Ясно, что подобным образом можно выражать тригонометрические функции кратного аргумента через тригонометрические функции исходного.

**Пример 2.** Выразить  $\sin^5 \varphi$  линейно через тригонометрические функции кратных аргументов.

Положим  $\alpha = \cos \varphi + i \sin \varphi$ , тогда  $\alpha^{-1} = \cos \varphi - i \sin \varphi$ ,  $\alpha^k = \cos k\varphi + i \sin k\varphi$ ,  $\alpha^{-k} = \cos k\varphi - i \sin k\varphi$ , откуда

$$\cos \varphi = \frac{\alpha + \alpha^{-1}}{2}, \quad \sin \varphi = \frac{\alpha - \alpha^{-1}}{2i}, \quad \cos k\varphi = \frac{\alpha^k + \alpha^{-k}}{2}, \quad \sin k\varphi = \frac{\alpha^k - \alpha^{-k}}{2i}.$$

Воспользуемся этими формулами:

$$\begin{aligned}\sin^5 \varphi &= \left( \frac{\alpha - \alpha^{-1}}{2i} \right)^5 = \frac{\alpha^5 - 5\alpha^3 + 10\alpha - 10\alpha^{-1} + 5\alpha^{-3} - \alpha^{-5}}{32i} = \\ &= \frac{(\alpha^5 - \alpha^{-5}) - 5(\alpha^3 - \alpha^{-3}) + 10(\alpha - \alpha^{-1})}{32i} = \\ &= \frac{2i \sin 5\varphi - 10i \sin 3\varphi + 20i \sin \varphi}{32i} = \frac{\sin 5\varphi - 5 \sin 3\varphi + 10 \sin \varphi}{16}.\end{aligned}$$

Аналогично, любое выражение вида  $\cos^k \varphi \sin^m \varphi$  можно представить линейно через тригонометрические функции кратных аргументов.

**Пример 3.** Преобразовать сумму  $B = \sin \varphi + \sin 2\varphi + \dots + \sin n\varphi$ .

Введем в рассмотрение другую сумму  $A = \cos \varphi + \cos 2\varphi + \dots + \cos n\varphi$  и запишем  $A + Bi = (\cos \varphi + i \sin \varphi) + (\cos 2\varphi + i \sin 2\varphi) + \dots + (\cos n\varphi + i \sin n\varphi)$ . Мы пришли к сумме геометрической прогрессии. Для дальнейших преобразований полезно ввести обозначение  $\alpha = \cos \frac{\varphi}{2} + i \sin \frac{\varphi}{2}$ . Тогда

$$A + Bi = \alpha^2 + \alpha^4 + \dots + \alpha^{2n} = \frac{\alpha^{2n+2} - \alpha^2}{\alpha^2 - 1}.$$

Вынесем теперь в числителе и знаменателе такие степени  $\alpha$ , чтобы в скобках оставались разности степеней с противоположными показателями (для возможности этого мы ввели сокращенное обозначение для  $\cos \frac{\varphi}{2} + i \sin \frac{\varphi}{2}$ , а не для  $\cos \varphi + i \sin \varphi$ , что, казалось бы, естественнее):

$$\begin{aligned}A + Bi &= \frac{\alpha^{n+2}(\alpha^n - \alpha^{-n})}{\alpha(\alpha - \alpha^{-1})} = \frac{\alpha^{n+1}(\alpha^n - \alpha^{-n})}{\alpha - \alpha^{-1}} = \\ &= \frac{\left( \cos \frac{n+1}{2} \varphi + i \sin \frac{n+1}{2} \varphi \right) 2i \sin \frac{n\varphi}{2}}{2i \sin \frac{\varphi}{2}} = \\ &= \frac{\sin \frac{n\varphi}{2}}{\sin \frac{\varphi}{2}} \left( \cos \frac{n+1}{2} \varphi + i \sin \frac{n+1}{2} \varphi \right),\end{aligned}$$

откуда

$$B = \frac{\sin \frac{n\varphi}{2} \sin \frac{(n+1)\varphi}{2}}{\sin \frac{\varphi}{2}}.$$

В качестве «бесплатного приложения» мы получили сумму

$$A = \frac{\sin \frac{n\varphi}{2} \cos \frac{(n+1)\varphi}{2}}{\sin \frac{\varphi}{2}}.$$

Аналогичным образом могут быть преобразованы суммы вида  $a_1 \cos b_1 + a_2 \cos b_2 + \dots + a_n \cos b_n$  и  $a_1 \sin b_1 + a_2 \sin b_2 + \dots + a_n \sin b_n$ , если аргументы  $b_1, b_2, \dots, b_n$  тригонометрических функций образуют арифметическую прогрессию, а коэффициенты  $a_1, a_2, \dots, a_n$  — геометрическую. Разумеется, рассмотренные примеры не исчерпывают возможности применений формулы Муавра к преобразованиям тригонометрических выражений.

### § 3. Извлечение корня из комплексного числа

**1. Вывод формулы извлечения корня.** Пусть  $n$  — натуральное число. Извлечь корень с показателем  $n$  из комплексного числа  $\alpha$  — это значит найти комплексное число (или числа)  $\beta$  так, что  $\beta^n = \alpha$ . Каждое число  $\beta$  такое, что  $\beta^n = \alpha$ , называется *корнем  $n$ -й степени* из  $\alpha$  и обозначается  $\sqrt[n]{\alpha}$ .

Ясно, что если  $\alpha = 0$ , то единственным значением  $\sqrt[n]{\alpha}$  является число 0, поэтому сосредоточим внимание на случае  $\alpha \neq 0$ . Запишем  $\alpha$  в тригонометрической форме  $\alpha = r(\cos \varphi + i \sin \varphi)$  и будем искать  $\beta$  тоже в тригонометрической записи:

$$\beta = R(\cos \theta + i \sin \theta).$$

Равенство  $\beta^n = \alpha$  запишется в виде

$$R^n(\cos n\theta + i \sin n\theta) = r(\cos \varphi + i \sin \varphi).$$

Приравнявая модули и аргументы (с учетом многозначности), получим, что последнее равенство равносильно равенствам:

$$R^n = r,$$

$$n\theta = \varphi + 2k\pi, \quad k \in \mathbb{Z}.$$

Данное число  $r$  положительно (ибо  $\alpha \neq 0$ ) и искомое число  $R$  должно быть тоже положительным. Известно, что для любого положительного числа существует единственное положительное значение корня  $n$ -й степени, называемое арифметическим значением корня, и это значение принято записывать в виде степени с дробным показателем. Итак,  $R = r^{1/n}$ . Аргумент же  $\theta$  находится просто делением:

$$\theta = \frac{\varphi + 2k\pi}{n}.$$

Таким образом, корни  $n$ -й степени из комплексного числа  $\alpha$  существуют, и все они даются формулой

$$\beta_k = r^{1/n} \left( \cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right) \quad (1)$$

при любом  $k \in \mathbb{Z}$  (мы ставим индекс  $k$  при  $\beta$  для того, чтобы подчеркнуть многозначность  $\sqrt[n]{\alpha}$  и зависимость его значений от параметра  $k$ , могущего принимать все целые значения).

## 2. Исследование формулы извлечения корня.

**Теорема 1.** *Существует ровно  $n$  значений корня  $n$ -й степени из отличного от нуля комплексного числа  $\alpha = r(\cos \varphi + i \sin \varphi)$ . Их дает формула*

$$\sqrt[n]{\alpha} = r^{1/n} \left( \cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right)$$

в предположении, что  $k$  пробегает какую-либо полную систему вычетов по модулю  $n$ , например,  $k = 0, 1, \dots, n-1$ .

**Доказательство.** Мы уже видели, что значения корня  $n$ -й степени из  $\alpha$  даются формулой (1). Покажем, что  $\beta_{k_1} = \beta_{k_2}$  в том и только в том случае, когда  $k_1 \equiv k_2 \pmod{n}$ . Действительно,

$$\beta_{k_1} = \beta_{k_2} \Leftrightarrow \frac{\varphi + 2k_1\pi}{n} = \frac{\varphi + 2k_2\pi}{n} + 2\pi t$$

при целом  $t$  (аргументы равных чисел равны или отличаются на целые кратные  $2\pi$ ; о модулях заботиться не нужно — они одинаковы у всех чисел  $\beta_k$ ). Это равенство, в свою очередь, равносильно  $\frac{k_1 - k_2}{n} = t$ , т. е.  $k_1 \equiv k_2 \pmod{n}$ . Итак, действительно,  $\beta_{k_1} = \beta_{k_2}$  в том и только в том случае, если  $k_1 \equiv k_2 \pmod{n}$ ; и, следовательно, мы получим все различные значения для  $\beta_k$ , если  $k$  пробегит значения по одному из каждого класса по модулю  $n$ , т. е. некоторую полную систему вычетов.

**Пример.** Найти  $\sqrt[3]{2+2i}$  (один из немногих «хорошо подташованных» численных примеров).

Имеем  $2+2i = \sqrt{8}(\cos 45^\circ + i \sin 45^\circ)$ . Согласно формуле

$$\begin{aligned} \sqrt[3]{2+2i} &= (\sqrt{8})^{1/3} \left( \cos \frac{45^\circ + k \cdot 360^\circ}{3} + i \sin \frac{45^\circ + k \cdot 360^\circ}{3} \right) = \\ &= \sqrt[3]{2} (\cos (15^\circ + k \cdot 120^\circ) + i \sin (15^\circ + k \cdot 120^\circ)). \end{aligned}$$

Для  $k$  достаточно взять значения 0, 1, 2. Получим три значения:

$$\beta_0 = \sqrt[3]{2} (\cos 15^\circ + i \sin 15^\circ),$$

$$\beta_1 = \sqrt[3]{2} (\cos 135^\circ + i \sin 135^\circ),$$

$$\beta_2 = \sqrt[3]{2} (\cos 255^\circ + i \sin 255^\circ).$$

Учитывая, что  $\cos 45^\circ = \sin 45^\circ = 1/\sqrt{2}$ , получим  $\beta_1 = -1 + i$ . Для вычисления  $\beta_0$  и  $\beta_2$  заметим, что  $15^\circ = 45^\circ - 30^\circ$ , так что

$$\cos 15^\circ = \cos 45^\circ \cos 30^\circ + \sin 45^\circ \sin 30^\circ = \frac{1}{\sqrt{2}} \left( \frac{\sqrt{3}}{2} + \frac{1}{2} \right),$$

$$\sin 15^\circ = \sin 45^\circ \cos 30^\circ - \cos 45^\circ \sin 30^\circ = \frac{1}{\sqrt{2}} \left( \frac{\sqrt{3}}{2} - \frac{1}{2} \right).$$

Поэтому

$$\beta_0 = \frac{\sqrt{3}+1}{2} + i \frac{\sqrt{3}-1}{2},$$

$$\beta_2 = -\frac{\sqrt{3}-1}{2} - i \frac{\sqrt{3}-1}{2}.$$

В заключение отметим, что среди  $n$  значений корня  $n$ -й степени из комплексного числа нет оснований, вообще говоря, предпочитать какое-либо одно значение остальным. Понятие «арифметического значения» при извлечении корня из комплексного числа не вводится и его невозможно ввести каким-либо естественным способом,

Легко проследить, что упоминавшееся выше «противоречие»  $-1 = i^2 = \sqrt{-1}\sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{1} = 1$  имеет своим источником путаницу в выборе значений квадратных корней. Дело в том, что в применении к комплексным числам формула  $\sqrt{\alpha}\sqrt{\beta} = \sqrt{\alpha\beta}$  верна (при выбранных значениях для  $\sqrt{\alpha}$  и  $\sqrt{\beta}$ ) лишь при одном выборе значения для  $\sqrt{\alpha\beta}$ , а при другом выборе она не верна и даже в случае, если  $\alpha\beta$  оказывается вещественным положительным числом, подходящее значение  $\sqrt{\alpha\beta}$  не обязано быть арифметическим. В рассмотренном примере игра идет на равенствах:  $\sqrt{-1}\sqrt{-1} = -1$  и  $\sqrt{-1}\sqrt{-1} = 1$ . Первое из них верно, если в качестве значений для обоих сомножителей взять одинаковые значения  $\sqrt{-1}$  (т. е.  $i$ ,  $i$  или  $-i$ ,  $-i$ ), второе верно, если взять различные значения (т. е.  $i$ ,  $-i$  или  $-i$ ,  $i$ ).

**3. Извлечение квадратного корня.** Извлечение квадратного корня из комплексного числа можно осуществить, не обращаясь к тригонометрической форме. Выведем алгебраическую формулу для выполнения этого действия.

Пусть  $x + yi = \sqrt{a + bi}$ , и положим, что  $b \neq 0$ , так как только этот случай представляет интерес. Тогда  $a + bi = (x + yi)^2 = x^2 - y^2 + 2xyi$ , что равносильно системе уравнений

$$x^2 - y^2 = a,$$

$$2xy = b,$$

причем нас интересуют только вещественные решения этой системы. Мы уже знаем, что задача имеет решения. Это дает право

предположить, что под буквами  $x$  и  $y$  подразумевается решение задачи. Тогда  $(x^2 - y^2)^2 = a^2$ ,  $4x^2y^2 = b^2$ . Складывая эти равенства, получим  $(x^2 + y^2)^2 = a^2 + b^2$ , откуда  $x^2 + y^2 = \sqrt{a^2 + b^2}$ , причем здесь должно брать арифметическое значение корня, ибо  $x^2 + y^2 > 0$ . Сопоставляя последнее равенство с первым уравнением системы, получим

$$\begin{aligned} 2x^2 &= \sqrt{a^2 + b^2} + a, \\ 2y^2 &= \sqrt{a^2 + b^2} - a. \end{aligned}$$

По замыслу задачи правые части обоих равенств должны быть неотрицательны, и это действительно имеет место, ибо  $\sqrt{a^2 + b^2} > \sqrt{a^2} = |a|$ .

Из последних равенств находим

$$x = \sigma_1 \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}, \quad y = \sigma_2 \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}.$$

Здесь снова берутся арифметические значения для корней, а  $\sigma_1$  и  $\sigma_2$  принимают значения  $\pm 1$ . Ясно, что так вычисленные числа  $x$  и  $y$  удовлетворяют первому уравнению системы  $x^2 - y^2 = a$ . Но они должны удовлетворять и второму:  $2xy = b$ . Это дает

$$2\sigma_1\sigma_2 \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \cdot \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} = b,$$

или, после очевидных преобразований,

$$\sigma_1\sigma_2 \sqrt{b^2} = b,$$

откуда  $\sigma_1\sigma_2 = 1$ , если  $b > 0$ , и  $\sigma_1\sigma_2 = -1$ , если  $b < 0$ , так что  $\sigma_2 = \sigma_1 \operatorname{sign} b$ , где  $\operatorname{sign} b$  обозначает знак  $b$ , т. е.  $+1$ , если  $b > 0$ , и  $-1$ , если  $b < 0$ .

Это дает формулу

$$\sqrt{a + bi} = \pm \left( \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i \operatorname{sign} b \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \right).$$

Пример 1.

$$\sqrt{i} = \pm \left( \sqrt{\frac{\sqrt{1+0+0}}{2}} + i \sqrt{\frac{\sqrt{1+0-0}}{2}} \right) = \pm \frac{1+i}{\sqrt{2}}.$$

Пример 2.

$$\sqrt{3-4i} = \pm \left( \sqrt{\frac{\sqrt{25+3}}{2}} - i \sqrt{\frac{\sqrt{25-3}}{2}} \right) = \pm (2-i).$$

## § 4. Корни из единицы

**1. Формула для корней из единицы.** Как и для всякого отличного от нуля комплексного числа, для числа 1 существует ровно  $n$  значений корня  $n$ -й степени. Так как  $1 \equiv \cos 0 + i \sin 0$ , то для корней  $n$ -й степени из 1 имеет место формула

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \text{ при } k = 0, 1, \dots, n-1.$$

Конечно, в качестве значений для  $k$  может быть взята любая полная система вычетов по модулю  $n$ .

**2. Геометрическое изображение.** Все корни из 1 имеют модуль, равный 1, так что их изображения находятся на окружности радиуса 1 с центром в точке 0. Один из них при  $k=0$  есть просто число 1 и изображается точкой пересечения положительной полуоси вещественной оси с единичной окружностью. Корень  $\varepsilon_1$  имеет своим аргументом  $\frac{2\pi}{n}$ , т. е.  $\frac{1}{n}$  часть полной окружности. Дальнейшие корни  $\varepsilon_2, \varepsilon_3, \dots, \varepsilon_{n-1}$  имеют своими аргументами  $\frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}$  части окружности, так что они все делят единичную окружность на  $n$  равных частей (рис. 6).

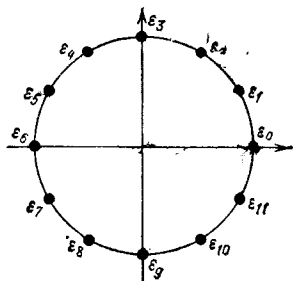


Рис. 6.

Все корни  $n$ -й степени из 1 являются корнями уравнения  $x^n - 1 = 0$ . По этой причине уравнение  $x^n - 1 = 0$  носит название *уравнения деления круга*.

**3. Первообразные корни  $n$ -й степени из 1.** Корень  $n$ -й степени из 1 называется *первообразным* или *принадлежащим показателю  $n$* , если он не является корнем из 1 с меньшим чем  $n$  натуральным показателем. Другими словами,  $\varepsilon$  есть первообразный корень  $n$ -й степени из 1, если  $\varepsilon^n = 1$ , но при любом натуральном  $m < n$ ,  $\varepsilon^m \neq 1$ . Число  $\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$  есть, очевидно, первообразный корень  $n$ -й степени из 1, но при  $n > 2$  существуют и другие первообразные корни. Именно, верна следующая теорема.

**Теорема 1.** Число  $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$  есть первообразный корень  $n$ -й степени из 1 в том и только в том случае, если  $k$  и  $n$  взаимно просты.

Действительно,  $\varepsilon_k^n = 1$  всегда. Пусть  $k$  и  $n$  взаимно просты и пусть  $\varepsilon_k^m = 1$ , где  $m$  — натуральное число. Тогда  $\frac{2km\pi}{n} = 2t\pi$  при целом  $t$  и  $\frac{km}{n} = t$ , т. е.  $km$  делится на  $n$ . Но  $k$  и  $n$  взаимно просты,

Следовательно,  $m$  делится на  $n$  и потому не может быть меньше  $n$ . Поэтому  $\varepsilon_k$  есть первообразный корень  $n$ -й степени из 1.

Предположим теперь, что  $\varepsilon_k$  есть первообразный корень  $n$ -й степени из 1, и пусть  $d = \text{н. о. д.}(k, n)$ ,  $n = dn_1$ ,  $k = dk_1$ . Тогда  $\varepsilon_k = \cos \frac{2k_1\pi}{n_1} + i \sin \frac{2k_1\pi}{n_1}$  и  $\varepsilon_k^{n_1} = 1$ . Отсюда следует, что  $d = 1$ , т. е.  $k$  и  $n$  взаимно просты, иначе  $n_1 < n$  и  $\varepsilon_k$  — не первообразный корень.

Из доказанной теоремы следует, что число первообразных корней  $n$ -й степени из 1 равно числу меньших  $n$  и взаимно простых с  $n$  чисел, т. е. оно равно значению  $\varphi(n)$  функции Эйлера. Например, при  $n = 12$  имеется четыре первообразных корня:  $\varepsilon_1$ ,  $\varepsilon_5$ ,  $\varepsilon_7$  и  $\varepsilon_{11}$ .

**Предложение 2.** Число  $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$  является первообразным корнем из 1 степени  $n_1 = \frac{n}{d}$ , где  $d = \text{н. о. д.}(k, n)$ .

Действительно, пусть  $n_1 = \frac{n}{d}$ ,  $k_1 = \frac{k}{d}$ . Тогда числа  $n_1$  и  $k_1$  взаимно просты и  $\varepsilon_k = \cos \frac{2k_1\pi}{n_1} + i \sin \frac{2k_1\pi}{n_1}$  есть первообразный корень степени  $n_1$  из 1 в силу только что доказанной теоремы.

Итак, среди корней  $n$ -й степени из 1 присутствуют первообразные корни из 1, принадлежащие всем показателям  $n_1 = \frac{n}{d}$ , являющимся делителями  $n$ . Например, среди корней 12-й степени из 1 присутствуют первообразные корни степени 12 ( $\varepsilon_1$ ,  $\varepsilon_5$ ,  $\varepsilon_7$ ,  $\varepsilon_{11}$ ), степени 6 ( $\varepsilon_2$  и  $\varepsilon_{10}$ ), степени 4 ( $\varepsilon_3$  и  $\varepsilon_9$ ), степени 3 ( $\varepsilon_4$  и  $\varepsilon_8$ ), степени 2 ( $\varepsilon_6$ ) и степени 1 ( $\varepsilon_0$ ).

#### 4. Свойства корней из 1.

**Предложение 3.** Произведение двух корней степени  $n$  из 1 есть корень степени  $n$  из 1.

**Доказательство.** Пусть  $\alpha$  и  $\beta$  — корни степени  $n$  из 1. Это значит, что  $\alpha^n = 1$  и  $\beta^n = 1$ . Но тогда и  $(\alpha\beta)^n = \alpha^n\beta^n = 1$ , т. е.  $\alpha\beta$  — тоже корень  $n$ -й степени из 1.

**Предложение 4.** Число, обратное корню степени  $n$  из 1, есть корень степени  $n$  из 1.

**Доказательство.** Если  $\alpha^n = 1$ , то  $(\alpha^{-1})^n = 1$ .

Эти два предложения означают, что корни степени  $n$  из 1 образуют абелеву группу относительно умножения.

**Предложение 5.** Пусть  $\varepsilon$  — любой первообразный корень степени  $n$  из 1. Тогда всякий корень степени  $n$  из 1 получается из  $\varepsilon$  возведением в некоторую степень с натуральным показателем.

**Доказательство.** Пусть  $\varepsilon$  — какой-либо первообразный корень степени  $n$  из 1. Тогда при любом целом  $k$  число  $\varepsilon^k$  будет корнем степени  $n$  из 1, ибо  $(\varepsilon^k)^n = (\varepsilon^n)^k = 1$ . Рассмотрим числа 1,  $\varepsilon$ ,  $\varepsilon^2$ , ...,  $\varepsilon^{n-1}$ . Все они суть корни степени  $n$  из 1. Среди них нет равных, ибо если  $\varepsilon^k = \varepsilon^m$  при  $0 \leq k < m \leq n-1$ , то  $\varepsilon^{m-k} = 1$ ,

что невозможно, ибо  $m - k$  есть натуральное число, меньшее  $n$ , а  $\varepsilon$  — первообразный корень степени  $n$ . Итак, числа  $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$  — попарно различные корни  $n$ -й степени из 1, и их число равно  $n$ , т. е. равно числу всех корней  $n$ -й степени из 1. Поэтому  $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$  суть все корни степени  $n$  из 1, что и требовалось доказать.

Заметим, что сопоставление целому числу  $k$  корня  $\varepsilon^k$  из 1 соотносит одному корню класс чисел по модулю  $n$ , и, так как при умножении степеней показатели складываются, сумме классов соответствует произведение корней. Тем самым группа корней  $n$ -й степени из 1 изоморфна группе классов вычетов по модулю  $n$  относительно сложения.

Предложение 6. Все значения  $\sqrt[n]{\alpha}$  ( $\alpha \neq 0$ ) получаются из одного значения посредством умножения на все корни степени  $n$  из 1.

Доказательство. Пусть  $\beta_0^n = \alpha$  и  $\beta^n = \alpha$ . Тогда  $(\beta\beta_0^{-1})^n = 1$ , так что  $\beta\beta_0^{-1} = \varepsilon$  есть корень  $n$ -й степени из 1 и  $\beta = \beta_0\varepsilon$ . Обратно, если  $\beta = \beta_0\varepsilon$  и  $\varepsilon$  есть корень степени  $n$  из 1, то  $\beta^n = \beta_0^n\varepsilon^n = \alpha$ .

Последнее предложение показывает, что корни степени  $n$  из 1 при действии извлечения корня  $n$ -й степени из комплексного числа играют такую же роль, как знаки  $\pm$  при извлечении квадратного корня. Это естественно, так как постановка знаков  $\pm$  равносильна умножению на  $\pm 1$ , т. е. на корни степени 2 из 1.

— 5. Алгебраическое вычисление некоторых корней из 1. При нескольких малых показателях корни из 1 легко вычисляются. Ясно, что квадратные корни из 1 суть  $\pm 1$ . Корни 4-й степени равны, очевидно,  $+1, -1, i, -i$ .

Для вычисления корней 3-й степени из 1 рассмотрим уравнение  $x^3 - 1 = 0$ . Разложение левой части на множители дает  $(x-1)(x^2+x+1) = 0$ . Приравнивание к нулю первого множителя дает  $x = 1$ . Второй множитель порождает корни  $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$ , являющиеся первообразными кубическими корнями из 1. Сравнение с формулой  $\varepsilon_k = \cos \frac{2k\pi}{3} + i \sin \frac{2k\pi}{3}$  показывает, что  $-\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos 120^\circ + i \sin 120^\circ$ . Сравнение компонент дает хорошо известные из тригонометрии формулы

$$\cos 120^\circ = -\cos 60^\circ = -\frac{1}{2}, \quad \sin 120^\circ = \sin 60^\circ = \frac{\sqrt{3}}{2}.$$

Разложение на множители многочлена

$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1).$$

показывает, что первообразные корни степени 6 из 1 суть корни  $\frac{1}{2} \pm i \frac{\sqrt{3}}{2}$  уравнения  $x^2 - x + 1 = 0$ , ибо приравнивание к нулю других множителей дает не первообразные корни.

Рассмотрим  $n = 5$ . Уравнение  $x^5 - 1 = 0$  приводит после разложения на множители к уравнению  $(x - 1)(x^4 + x^3 + x^2 + x + 1) = 0$ . Первообразные корни являются корнями уравнения  $x^4 + x^3 + x^2 + x + 1 = 0$ . Оно равносильно уравнению  $x^2 + x^{-2} + x + x^{-1} + 1 = 0$ . Положив  $x + x^{-1} = z$  и заметив, что  $x^2 + 2 + x^{-2} = z^2$ , мы получим следующее уравнение относительно  $z$ :  $z^2 + z - 1 = 0$ , откуда  $z_1 = -\frac{1}{2} + \frac{\sqrt{5}}{2}$ ;  $z_2 = -\frac{1}{2} - \frac{\sqrt{5}}{2}$ . Корни из 1 находятся из уравнений  $x^2 - z_1x + 1 = 0$  и  $x^2 - z_2x + 1 = 0$ , откуда  $x = \frac{z_1 \pm i \sqrt{4 - z_1^2}}{2}$  и  $x = \frac{z_2 \pm i \sqrt{4 - z_2^2}}{2}$ . Подставив вместо  $z_1$  и  $z_2$  их значения, получим

$$\begin{aligned} x_1 &= \frac{\sqrt{5}-1}{4} + i \frac{\sqrt{10+2\sqrt{5}}}{4}, & x_2 &= \frac{\sqrt{5}-1}{4} - i \frac{\sqrt{10+2\sqrt{5}}}{4}, \\ x_3 &= -\frac{\sqrt{5}-1}{4} + i \frac{\sqrt{10-2\sqrt{5}}}{4}, & x_4 &= -\frac{\sqrt{5}-1}{4} - i \frac{\sqrt{10-2\sqrt{5}}}{4}. \end{aligned}$$

Сопоставление с формулой  $x_k = \cos \frac{2k\pi}{5} + i \sin \frac{2k\pi}{5} = \cos k \cdot 72^\circ + i \sin k \cdot 72^\circ$  дает сравнительно мало известную формулу  $\cos 72^\circ = \frac{\sqrt{5}-1}{4}$ .

Из нее легко выводится формула для длины стороны  $a_{10}$  правильного десятиугольника, вписанного в круг радиуса  $r$ . Именно,

$$\begin{aligned} a_{10} &= 2r \sin \frac{2\pi}{10 \cdot 2} = 2r \sin \frac{\pi}{10} = 2r \cos \left( \frac{\pi}{2} - \frac{\pi}{10} \right) = 2r \cos \frac{2\pi}{5} = \\ &= r \frac{\sqrt{5}-1}{2}. \end{aligned}$$

Из этой формулы следует способ построения стороны правильного десятиугольника циркулем и линейкой (рис. 7), известный еще в глубокой древности и описанный Евклидом.

Разумеется, формулу  $a_{10} = r \frac{\sqrt{5}-1}{2}$  легко обосновать без привлечения задачи о корнях из 1. Именно (рис. 8), равнобедренный треугольник с основанием  $a_{10}$  и боковыми сторонами  $r$  имеет угол  $36^\circ$  при вершине и, следовательно, углы  $72^\circ$  при основании. Биссектриса одного из этих углов разбивает треугольник снова на два равнобедренных треугольника, так что  $|OD| = |BD| = |AB| = a_{10}$ . Из подобия треугольников  $OAB$  и  $BDA$  получаем  $\frac{a_{10}}{r} = \frac{r - a_{10}}{a_{10}}$ , откуда  $a_{10}^2 + ra_{10} - r^2 = 0$  и  $a_{10} = r \frac{\sqrt{5}-1}{2}$ .

Во времена Евклида были известны способы построения циркулем и линейкой правильных  $n$ -угольников, вписанных в данный круг, для следующих значений  $n$ :  $n = 4$ ,  $n = 6$  (а значит, и  $n = 3$ ),  $n = 10$  (с ним и  $n = 5$  и  $n = 15$ , ибо  $\frac{1}{15} = \frac{1}{6} - \frac{1}{10}$ ) — и прием удвоения числа сторон, что приводило к возможности построения при  $n = 2^k$ ,  $n = 3 \cdot 2^k$ ,  $n = 5 \cdot 2^k$  и  $n = 15 \cdot 2^k$ . Никаких других случаев возможности аналогичного построения не было известно до конца 18 в. Тем более поразительным было открытие в 1801 г. способа построения правильного 17-угольника восемнадцатилетним немецким математиком К. Ф. Гауссом. Более того, Гаусс показал, что для возможности построения циркулем и линейкой вписанного

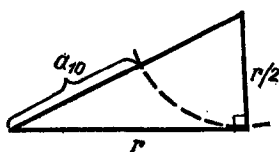


Рис. 7.

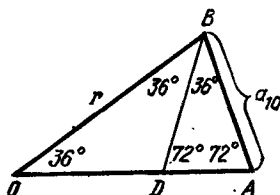


Рис. 8.

в данный круг правильного  $n$ -угольника необходимо и достаточно, чтобы каноническое разложение числа  $n$  имело вид  $2^k p q \dots r$ , где  $k$  — любое целое число, а  $p, q, \dots, r$  — так называемые простые числа Ферма. Простое число  $p$  называется *числом Ферма*, если  $p - 1$  есть степень числа 2. Наименьшими простыми числами Ферма являются  $3 = 2 + 1$ ,  $5 = 2^2 + 1$ ,  $17 = 2^4 + 1$ ,  $257 = 2^8 + 1$ ,  $65537 = 2^{16} + 1$ . Легко видеть, что для простоты числа  $2^n + 1$  необходимо, чтобы показатель  $n$  сам был степенью двойки (но не достаточно:  $2^{32} + 1$  — не простое число). Существует ли бесконечно много простых чисел Ферма, или их лишь конечное число — вопрос, не решенный до настоящего времени.

Выведем формулы, из которых следует, что построение вписанного в круг правильного 17-угольника выполнимо циркулем и линейкой. Разумеется, мы в состоянии это сделать здесь лишь формально, не вскрывая глубоких причин успеха.

Прежде всего заметим, что длина стороны  $a_{34}$  правильного 34-угольника, вписанного в круг радиуса  $r$ , равна  $2r \sin \frac{2\pi}{2 \cdot 34} = 2r \sin \frac{\pi}{34} = 2r \cos\left(\frac{\pi}{2} - \frac{\pi}{34}\right) = 2r \cos \frac{8\pi}{17}$ . Положим  $\varepsilon = \cos \frac{2\pi}{17} + i \sin \frac{2\pi}{17}$ . Рассмотрим следующие два числа:

$$\begin{aligned} \alpha_1 &= \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16}, \\ \alpha_2 &= \varepsilon^3 + \varepsilon^5 + \varepsilon^6 + \varepsilon^7 + \varepsilon^{10} + \varepsilon^{11} + \varepsilon^{12} + \varepsilon^{14}. \end{aligned}$$

Заметим, что  $\varepsilon + \varepsilon^2 + \dots + \varepsilon^{16} = \frac{\varepsilon^{17} - \varepsilon}{\varepsilon - 1} = \frac{1 - \varepsilon}{\varepsilon - 1} = -1$ . Поэтому  $\alpha_1 + \alpha_2 = -1$ .

Далее, числа  $\alpha_1$  и  $\alpha_2$  вещественны, ибо  $\varepsilon^k$  и  $\varepsilon^{17-k} = \varepsilon^{-k}$  комплексно сопряжены, и, учитывая расположение на единичном круге слагаемых  $\varepsilon^k$ , легко убедиться, что  $\alpha_1 > 0$ ,  $\alpha_2 < 0$ .

Вычислим теперь

$$\begin{aligned} \alpha_1 \alpha_2 = & \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^8 + \varepsilon^{11} + \varepsilon^{12} + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^5 + \varepsilon^7 + \\ & + \varepsilon^8 + \varepsilon^9 + \varepsilon^{12} + \varepsilon^{13} + \varepsilon^{14} + \varepsilon^{16} + \varepsilon^7 + \varepsilon^9 + \varepsilon^{10} + \varepsilon^{11} + \\ & + \varepsilon^{14} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon + \varepsilon^{11} + \varepsilon^{13} + \varepsilon^{14} + \varepsilon^{15} + \varepsilon + \varepsilon^2 + \\ & + \varepsilon^3 + \varepsilon^5 + \varepsilon^{12} + \varepsilon^{14} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \\ & + \varepsilon^{16} + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^6 + \varepsilon^7 + \varepsilon^8 + \varepsilon^{10} + \varepsilon + \varepsilon^3 + \\ & + \varepsilon^4 + \varepsilon^5 + \varepsilon^8 + \varepsilon^9 + \varepsilon^{10} + \varepsilon^{12} + \varepsilon^2 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6 + \\ & + \varepsilon^9 + \varepsilon^{10} + \varepsilon^{11} + \varepsilon^{13}. \end{aligned}$$

Пока мы просто умножили каждое слагаемое из  $\alpha_1$  на каждое слагаемое из  $\alpha_2$ , заменив все показатели, большие 16, их остатками от деления на 17. Внимательное рассмотрение получившейся суммы показывает, что среди 64 слагаемых присутствуют все числа  $\varepsilon, \varepsilon^2, \dots, \varepsilon^{16}$ , каждое по четыре раза. Поэтому  $\alpha_1 \alpha_2 = 4(\varepsilon + \varepsilon^2 + \dots + \varepsilon^{16}) = -4$ . Итак,  $\alpha_1 + \alpha_2 = -1$ ,  $\alpha_1 \alpha_2 = -4$ ,  $\alpha_1 > 0$ ,  $\alpha_2 < 0$ . Поэтому

$$\alpha_1 = \frac{-1 + \sqrt{17}}{2}, \quad \alpha_2 = \frac{-1 - \sqrt{17}}{2}.$$

Рассмотрим теперь числа  $\beta_1 = \varepsilon + \varepsilon^4 + \varepsilon^{13} + \varepsilon^{16}$  и  $\beta_2 = \varepsilon^2 + \varepsilon^8 + \varepsilon^9 + \varepsilon^{15}$ . Из расположения слагаемых на единичной окружности легко получить, что  $\beta_1 > 0$ ,  $\beta_2 < 0$ .

Далее,  $\beta_1 + \beta_2 = \alpha_1$ ,  $\beta_1 \beta_2 = \varepsilon^3 + \varepsilon^9 + \varepsilon^{10} + \varepsilon^{16} + \varepsilon^6 + \varepsilon^{12} + \varepsilon^{13} + \varepsilon^2 + \varepsilon^{15} + \varepsilon^4 + \varepsilon^5 + \varepsilon^{11} + \varepsilon + \varepsilon^7 + \varepsilon^8 + \varepsilon^{14} = -1$ . Поэтому

$$\beta_1 = \frac{\alpha_1 + \sqrt{\alpha_1^2 + 4}}{2}, \quad \beta_2 = \frac{\alpha_1 - \sqrt{\alpha_1^2 + 4}}{2}.$$

Возьмем еще  $\beta_3 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{12} + \varepsilon^{14}$ ,  $\beta_4 = \varepsilon^6 + \varepsilon^7 + \varepsilon^{10} + \varepsilon^{11}$ . Для них аналогично получим, что  $\beta_3 + \beta_4 = \alpha_2$ ,  $\beta_3 \beta_4 = -1$ ,  $\beta_3 > 0$ ,  $\beta_4 < 0$ , откуда

$$\beta_3 = \frac{\alpha_2 + \sqrt{\alpha_2^2 + 4}}{2}, \quad \beta_4 = \frac{\alpha_2 - \sqrt{\alpha_2^2 + 4}}{2}.$$

Теперь положим  $\gamma_1 = \varepsilon^4 + \varepsilon^{13}$ ,  $\gamma_2 = \varepsilon + \varepsilon^{16}$ . Ясно, что  $\gamma_2 > \gamma_1 > 0$ . Далее,  $\gamma_1 + \gamma_2 = \beta_1$ ,  $\gamma_1 \gamma_2 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12} = \beta_3$ , откуда

$$\gamma_1 = \frac{\beta_1 - \sqrt{\beta_1^2 - 4\beta_3}}{2}. \quad \text{Но } \gamma_1 = 2 \cos \frac{4 \cdot 2\pi}{17} = \frac{1}{r} a_{34}.$$

Итак, сторона правильного 34-угольника, вписанного в круг радиуса  $r$ , находится по формуле

$$a_{34} = r \frac{\beta_1 - \sqrt{\beta_1^2 - 4\beta_3}}{2},$$

где

$$\beta_1 = \frac{\alpha_1 + \sqrt{\alpha_1^2 + 4}}{2}, \quad \beta_3 = \frac{\alpha_2 + \sqrt{\alpha_2^2 + 4}}{2}, \quad \alpha_1 = \frac{-1 + \sqrt{17}}{2},$$

$$\alpha_2 = \frac{-1 - \sqrt{17}}{2}.$$

Таким образом, для вычисления  $a_{34}$  нужно кроме арифметических действий сделать несколько извлечений квадратного корня. Все эти действия выполнимы при помощи циркуля и линейки.

## § 5. Показательная и логарифмическая функции комплексной переменной

**1. Определение показательной функции.** Показательная функция  $a^x$  вещественной переменной  $x$  (при положительном основании) определяется в несколько приемов. Сперва, для натуральных значений  $x$  — как произведение равных сомножителей. Затем определение распространяется на целые отрицательные и ненулевые значения для  $x$  по правилам  $a^{-n} = \frac{1}{a^n}$  и  $a^0 = 1$ . Далее рассматриваются дробные показатели, при которых значение показательной функции определяется при помощи корней:  $a^{p/q} = \sqrt[q]{a^p}$ . Для иррациональных значений определение связано уже с основным понятием математического анализа — с предельным переходом, из соображений непрерывности. Все эти соображения никак не применимы к попыткам распространить показательную функцию на комплексные значения показателя, и что такое, например,  $2^{1+i}$  — совершенно непонятно.

Впервые степень с комплексным показателем при натуральном основании  $e = 2,71828\dots$  была введена Эйлером на основе анализа ряда построений интегрального исчисления. Иногда очень похожие алгебраические выражения при интегрировании дают совершенно разные ответы:

$$\int \frac{1}{1-x^2} dx = \frac{1}{2} \ln \frac{x+1}{x-1} + C,$$

$$\int \frac{1}{1+x^2} dx = \arctg x + C.$$

В то же время здесь второй интеграл формально получается из первого при замене  $x$  на  $xi$ .

Отсюда можно сделать заключение, что при надлежащем определении показательной функции с комплексным показателем обратные тригонометрические функции родственны логарифмам и тем самым показательная функция связана с тригонометрическими.

У Эйлера хватило смелости и фантазии дать разумное определение для показательной функции с основанием  $e$ , именно,

$$e^{a+bi} = e^a (\cos b + i \sin b).$$

Это определение, и потому данная формула не доказывается, можно лишь искать доводы в пользу разумности и целесообразности такого определения. Математический анализ доставляет очень много доводов этого рода. Мы ограничимся лишь одним.

Известно, что при вещественном  $x$  имеет место предельное соотношение:  $e^x = \lim_{n \rightarrow \infty} \left(1 + \frac{x}{n}\right)^n$ . В правой части находится многочлен, имеющий смысл и при комплексных значениях для  $x$ . Предел последовательности комплексных чисел определяется естественным образом. Последовательность  $c_n = a_n + b_n i$  считается *сходящейся*, если сходятся последовательности  $a_n$  и  $b_n$  вещественных и мнимых частей и принимается  $\lim_{n \rightarrow \infty} c_n = \lim_{n \rightarrow \infty} a_n + i \lim_{n \rightarrow \infty} b_n$ .

Найдем  $\lim_{n \rightarrow \infty} \left(1 + \frac{a+bi}{n}\right)^n$ . Для этого обратимся к тригонометрической форме  $1 + \frac{a}{n} + \frac{b}{n}i = r_n (\cos \varphi_n + i \sin \varphi_n)$ , причем для аргумента будем выбирать значения из промежутка  $-\pi < \varphi_n \leq \pi$ . При таком выборе ясно, что  $\varphi_n \rightarrow 0$ , ибо  $1 + \frac{a}{n} + \frac{b}{n}i \rightarrow 1$ . Далее,

$$r_n = \sqrt{\left(1 + \frac{a}{n}\right)^2 + \frac{b^2}{n^2}} = \left(1 + \frac{2a}{n} + \frac{a^2 + b^2}{n^2}\right)^{1/2},$$

$$\cos \varphi_n = \frac{1 + \frac{a}{n}}{r_n}, \quad \sin \varphi_n = \frac{b}{nr_n}.$$

Теперь

$$\left(1 + \frac{a}{n} + \frac{b}{n}i\right)^n = r_n^n (\cos n\varphi_n + i \sin n\varphi_n).$$

Для предельного перехода нужно убедиться в существовании пределов для  $r_n^n$  и  $n\varphi_n$  и найти эти пределы. Ясно, что  $r_n \rightarrow 1$  и

$$\begin{aligned} r_n^n &= \left(1 + \frac{2a}{n} + \frac{a^2 + b^2}{n^2}\right)^{\frac{n}{2}} = \\ &= \left[\left(1 + \frac{2a}{n} + \frac{a^2 + b^2}{n^2}\right)^{\frac{1}{\frac{2a}{n} + \frac{a^2 + b^2}{n^2}}}\right]^{\left(\frac{2a}{n} + \frac{a^2 + b^2}{n^2}\right) \frac{n}{2}} \rightarrow e^a. \end{aligned}$$

Далее,  $n\varphi_n = n \sin \varphi_n \cdot \frac{\varphi_n}{\sin \varphi_n} = \frac{b}{r_n} \cdot \frac{\varphi_n}{\sin \varphi_n} \rightarrow b$ .

Итак, в выражении

$$\left(1 + \frac{a}{n} + \frac{b}{n}i\right)^n = r_n^n \cos n\varphi_n + ir_n^n \sin n\varphi_n$$

вещественная часть стремится к  $e^a \cos b$ , мнимая — к  $e^a \sin b$ , так что

$$\lim_{n \rightarrow \infty} \left(1 + \frac{a}{n} + \frac{b}{n}i\right)^n = e^a (\cos b + i \sin b).$$

Это несложное рассуждение дает один из доводов в пользу определения Эйлера показательной функции.

Установим теперь, что при умножении значений показательной функции показатели складываются. Действительно:

$$\begin{aligned} e^{a_1+b_1i} \cdot e^{a_2+b_2i} &= e^{a_1} (\cos b_1 + i \sin b_1) e^{a_2} (\cos b_2 + i \sin b_2) = \\ &= e^{a_1+a_2} (\cos(b_1+b_2) + i \sin(b_1+b_2)) = e^{a_1+a_2+(b_1+b_2)i}. \end{aligned}$$

**2. Формулы Эйлера.** Положим в определении показательной функции  $a = 0$ . Получим:

$$\cos b + i \sin b = e^{bi}.$$

Заменив  $b$  на  $-b$ , получим

$$\cos b - i \sin b = e^{-bi}.$$

Складывая и вычитая почленно эти равенства, найдем формулы

$$\cos b = \frac{e^{bi} + e^{-bi}}{2}, \quad \sin b = \frac{e^{bi} - e^{-bi}}{2i},$$

носящие название *формул Эйлера*. Они устанавливают связь между тригонометрическими функциями и показательной с мнимыми показателями.

**3. Натуральный логарифм комплексного числа.** Комплексное число, заданное в тригонометрической форме  $\alpha = r(\cos \varphi + i \sin \varphi)$ , можно записать в форме  $re^{i\varphi}$ . Эта форма записи комплексного числа называется *показательной*. Она сохраняет все хорошие свойства тригонометрической формы, но еще более краткая. Далее,  $\alpha = re^{i\varphi} = e^{\ln r} e^{i\varphi} = e^{\ln r + i\varphi}$ . Поэтому естественно считать, что  $\ln \alpha = \ln r + i\varphi$ , так что вещественной частью логарифма комплексного числа оказывается логарифм его модуля, мнимой частью — его аргумент. Это в некоторой степени объясняет «логарифмическое» свойство аргумента — аргумент произведения равен сумме аргументов сомножителей.

Введенная таким образом логарифмическая функция определена для всех комплексных чисел, за исключением нуля. Необходимо только помнить, что логарифмическая функция многозначна, в силу многозначности аргумента. Однозначность можно было бы установить, например, выбирая ветвь логарифма, для которой  $-\pi < \varphi \leq \pi$ , но это приводит к ряду неудобств. В частности, свойство логарифма — логарифм произведения равен сумме логарифмов

мов сомножителей — верно лишь с учетом многозначности. Так, например, один из значений  $\ln 1$  является 0, одним из значений  $\ln(-1)$  является  $\pi i$ , ибо  $-1 = \cos \pi + i \sin \pi = e^{\pi i}$ . Однако  $\ln[(-1) \cdot (-1)] = \pi i + \pi i = 2\pi i$ . Это одно из значений логарифма 1 (ибо  $1 = \cos 2k\pi + i \sin 2k\pi$ ), но отличное от 0.

**4. Показательная функция с произвольным основанием.** Пусть  $\alpha$  — комплексное число, отличное от нуля. Тогда  $\alpha = e^{\ln \alpha}$  при любом значении  $\ln \alpha$ . Поэтому естественно считать по определению  $\alpha^\beta = e^{\beta \ln \alpha}$ . Это снова многозначная функция от  $\alpha$  и  $\beta$ , в силу многозначности  $\ln \alpha$ , который определен с точностью до слагаемого  $2k\pi i$ . Посмотрим, например, чему равно  $i^i$ . Так как  $\ln i = i\left(\frac{\pi}{2} + 2k\pi\right)$ ,  $i^i = e^{-\left(\frac{\pi}{2} + 2k\pi\right)}$ . Результат кажется несколько парадоксальным — все значения «очень мнимого» выражения  $i^i$  вещественны.

# ПРОСТЕЙШИЕ СВЕДЕНИЯ ОБ АЛГЕБРЕ ПОЛИНОМОВ

## § 1. Полиномы от одной буквы

**1. Определение.** В школьной алгебре одночленом от некоторой буквы  $x$  называется алгебраическое выражение вида  $ax^m$ , где  $a$  — некоторое число,  $x$  — буква,  $m$  — целое неотрицательное число. Одночлен  $ax^0$  отождествляется с числом  $a$ , так что числа рассматриваются как одночлены. Далее, одночлены называются подобными, если показатели при букве  $x$  одинаковы. Подобные одночлены складываются по правилу  $ax^m + bx^m = (a + b)x^m$ , называемому приведением подобных членов. Многочленом или полиномом называется алгебраическая сумма одночленов. В полиноме порядок слагаемых безразличен и подобные одночлены можно соединить, согласно приведению подобных членов. Поэтому любой полином можно записать в канонической форме  $a_0x^n + a_1x^{n-1} + \dots + a_n$ , с расположением членов в порядке убывания показателей. Иногда оказывается удобным записывать члены полинома в порядке возрастания показателей.

Буква  $x$  обычно обозначает произвольное число. Иногда  $x$  считается переменной, тогда полином задает функцию от  $x$ , называемую целой рациональной функцией.

Два полинома называются формально равными, если они, в канонической записи, составлены из одинаковых одночленов. Ясно, что формально равные полиномы равны тождественно, т. е. принимают одинаковые значения при каждом значении буквы  $x$ . Верно и обратное утверждение: если два полинома равны тождественно, то они равны формально — но это совсем не очевидно и требует доказательства, которое будет дано в п. 7.

Наша ближайшая задача состоит в том, чтобы несколько расширить понятие полинома. Пусть  $A$  — некоторое коммутативное ассоциативное кольцо с единицей, и пусть  $x$  — буква, посторонняя для кольца  $A$ . Одночленом от буквы  $x$  с коэффициентом из  $A$  называется выражение  $ax^m$ , где  $a \in A$ ,  $m$  — целое неотрицательное число. Считается, что  $ax^0 = a$ , так что элементы кольца  $A$  являются одночленами частного вида. Выражение  $ax^m$  рассматривается формально — как «картинка», изображенная на бумаге. Для одночленов естественным образом определяются действия приведения подобных членов  $ax^m + bx^m = (a + b)x^m$  и действия умножения  $ax^m \cdot bx^k = abx^{m+k}$ . «Картинка», состоящая из нескольких

одночленов, соединенных знаком  $+$ , называется *многочленом* или *полиномом* от  $x$  с коэффициентами из  $A$ . Предполагается, что порядок следования одночленов безразличен, подобные одночлены можно соединять, а также вставлять и выбрасывать одночлены с нулевыми коэффициентами. Без нарушения общности можно считать полином записанным в канонической форме  $a_0x^n + a_1x^{n-1} + \dots + a_n$  (т. е. в порядке убывания степеней) или в порядке возрастания степеней  $c_0 + c_1x + \dots + c_nx^n$ .

Дадим теперь естественные определения равенства полиномов и основных действий над ними.

1. Два полинома считаются *равными*, если они составлены в канонической записи из одинаковых одночленов, т. е.

$$a_0x^n + a_1x^{n-1} + \dots + a_n = b_0x^n + b_1x^{n-1} + \dots + b_n$$

в том и только в том случае, если  $a_i = b_i$ ,  $i = 0, 1, \dots, n$  (снова «формальное» равенство).

2. *Суммой* двух полиномов называется полином, получающийся посредством объединения одночленов, составляющих слагаемые.

Разумеется, после объединения следует привести подобные члены. Таким образом,

$$\begin{aligned} (a_0x^n + a_1x^{n-1} + \dots + a_n) + (b_0x^n + b_1x^{n-1} + \dots + b_n) = \\ = (a_0 + b_0)x^n + (a_1 + b_1)x^{n-1} + \dots + (a_n + b_n). \end{aligned}$$

3. *Произведением* двух полиномов называется полином, составленный из произведений всех членов первого сомножителя на все члены второго.

Здесь снова возможно приведение подобных членов. Таким образом,

$$\begin{aligned} (a_0x^n + a_1x^{n-1} + \dots + a_n)(b_0x^m + b_1x^{m-1} + \dots + b_m) = \\ = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \dots + a_nb_m. \end{aligned}$$

Коэффициент при  $x^{n+m-k}$  равен  $a_0b_k + a_1b_{k-1} + \dots + a_kb_0$ , если условиться считать, что  $a_i = 0$  при  $i > n$  и  $b_j = 0$  при  $j > m$ .

Множество полиномов от буквы  $x$  с коэффициентами из кольца  $A$  составляет, как легко проверить, кольцо по отношению к определённым выше действиям сложения и умножения. Кольцо это коммутативно и ассоциативно. Оно называется *кольцом полиномов* от буквы  $x$  над кольцом  $A$  и обозначается  $A[x]$ . Роль нуля в этом кольце играет нулевой полином, т. е. нуль кольца  $A$ , рассматриваемый как полином, не содержащий одночленов с ненулевыми коэффициентами. Роль единицы играет единица кольца  $A$ .

В данном выше определении одночлена и полинома имеется одно сомнительное место. Именно, было сказано, что  $x$  есть буква, посторонняя для кольца  $A$ , и не было объяснено, что это значит. Сказать, что  $x$  не принадлежит кольцу  $A$  — это сказать слишком

мало, так как при этом не исключаются нежелательные возможности  $x^2 \in A$  или  $\frac{1-x}{1+x} \in A$  и т. д. Однако мы в состоянии избавиться от «сомнительной» буквы  $x$  подобно тому, как избавились от символа  $i$  в обосновании комплексных чисел. Обратим внимание на те действия над коэффициентами полиномов, которые должны выполняться при действиях над самими полиномами. Опишем эти действия, исходя из расположения полиномов по возрастающим степеням буквы. Именно, вместо полиномов рассмотрим бесконечные последовательности  $(a_0, a_1, \dots, a_k, \dots)$  элементов кольца  $A$ , в которых все элементы, начиная с некоторого, равны нулю. Вводим теперь определения равенства и основных действий.

I.  $(a_0, a_1, \dots, a_k, \dots) = (b_0, b_1, \dots, b_k, \dots)$  тогда и только тогда, когда  $a_i = b_i, i = 0, 1, \dots, k, \dots$

II.  $(a_0, a_1, \dots, a_k, \dots) + (b_0, b_1, \dots, b_k, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, \dots)$ .

Ясно, что требование об обращении в нуль всех членов, начиная с некоторого, сохраняется при сложении.

III.  $(a_0, a_1, \dots, a_k, \dots)(b_0, b_1, \dots, b_k, \dots) = (a_0b_0, a_0b_1 + a_1b_0, \dots, a_0b_k + a_1b_{k-1} + \dots + a_kb_0, \dots)$ .

Здесь тоже сохраняется требование об обращении в нуль всех членов, начиная с некоторого места.

Легко проверяется коммутативность и ассоциативность сложения и умножения и дистрибутивность умножения со сложением. Далее, ясно, что  $(a, 0, \dots, 0, \dots) + (b, 0, \dots, 0, \dots) = (a + b, 0, \dots, 0, \dots)$  и  $(a, 0, \dots, 0, \dots)(b, 0, \dots, 0, \dots) = (ab, 0, \dots, 0, \dots)$ , и, более общо,  $(a, 0, \dots, 0, \dots)(b_0, b_1, \dots, b_k, \dots) = (ab_0, ab_1, \dots, ab_k, \dots)$ .

IV.  $a \in A$  отождествляется с последовательностью  $(a, 0, \dots, 0, \dots)$ .

Легко проверяется, что аксиома IV не находится в противоречии с первыми тремя.

Рассмотрим теперь последовательность  $(0, 1, 0, \dots, 0, \dots)$ , обозначив ее буквой  $x$ . Тогда  $x^2 = (0, 0, 1, 0, \dots, 0, \dots)$  и т. д. Поэтому

$$\begin{aligned} (a_0, a_1, a_2, \dots, a_n, 0, \dots) &= (a_0, 0, 0, \dots, 0, \dots) + \\ &+ (0, a_1, 0, \dots, 0, 0, \dots) + \dots + (0, 0, \dots, a_n, 0, \dots) = \\ &= a_0 + a_1(0, 1, 0, \dots) + a_2(0, 0, 1, 0, \dots) + \dots \\ &\therefore + a_n(0, 0, \dots, 1, 0, \dots) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n. \end{aligned}$$

Таким образом, нам удалось построить элементы кольца полиномов.

**2. Высший член и степень полинома.** Пусть  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ , причем  $a_0 \neq 0$ . Одночлен  $a_0x^n$  называется **высшим членом** полинома  $f(x)$  и показатель  $n$  называется **степенью**  $f(x)$  и обозначается  $\deg f$ . Нулевой полином не имеет выс-

шего члена в смысле данного определения и считается, что он равен 0. Степень нулевого полинома условно считается равной символу  $-\infty$ .

Предположим теперь, что кольцо  $A$  есть область целостности, т. е. что произведение двух элементов из  $A$  может равняться нулю, только если один из сомножителей равен нулю.

Пусть даны два полинома  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  и  $g(x) = b_0x^m + b_1x^{m-1} + \dots + b_m$  из кольца  $A[x]$ , причем  $a_0 \neq 0$  и  $b_0 \neq 0$ . Тогда произведение  $f(x)g(x)$  содержит ненулевой член  $a_0x^n \cdot b_0x^m = a_0b_0x^{n+m}$ , который будет, очевидно, высшим членом для  $f(x)g(x)$ , ибо остальные произведения членов  $f(x)$  на члены  $g(x)$  имеют меньшую чем  $n + m$  степень.

Отсюда непосредственно следует справедливость следующей важной теоремы:

**Теорема 1.** Если кольцо  $A$  есть область целостности, то кольцо полиномов  $A[x]$  — тоже область целостности.

В частности, кольцо полиномов над полем есть область целостности.

Из формы высшего члена произведения двух ненулевых полиномов следует, что степень произведения двух полиномов (над областью целостности) равна сумме степеней сомножителей. Это свойство сохраняется и в случае, когда один или оба сомножителя равны 0, если только условиться в правилах:  $(-\infty) + (-\infty) = -\infty$ ,  $(-\infty) + k = -\infty$  при любом  $k$ .

**3. Степени элемента в ассоциативном кольце.** Пусть  $B$  — некоторое ассоциативное кольцо и  $a$  — его элемент. Введем в рассмотрение степени  $a$  с натуральными показателями согласно следующим определениям:  $a^1 = a$ ,  $a^2 = a \cdot a$ ,  $a^3 = a^2 \cdot a$ , ...,  $a^k = a^{k-1} \cdot a$ . Здесь степени определяются одна за другой и  $k$ -я степень определяется после того, как  $(k-1)$ -я уже определена. Определения такого типа называются индуктивными.

**Теорема 2.** При натуральных  $k$  и  $m$  имеет место  $a^k a^m = a^{k+m}$ .

**Доказательство.** Если  $m = 1$ , утверждение теоремы верно согласно определению. При  $m > 1$  обратимся к методу математической индукции, допустив, что утверждение верно при сумме показателей, меньшей  $k + m$ . Итак, пусть  $m > 1$ . Тогда  $a^m = a^{m-1}a$  и  $a^k a^m = a^k (a^{m-1}a) = (a^k a^{m-1})a$  в силу ассоциативности. Далее,  $a^k a^{m-1} = a^{k+m-1}$  в силу индуктивного предположения и, наконец,  $(a^{k+m-1})a = a^{k+m}$  в силу определения степени, что и требовалось доказать.

Из теоремы следует, в частности, что  $a^3 = a^2 a = a a^2$ ,  $a^4 = a^3 a = a^2 a^2 = a a^3$ , и т. д.

Степени элемента  $a$  коммутируют при умножении, ибо  $a^k \cdot a^m = a^{k+m} = a^{m+k} = a^m \cdot a^k$ .

**4. Значение полинома.** Пусть  $B$  — ассоциативное кольцо, содержащее кольцо  $A$  в своем центре, т. е. элементы кольца  $A$  коммутируют со всеми элементами из  $B$ , и пусть единицей кольца  $B$

является единица кольца  $A$ . В частности, кольцо  $B$  может совпадать с кольцом  $A$ .

Пусть  $c \in B$  и пусть дан полином  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ . Значением полинома  $f$  в  $c$  (или, с некоторой вольностью языка, при  $x = c$ ) называется элемент

$$f(c) = a_0c^n + a_1c^{n-1} + \dots + a_n$$

кольца  $B$ .

Легко получаются следующие свойства:

$$\text{если } F(x) = f_1(x) + f_2(x), \text{ то } F(c) = f_1(c) + f_2(c)$$

и

$$\text{если } \Phi(x) = f_1(x) f_2(x), \text{ то } \Phi(c) = f_1(c) f_2(c).$$

Действительно, для одночленов это очевидно, а действия над полиномами определяются через действия над составляющими их одночленами.

Из сказанного следует, что значения полиномов из  $A[x]$  в одном и том же элементе  $c \in B$  коммутируют при умножении, и их множество, обозначаемое через  $A[c]$ , есть коммутативное подкольцо ассоциативного, но не обязательно коммутативного кольца  $B$ .

**5. Схема Хорнера и теорема Безу.** Если для полиномов  $f(x)$  и  $g(x)$  из  $A[x]$  существует такой полином  $h(x) \in A[x]$ , что  $f(x) = g(x)h(x)$ , то говорят, что полином  $f(x)$  делится на полином  $g(x)$ . Наша ближайшая задача заключается в выяснении вопроса о делимости  $f(x) \in A[x]$  на линейный двучлен  $x - c$  при  $c \in A$ .

Прежде всего установим, что всегда осуществимо так называемое деление с остатком:  $f(x) = (x - c)h(x) + r$  при  $r \in A$ . Здесь полином  $h(x)$  называется *неполным частным*, а  $r$  — *остатком*.

**Теорема 3.** Пусть  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \in A[x]$  и  $c \in A$ . Найдутся полином  $h(x) \in A[x]$  и элемент  $r \in A$  такие, что  $f(x) = (x - c)h(x) + r$ .

**Доказательство.** Естественно искать  $h(x)$  в форме  $b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$ . Сравнение коэффициентов показывает равносильность равенства  $a_0x^n + a_1x^{n-1} + \dots + a_n = (x - c)(b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}) + r$  цепочке равенств

$$a_0 = b_0,$$

$$a_1 = b_1 - cb_0,$$

$$a_2 = b_2 - cb_1,$$

$$\dots \dots \dots$$

$$a_{n-1} = b_{n-1} - cb_{n-2},$$

$$a_n = r - cb_{n-1},$$

откуда последовательно определяются коэффициенты  $h(x)$  и остаток  $r$ :

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + cb_0, \\ b_2 &= a_2 + cb_1, \\ &\dots \dots \dots \\ b_{n-1} &= a_{n-1} + cb_{n-2}, \\ r &= a_n + cb_{n-1}. \end{aligned}$$

Теорема доказана. Кроме того, получен очень удобный способ вычисления коэффициентов  $h(x)$  и остатка  $r$ . Этот способ носит название *схемы Хорнера*.

Заметим сразу, что остаток  $r$  равен значению  $f(c)$  полинома  $f(x)$  при  $x=c$ . Действительно, переходя в равенстве  $f(x) = (x-c)h(x) + r$  к значениям при  $x=c$ , получим  $f(c) = (c-c)h(c) + r$ , откуда  $r = f(c)$ .

**Пример.** Найти неполное частное и остаток при делении полинома  $x^5$  на  $x-2$ .

Выпишем последовательно коэффициенты полинома  $x^5$  и, после вертикальной черты, число 2:

$$1 \ 0 \ 0 \ 0 \ 0 \ 0 | 2.$$

Под этой строкой запишем коэффициенты неполного частного и остаток, пользуясь только что выведенными формулами:

$$\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 1 & 2 & 4 & 8 & 16 & 32 & \end{array}$$

(остаток — подчеркнутое число). Итак,

$$x^5 = (x-2)(x^4 + 2x^3 + 4x^2 + 8x + 16) + 32.$$

**Теорема 4 (Безу).** Для того чтобы полином  $f(x) \in A[x]$  делился на  $x-c$ , необходимо и достаточно, чтобы  $f(c) = 0$ .

**Доказательство.** Необходимость. Пусть  $f(x)$  делится на  $x-c$ , т. е.  $f(x) = (x-c)h(x)$ . Тогда  $f(c) = 0$ .

**Достаточность.** Пусть  $f(c) = 0$ . Тогда в равенстве  $f(x) = (x-c)h(x) + r$  будет  $r = f(c) = 0$ , т. е.  $f(x) = (x-c)h(x)$ . Теорема доказана полностью.

Элемент  $c$  кольца  $A$  называется *корнем* полинома  $f(x)$ , если  $f(c) = 0$ . Таким образом, теорема Безу может быть сформулирована так: для того чтобы полином  $f(x) \in A[x]$  делился на двучлен  $x-c$  при  $c \in A$ , необходимо и достаточно, чтобы  $c$  было корнем  $f(x)$ .

**6. Число корней полинома в коммутативной области целостности.**

**Лемма.** В области целостности возможно сокращение в равенстве, т. е. из  $ab = ac$  при  $a \neq 0$  следует  $b = c$ .

Действительно, равенство  $ab = ac$  равносильно равенству  $a(b - c) = 0$ . Так как  $a \neq 0$  и мы оперируем в области целостности, должно быть  $b - c = 0$ , т. е.  $b = c$ .

**Теорема 5.** Пусть  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  — полином из  $A[x]$ , где  $A$  — (коммутативная) область целостности. Тогда число корней  $f(x)$  в  $A$  не превосходит его степени  $n$ .

**Доказательство.** Применим метод математической индукции по степени полинома. База для индукции имеется — полином  $a_0 \neq 0$  нулевой степени не имеет корней. Допустим, что  $n \geq 1$  и что теорема доказана для полиномов степени  $n-1$ , и в этом предположении докажем ее для полинома  $f(x)$  степени  $n$ . Если  $f(x)$  не имеет корней в  $A$ , то утверждение теоремы верно. Пусть корни есть и  $c_1$  — один из корней. Тогда

$$f(x) = (x - c_1)h(x), \text{ где } h(x) = a_0x^{n-1} + b_1x^{n-2} + \dots$$

$$\dots + b_{n-1} \in A[x].$$

Если  $c_2$  — какой-либо корень  $f(x)$ , отличный от  $c_1$ , то  $0 = f(c_2) = (c_2 - c_1)h(c_2)$ , но  $c_2 - c_1 \neq 0$ , следовательно,  $h(c_2) = 0$ . Таким образом, любой корень  $f(x)$ , кроме  $c_1$ , является корнем полинома  $h(x)$  степени  $n-1$ . В силу индуктивного предположения этот полином имеет не более  $n-1$  корней в  $A$  и, следовательно,  $f(x)$  имеет не более  $n$  корней, что и требовалось доказать.

Заметим, что предположение о том, что кольцо  $A$  есть область целостности, здесь существенно. Так, в кольце вычетов по модулю 8 полином  $x^2 - 1$  имеет 4 корня: 1, 3, 5, 7.

**7. Теорема о тождестве.** Пусть, по-прежнему,  $A$  — коммутативная область целостности и  $A[x]$  — кольцо полиномов над  $A$ .

**Теорема 6** (о тождестве). Если  $A$  содержит бесконечно много элементов, то два полинома  $f_1(x)$  и  $f_2(x)$ , принимающие одинаковые значения при всех  $c \in A$ , равны.

**Доказательство.** Допустим, что разность  $F(x) = f_1(x) - f_2(x)$  отлична от нуля, так что  $F(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  при  $a_0 \neq 0$ . Возьмем попарно различные элементы  $c_1, c_2, \dots, c_{n+1}$  кольца  $A$ . Тогда, в силу условия теоремы,  $f_1(c_1) = f_2(c_1)$ ,  $f_1(c_2) = f_2(c_2)$ ,  $\dots$ ,  $f_1(c_{n+1}) = f_2(c_{n+1})$ , так что полином  $n$ -й степени  $F(x)$  имеет более чем  $n$  корней:  $c_1, c_2, \dots, c_{n+1}$ . Это невозможно. Следовательно,  $F(x) = 0$  и  $f_1(x) = f_2(x)$ , что и требовалось доказать.

Здесь было существенно, что кольцо  $A$  имеет бесконечно много элементов. Так, если  $A = \text{GF}(5)$  есть поле вычетов по модулю 5 и  $f_1(x) = x^5 + x^4 + 2x^2 + x + 1$ ,  $f_2(x) = x^4 + 2x^2 + 2x + 1$  — полиномы из  $A[x]$ , то  $f_1(0) = f_2(0) = 1$ ,  $f_1(1) = f_2(1) = 1$ ,  $f_1(2) = f_2(2) = 4$ ,  $f_1(3) = f_2(3) = 1$ ,  $f_1(4) = f_2(4) = 2$ . Полиномы  $f_1(x)$  и  $f_2(x)$  принимают одинаковые значения при всех элементах кольца  $A$ , и тем не менее они различны. Их разность  $x^5 - x$  есть отличный от нуля полином, все значения которого в  $A$  равны 0.

**8. Алгебраически замкнутое поле.** Поле  $K$  называется алгебраически замкнутым, если любой полином  $f(x) \in K[x]$  выше чем

нулевой степени имеет по крайней мере один корень в поле  $K$ . В дальнейшем будет доказана так называемая «основная теорема алгебры», утверждающая, что любой полином с комплексными коэффициентами имеет по крайней мере один комплексный корень. Иными словами, основная теорема алгебры утверждает, что поле  $\mathbb{C}$  комплексных чисел алгебраически замкнуто. По существу, эта теорема принадлежит скорее к математическому анализу, чем к алгебре, так как для ее доказательства нужно привлечение средств анализа. Она будет доказана в гл. IX.

Другие знакомые нам поля не замкнуты алгебраически. Так, в поле  $\mathbb{Q}$  рациональных чисел полином  $x^2 - 2$  не имеет корней, в поле  $\mathbb{R}$  действительных чисел не имеет корней полином  $x^2 + 2$ . Нетрудно установить, что поля  $\text{GF}(p)$  вычетов по простым модулям тоже не алгебраически замкнуты.

**Теорема 7.** *В алгебраически замкнутом поле любой полином  $a_0x^n + a_1x^{n-1} + \dots + a_n$ ,  $a_0 \neq 0$ ,  $n \geq 1$ , имеет разложение на линейные множители вида  $a_0(x - c_1)(x - c_2) \dots (x - c_n)$ , и такое разложение единственно.*

**Доказательство.** Оба утверждения теоремы будем доказывать методом математической индукции по степени полинома.

Начнем с доказательства возможности разложения. Полином первой степени  $a_0x + a_1$  при  $a_0 \neq 0$  в любом поле имеет корень  $c = -\frac{a_1}{a_0}$ , и  $a_0x + a_1 = a_0(x - c)$ .

Пусть теперь  $n > 1$ . В силу алгебраической замкнутости  $f(x)$  имеет по крайней мере один корень  $c_1 \in k$  и, следовательно,  $f(x) = (x - c_1)f_1(x)$ , где  $f_1(x) = a_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$  — полином  $(n-1)$ -й степени. В силу индуктивного предположения  $f_1(x) = a_0(x - c_2) \dots (x - c_n)$ , откуда  $f(x) = a_0(x - c_1)(x - c_2) \dots (x - c_n)$ .

Теперь докажем единственность разложения, снова по индукции. При  $n = 1$  она очевидна: если  $a_0x + a_1 = a_0(x - c) = a_0(x - c')$ , то  $a_0(c' - c) = 0$ , откуда  $c' = c$ , ибо  $a_0 \neq 0$ .

Пусть теперь  $n > 1$  и имеются два разложения:  $f(x) = a_0(x - c_1)(x - c_2) \dots (x - c_n) = a_0(x - c'_1)(x - c'_2) \dots (x - c'_n)$ . Положив  $x = c_1$ , получим

$$f(c_1) = 0 = a_0(c_1 - c'_1)(c_1 - c'_2) \dots (c_1 - c'_n).$$

Из равенства нулю произведения заключаем о равенстве нулю одного из сомножителей. Так как  $a_0 \neq 0$ , должен обращаться в нуль один из следующих сомножителей и, без нарушения общности, можно считать, что  $c_1 - c'_1 = 0$ , иначе можно изменить нумерацию элементов  $c'_1, c'_2, \dots, c'_n$ . Итак,  $c'_1 = c_1$  и

$$a_0(x - c_1)(x - c_2) \dots (x - c_n) = a_0(x - c_1)(x - c'_2) \dots (x - c'_n).$$

Так как кольцо полиномов над полем есть область целостности, можно сократить обе части равенства на  $x - c_1$ . Получим

$$a_0(x - c_2) \dots (x - c_n) = a_0(x - c'_2) \dots (x - c'_n).$$

В силу индуктивного предположения эти разложения совпадают. Следовательно, совпадают и исходные разложения  $f(x)$ . Теорема доказана полностью.

Среди сомножителей в разложении

$$f(x) = a_0(x - c_1)(x - c_2) \dots (x - c_n)$$

могут быть равные. Соединив их в виде степеней, получим разложение в виде

$$f(x) = a_0(x - c_1)^{m_1} \dots (x - c_k)^{m_k},$$

где  $c_1, \dots, c_k$  уже попарно различны.

Ясно, что  $c_1, \dots, c_k$  являются корнями полинома  $f(x)$  и других корней  $f(x)$  в поле  $K$  не имеет. Показатели  $m_1, \dots, m_k$  называются *кратностями* соответствующих корней.

Корни кратности 1 называются *простыми* корнями, корни кратности 2 — *двойными* или *двукратными*, и т. д.

Из последней формы разложения полинома на линейные множители следует, что *в алгебраически замкнутом поле число корней полинома равно его степени, если условиться считать каждый корень столько раз, какова его кратность.*

## § 2. Алгебраическое решение уравнений третьей и четвертой степени

Этот параграф имеет скорее историческое, чем научное значение. Правила решений алгебраических уравнений первой и второй степени были известны еще в античные времена. Для уравнений более высоких степеней были известны лишь некоторые приемы решения уравнений частных видов. В 16-м веке в Италии несколькими математиками одновременно был открыт способ алгебраического решения кубических уравнений. Он был опубликован не первооткрывателем метода, но выдающимся разносторонним ученым Кардано, имя которого известно теперь каждому автомобилисту и трактористу, так как Кардано изобрел простое и практичное приспособление для передачи вращения с одного вала на другой, не жестко скрепленный с первым. Ученики Кардано обнаружили, что решение общего уравнения четвертой степени можно свести к решению кубического уравнения и нескольких квадратных.

1. Алгебраическое решение уравнений третьей степени. Общее кубическое уравнение имеет вид

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0.$$

Мы будем считать, что коэффициенты — комплексные числа, и задача состоит в отыскании комплексных корней. Без нарушения общности можно считать, что  $a_0 = 1$ , ибо  $a_0 \neq 0$  и на него можно поделить обе части уравнения. Сделаем замену  $x = y - \frac{a_1}{3}$ . Получим  $(y - \frac{a_1}{3})^3 + a_1(y - \frac{a_1}{3})^2 + a_2(y - \frac{a_1}{3}) + a_3 = 0$  и, раскрывая скобки и приведя подобные члены, придем к уравнению

$$y^3 + \left(a_2 - \frac{a_1^2}{3}\right)y + \left(a_3 - \frac{a_1 a_2}{3} + \frac{2}{27}a_1^3\right) = 0.$$

Обозначив  $a_2 - \frac{a_1^2}{3} = p$ ,  $a_3 - \frac{a_1 a_2}{3} + \frac{2}{27}a_1^3 = q$ , придем к уравнению

$$y^3 + py + q = 0.$$

Для дальнейшего исследования нужна следующая элементарная лемма: существует пара чисел  $\alpha$  и  $\beta$  с наперед заданными суммой  $\alpha + \beta = a$  и произведением  $\alpha\beta = b$ . Именно, эти числа являются корнями квадратного уравнения  $z^2 - az + b = 0$ .

Положим теперь  $y = \alpha + \beta$ . Уравнение примет вид  $\alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 + p(\alpha + \beta) + q = 0$  или  $\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0$ .

Положим  $3\alpha\beta + p = 0$ . Тогда  $\alpha^3 + \beta^3 + q = 0$ . Ясно, что если  $\alpha^3 + \beta^3 + q = 0$  и  $3\alpha\beta + p = 0$ , то  $y = \alpha + \beta$  будет удовлетворять уравнению  $y^3 + py + q = 0$ . Таким образом, нам нужно решить систему

$$\alpha^3 + \beta^3 = -q,$$

$$3\alpha\beta = -p.$$

Возведем второе уравнение в куб:  $\alpha^3\beta^3 = -\frac{p^3}{27}$ . Мы получили, что для  $\alpha^3$  и  $\beta^3$  известны сумма и произведение. Поэтому числа  $\alpha^3$  и  $\beta^3$  находятся как корни квадратного уравнения

$$z^2 + qz - \frac{p^3}{27} = 0,$$

откуда

$$\alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad \beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

и

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Для  $y$  получается так называемая *формула Кардано*:

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Для каждого из кубических корней в поле комплексных чисел имеются три значения и для обоих корней имеется девять комбинаций. Однако из них нужно сохранить только те, для которых  $\alpha\beta = -\frac{p}{3}$ , т. е. брать  $\beta = -\frac{p}{3\alpha}$ . Обозначим через  $\omega_1$  и  $\omega_2$  первообразные кубические корни из 1, т. е.  $\omega_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ,  $\omega_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ . Пусть  $\alpha_1$  и  $\beta_1$  — одна подходящая пара значений для  $\alpha$  и  $\beta$ . Остальные значения для  $\alpha$  будут  $\alpha_1\omega_1$  и  $\alpha_1\omega_2$ , соответствующие значения для  $\beta$  будут  $\beta_1\omega_2$  и  $\beta_1\omega_1$ . Поэтому формула Кардано дает три корня уравнения:

$$y_1 = \alpha_1 + \beta_1,$$

$$y_2 = \alpha_1\omega_1 + \beta_1\omega_2,$$

$$y_3 = \alpha_1\omega_2 + \beta_1\omega_1.$$

Пример 1.  $y^3 + (3 - 3i)y + (-2 + i) = 0$ .

$$\begin{aligned} y &= \sqrt[3]{1 - \frac{i}{2}} + \sqrt{\left(1 - \frac{i}{2}\right)^2 + (1 - i)^3} + \\ &+ \sqrt[3]{1 - \frac{i}{2}} - \sqrt{\left(1 - \frac{i}{2}\right)^2 + (1 - i)^3} = \\ &= \sqrt[3]{1 - \frac{i}{2}} + \sqrt{-\frac{5}{4} - 3i} + \sqrt[3]{1 - \frac{i}{2}} - \sqrt{-\frac{5}{4} - 3i} = \\ &= \sqrt[3]{1 - \frac{i}{2} + \left(\frac{3}{2}i - 1\right)} + \sqrt[3]{1 - \frac{i}{2} - \left(\frac{3}{2}i - 1\right)} = \\ &= \sqrt[3]{i} + \sqrt[3]{2 - 2i}. \end{aligned}$$

При извлечении кубических корней нужно помнить, что их произведение должно равняться  $-\frac{p}{3} = -1 + i$ . Поэтому, взяв для первого корня значение  $-i$ , для второго нужно взять  $-1 - i$ .

Корни данного уравнения суть:

$$y_1 = -i + (-1 - i) = -1 - 2i,$$

$$y_2 = -i\omega_1 + (-1 - i)\omega_2 = \frac{1}{2} + \left(\frac{\sqrt{3}}{2} + 1\right)i,$$

$$y_3 = -i\omega_2 + (-1 - i)\omega_1 = \frac{1}{2} + \left(-\frac{\sqrt{3}}{2} + 1\right)i.$$

Пример 2.  $y^3 - 9y + 28 = 0$ .

$$\begin{aligned} y &= \sqrt[3]{-14} + \sqrt{14^2 - 3^3} + \sqrt[3]{-14 - \sqrt{14^2 - 3^3}} = \\ &= \sqrt[3]{-14 + 13} + \sqrt[3]{-14 - 13} = \sqrt[3]{-1} + \sqrt[3]{-27}. \end{aligned}$$

Нужно помнить, что произведение кубических корней должно равняться  $-\frac{p}{3}=3$ , так что, взяв для первого корня значение  $-1$ , для второго нужно взять  $-3$ . Корни данного уравнения суть:

$$y_1 = -1 - 3 = -4,$$

$$y_2 = -\omega_1 - 3\omega_2 = 2 + i\sqrt{3},$$

$$y_3 = -\omega_2 - 3\omega_1 = 2 - i\sqrt{3}.$$

Данный пример решился очень благополучно, что является скорее исключением, чем правилом, как будет видно из дальнейшего исследования.

**2. Исследование формулы Кардано.** Проведем исследование формулы Кардано в предположении, что коэффициенты  $p$  и  $q$  уравнения  $y^3 + py + q = 0$  являются действительными числами.

Из вида формулы

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

ясно, что знак выражения  $\frac{q^2}{4} + \frac{p^3}{27}$  должен оказывать существенное влияние на характер корней уравнения. Рассмотрим три случая.

**Случай 1.**  $\frac{q^2}{4} + \frac{p^3}{27} > 0$ . В этом случае числа  $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  и  $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  оба действительные и они различны. Если значение  $\alpha_1$  первого кубического корня взято действительным, то и для второго корня нужно взять тоже действительное значение  $\beta_1$ , так как их произведение должно быть действительным числом  $-\frac{p}{3}$ . Таким образом, в этом случае корни будут

$$y_1 = \alpha_1 + \beta_1,$$

$$y_2 = \alpha_1\omega_1 + \beta_1\omega_2 = -\frac{\alpha_1 + \beta_1}{2} + \frac{\alpha_1 - \beta_1}{2}i\sqrt{3},$$

$$y_3 = \alpha_1\omega_2 + \beta_1\omega_1 = -\frac{\alpha_1 + \beta_1}{2} - \frac{\alpha_1 - \beta_1}{2}i\sqrt{3}.$$

Следовательно,  $y_1$  — действительный корень,  $y_2$  и  $y_3$  — комплексно сопряженные не действительные корни, ибо  $\alpha_1 \neq \beta_1$ .

**Случай 2.**  $\frac{q^2}{4} + \frac{p^3}{27} = 0$ . В этом случае числа  $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  и  $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  действительные, но равные. Действительному значению  $\alpha_1$  первого кубического корня должно соответствовать действительное же значение  $\beta_1$  второго, и на этот раз  $\alpha_1 = \beta_1$ . Комплексные же значения кубических корней нужно

подбирать по прежнему правилу, обеспечивающему равенство  $\alpha\beta = -\frac{p}{3}$ .

$$\begin{aligned}\text{Итак:} \quad y_1 &= \alpha_1 + \beta_1 = 2\alpha_1, \\ y_2 &= \alpha_1\omega_1 + \beta_1\omega_2 = -\alpha_1, \\ y_3 &= \alpha_1\omega_2 + \beta_1\omega_1 = -\alpha_1.\end{aligned}$$

В этом случае все три корня действительны, но среди них имеются два равных.

Случай 3.  $\frac{q^2}{4} + \frac{p^3}{27} < 0$ . Это возможно только при отрицательном  $p$ . Пусть  $p = -p_1$ , где  $p_1 > 0$ . В этом случае под знаками кубических корней окажутся сопряженные комплексные числа  $-\frac{q}{2} + i\sqrt{\frac{p_1^3}{27} - \frac{q^2}{4}}$  и  $-\frac{q}{2} - i\sqrt{\frac{p_1^3}{27} - \frac{q^2}{4}}$ .

Для извлечения кубического корня запишем число  $-\frac{q}{2} + i\sqrt{\frac{p_1^3}{27} - \frac{q^2}{4}}$  в тригонометрической форме:  $r(\cos \varphi + i \sin \varphi)$ . Имеем:

$$r^2 = \left(-\frac{q}{2}\right)^2 + \left(\sqrt{\frac{p_1^3}{27} - \frac{q^2}{4}}\right)^2 = \frac{p_1^3}{27}, \quad \cos \varphi = -\frac{q}{2r}, \quad \sin \varphi > 0.$$

Отсюда  $r = \sqrt[3]{\frac{p_1^3}{27}}$  и

$$\begin{aligned}\alpha &= \sqrt[3]{-\frac{q}{2} + i\sqrt{\frac{p_1^3}{27} - \frac{q^2}{4}}} = r^{\frac{1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} + i \sin \frac{\varphi + 2k\pi}{3} \right) = \\ &= \sqrt[3]{\frac{p_1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} + i \sin \frac{\varphi + 2k\pi}{3} \right),\end{aligned}$$

где  $k = 0, 1, 2$ . В этом случае  $\alpha\beta = \frac{p_1}{3}$ , откуда

$$\begin{aligned}\beta &= \frac{\frac{p_1}{3}}{\sqrt[3]{\frac{p_1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} + i \sin \frac{\varphi + 2k\pi}{3} \right)} = \\ &= \sqrt[3]{\frac{p_1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} - i \sin \frac{\varphi + 2k\pi}{3} \right).\end{aligned}$$

Таким образом,  $\beta$  оказывается числом, сопряженным с  $\alpha$ , в чем можно было убедиться из того соображения, что произведение  $\alpha\beta$  должно равняться действительному числу  $\frac{p_1}{3} = |\alpha|^2$ .

Итак,

$$y = \sqrt{\frac{p_1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} + i \sin \frac{\varphi + 2k\pi}{3} \right) + \\ + \sqrt{\frac{p_1}{3}} \left( \cos \frac{\varphi + 2k\pi}{3} - i \sin \frac{\varphi + 2k\pi}{3} \right) = 2 \sqrt{\frac{p_1}{3}} \cos \frac{\varphi + 2k\pi}{3},$$

где  $k = 0, 1, 2$ .

Все три корня оказываются действительными и, как нетрудно видеть, попарно различными. Интересно отметить, что в этом, казалось бы, самом лучшем (в смысле действительности корней) случае комплексные числа появляются по существу, и это было одним из стимулов введения комплексных чисел в математику.

Рассмотрим еще примеры.

Пример 3.  $y^3 - 9y + 8 = 0$ . Здесь имеется бросающийся в глаза корень  $y = 1$ . Посмотрим, что дает формула Кардано

$$y = \sqrt[3]{-4 + \sqrt{16 - 27}} + \sqrt[3]{-4 - \sqrt{16 - 27}} = \\ = \sqrt[3]{-4 + i\sqrt{11}} + \sqrt[3]{-4 - i\sqrt{11}}.$$

Ничего похожего на число 1 мы не видим. Однако если знать, что  $-4 + i\sqrt{11} = \left( \frac{1 - i\sqrt{11}}{2} \right)^3$  (о чем нетрудно догадаться, заранее зная, что исходное уравнение имеет корень 1), то получим

$$y_1 = \frac{1 - i\sqrt{11}}{2} + \frac{1 + i\sqrt{11}}{2} = 1, \\ y_2 = \frac{1 - i\sqrt{11}}{2} \omega_1 + \frac{1 + i\sqrt{11}}{2} \omega_2 = -\frac{1}{2} + \frac{\sqrt{33}}{2}, \\ y_3 = \frac{1 - i\sqrt{11}}{2} \omega_2 + \frac{1 + i\sqrt{11}}{2} \omega_1 = -\frac{1}{2} - \frac{\sqrt{33}}{2}.$$

В случае, когда все три корня вещественны, можно доказать, что при алгебраическом решении уравнения третьей степени извлечение кубического корня из комплексного числа неизбежно.

Однако и в первом случае, когда нет необходимости в действии извлечения кубического корня из комплексного числа, как правило, «хорошие» корни, если они есть, формула Кардано преподносит «под маской». Благополучный пример, типа приведенного выше примера 2, является исключением.

Рассмотрим еще один пример.

Пример 4.  $x^3 + 3x - 4 = 0$ . Здесь снова «светится» корень  $x = 1$ . Формула Кардано дает:

$$x = \sqrt[3]{2 + \sqrt{4 + 1}} + \sqrt[3]{2 - \sqrt{4 + 1}} = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}.$$

Правда, и здесь можно «снять маску», если знать, что  $2 + \sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^3$  и  $2 - \sqrt{5} = \left(\frac{1-\sqrt{5}}{2}\right)^3$ . Если принять это во внимание, получим

$$x_1 = \frac{1}{2} + \frac{1}{2} \sqrt{5} + \frac{1}{2} - \frac{1}{2} \sqrt{5} = 1,$$

$$x_2 = \left(\frac{1}{2} + \frac{1}{2} \sqrt{5}\right) \omega_1 + \left(\frac{1}{2} - \frac{1}{2} \sqrt{5}\right) \omega_2 = -\frac{1}{2} + \frac{i\sqrt{15}}{2},$$

$$x_3 = \left(\frac{1}{2} + \frac{1}{2} \sqrt{5}\right) \omega_2 + \left(\frac{1}{2} - \frac{1}{2} \sqrt{5}\right) \omega_1 = -\frac{1}{2} - \frac{i\sqrt{15}}{2}.$$

**3. Решение уравнений четвертой степени.** Вскоре после того, как Кардано опубликовал способ решения кубических уравнений, его ученики и последователи нашли способы сведения общего уравнения четвертой степени к кубическому уравнению. Изложим наиболее простой способ, принадлежащий Л. Феррари.

При изложении способа нужно будет воспользоваться следующей элементарной леммой.

**Лемма.** Для того чтобы квадратный трехчлен  $Ax^2 + Bx + C$  был квадратом линейного двучлена, необходимо и достаточно, чтобы его дискриминант  $B^2 - 4AC$  равнялся нулю.

**Доказательство.** Необходимость. Пусть  $Ax^2 + Bx + C = (kx + l)^2$ . Тогда  $A = k^2$ ,  $B = 2kl$ ,  $C = l^2$  и  $B^2 - 4AC = 0$ .

**Достаточность.** Пусть  $B^2 - 4AC = 0$ . Тогда  $Ax^2 + Bx + C = \left(\sqrt{A}x + \frac{B}{2\sqrt{A}}\right)^2 + C - \frac{B^2}{4A} = \left(\sqrt{A}x + \frac{B}{2\sqrt{A}}\right)^2 + \frac{4AC - B^2}{4A} = \left(\sqrt{A}x + \frac{B}{2\sqrt{A}}\right)^2$ .

Идея излагаемого способа состоит в том, чтобы представить левую часть уравнения  $x^4 + ax^3 + bx^2 + cx + d = 0$  в виде разности двух квадратов. Тогда ее можно будет разложить на два множителя второй степени, и решение уравнения приведет к решению двух квадратных уравнений. Для достижения цели левую часть представим в виде:

$$\begin{aligned} & \left(x^2 + \frac{a}{2}x + \frac{y}{2}\right)^2 - \frac{a^2}{4}x^2 - \frac{ayx}{2} - \frac{y^2}{4} - yx^2 + bx^2 + cx + d = \\ & = \left(x^2 + \frac{a}{2}x + \frac{y}{2}\right)^2 - \left[\left(\frac{a^2}{4} + y - b\right)x^2 + \left(\frac{ay}{2} - c\right)x + \left(\frac{y^2}{4} - d\right)\right]. \end{aligned}$$

Здесь  $y$  — вспомогательная неизвестная, которую нужно подобрать так, чтобы выражение в квадратных скобках оказалось квадратом линейного двучлена. В силу леммы для этого необходимо и достаточно выполнения условия

$$\left(\frac{ay}{2} - c\right)^2 - 4\left(\frac{a^2}{4} + y - b\right)\left(\frac{y^2}{4} - d\right) = 0.$$

Это условие есть уравнение третьей степени относительно  $y$ . После раскрытия скобок оно преобразуется к виду

$$y^3 - by^2 + (ac - 4d)y - (c^2 + a^2d - 4bd) = 0.$$

Пусть  $y_1$  — один из корней этого уравнения. Тогда при  $y = y_1$  условие будет выполнено, так что имеет место

$$\left(\frac{a^2}{4} + y_1 - b\right)x^2 + \left(\frac{ay_1}{2} - c\right)x + \left(\frac{y_1^2}{4} - d\right) = (kx + l)^2$$

при некоторых  $k$  и  $l$ . Исходное уравнение примет вид

$$\left(x^2 + \frac{a}{2}x + \frac{y_1}{2}\right)^2 - (kx + l)^2 = 0,$$

или

$$\left(x^2 + \frac{a}{2}x + \frac{y_1}{2} + kx + l\right)\left(x^2 + \frac{a}{2}x + \frac{y_1}{2} - kx - l\right) = 0.$$

Приравнявая нулю каждый из сомножителей, мы найдем четыре корня исходного уравнения.

Сделаем еще одно замечание. Пусть  $x_1$  и  $x_2$  — корни первого сомножителя,  $x_3$  и  $x_4$  — корни второго. Тогда  $x_1x_2 = \frac{y_1}{2} + l$ ,  $x_3x_4 = \frac{y_1}{2} - l$ . Сложив эти равенства, получим, что  $y_1 = x_1x_2 + x_3x_4$ . Таким образом, мы получили выражение корня  $y_1$  вспомогательного кубического уравнения через корни исходного уравнения четвертой степени.

**Пример.** Решить уравнение  $x^4 + 2x^3 - 6x^2 - 5x + 2 = 0$ .

Согласно изложенному выше методу преобразуем левую часть:

$$\begin{aligned} x^4 + 2x^3 - 6x^2 - 5x + 2 &= \\ &= \left(x^2 + x + \frac{y}{2}\right)^2 - yx^2 - x^2 - xy - \frac{y^2}{4} - 6x^2 - 5x + 2 = \\ &= \left(x^2 + x + \frac{y}{2}\right)^2 - \left[(y+7)x^2 + (y+5)x + \left(\frac{y^2}{4} - 2\right)\right]. \end{aligned}$$

Теперь положим  $(y+5)^2 - 4(y+7)\left(\frac{y^2}{4} - 2\right) = 0$ . После преобразований получим уравнение

$$y^3 + 6y^2 - 18y - 81 = 0.$$

Легко видеть, что одним из корней этого уравнения является число  $y_1 = -3$ . Подставив его в преобразованную левую часть исходного уравнения, получим:

$$\begin{aligned} x^4 + 2x^3 - 6x^2 - 5x + 2 &= \left(x^2 + x - \frac{3}{2}\right)^2 - \left[4x^2 + 2x + \frac{1}{4}\right] = \\ &= \left(x^2 + x - \frac{3}{2}\right)^2 - \left(2x + \frac{1}{2}\right)^2 = (x^2 + 3x - 1)(x^2 - x - 2). \end{aligned}$$

Приравнивая сомножители нулю, получим

$$x_1 = \frac{-3 + \sqrt{13}}{2}, \quad x_2 = \frac{-3 - \sqrt{13}}{2}, \quad x_3 = 2, \quad x_4 = -1.$$

Что касается уравнений выше четвертой степени, то здесь были известны некоторые классы уравнений сравнительно частного вида, допускающих алгебраические решения в радикалах, т. е. в виде результатов арифметических действий и действия извлечения корня. Однако попытки дать решение общих уравнений пятой степени и выше были безуспешны, пока, наконец, в начале 19 в. Руффини и Абель не доказали, что решение такого рода для общих уравнений выше четвертой степени невозможно. Наконец, в 1830 г. гениальному французскому математику Э. Галуа удалось найти необходимые и достаточные условия (проверяемые довольно сложно) для разрешимости в радикалах конкретно заданного уравнения. При этом Галуа создал и использовал новую для своего времени теорию групп подстановок.

### § 3. Полиномы от нескольких букв

**1. Определение и основные действия.** Пусть дано коммутативное кольцо  $A$  с единицей и несколько посторонних для  $A$  букв  $x_1, \dots, x_m$ . *Одночленом* относительно этих букв называется выражение  $ax_1^{k_1} \dots x_m^{k_m}$ , где  $a \in A$ ,  $k_1, \dots, k_m$  — целые неотрицательные числа. Показатели  $k_1, \dots, k_m$  называются степенями одночлена относительно соответствующих букв, а  $k_1 + \dots + k_m$  называется полной степенью или просто *степенью* одночлена. Для подобных одночленов  $ax_1^{k_1} \dots x_m^{k_m}$  и  $bx_1^{k_1} \dots x_m^{k_m}$  определено сложение  $ax_1^{k_1} \dots x_m^{k_m} + bx_1^{k_1} \dots x_m^{k_m} = (a + b)x_1^{k_1} \dots x_m^{k_m}$  («приведение подобных членов») и определено умножение одночленов:

$$ax_1^{k_1} \dots x_m^{k_m} \cdot bx_1^{l_1} \dots x_m^{l_m} = abx_1^{k_1+l_1} \dots x_m^{k_m+l_m}.$$

*Многочленом* или *полиномом* называется формальная сумма одночленов, причем порядок слагаемых безразличен.

Максимальная из степеней одночленов, составляющих полином, называется его *степенью*. Полином, все члены которого имеют одинаковую степень, называется *однородным* полиномом или *формой*. Максимальная из степеней относительно какой-нибудь буквы называется степенью полинома относительно этой буквы.

Два полинома считаются *равными*, если они составлены из одинаковых одночленов. Для полиномов естественным образом определяются действия сложения и умножения. Именно, *сумма* двух полиномов составлена из объединения всех одночленов, составляющих слагаемые; *произведение* есть сумма произведений всех членов первого сомножителя на все члены второго. Полиномы

образуют ассоциативное и коммутативное кольцо, обозначаемое  $A[x_1, \dots, x_m]$ .

Ясно, что полином от букв  $x_1, \dots, x_m$  можно рассматривать как полином от  $x_1$  с коэффициентами, являющимися полиномами от остальных букв.

**Теорема 1.** *Кольцо полиномов от нескольких букв над областью целостности есть область целостности.*

**Доказательство.** Применяем метод математической индукции по числу букв. База индукции имеется — для полиномов от одной буквы теорема была установлена в п. 2 § 1. Положим теперь, что кольцо полиномов от  $m-1$  букв есть область целостности. Тогда и кольцо полиномов от  $m$  букв есть область целостности, ибо оно есть кольцо полиномов от одной буквы над кольцом полиномов от  $m-1$  букв, которое есть область целостности по индуктивному предположению.

**2. Значения полиномов от нескольких букв.** Пусть  $B$  — ассоциативное коммутативное кольцо (для полиномов от одной переменной коммутативность  $B$  была не обязательна), содержащее  $A$ , и с единицей, совпадающей с единицей  $A$ . Пусть дан полином

$$F(x_1, \dots, x_m) = \sum a_{k_1, \dots, k_m} x_1^{k_1} \dots x_m^{k_m} \in A[x_1, \dots, x_m]$$

и даны  $b_1, \dots, b_m \in B$ . Значением полинома  $F(x_1, \dots, x_m)$  в точке  $(b_1, \dots, b_m)$  (или при  $x_1 = b_1, \dots, x_m = b_m$ ) называется

$$F(b_1, \dots, b_m) = \sum a_{k_1, \dots, k_m} b_1^{k_1} \dots b_m^{k_m} \in B.$$

Ясно, что если  $H(x_1, \dots, x_m) = F_1(x_1, \dots, x_m) + F_2(x_1, \dots, x_m)$  и  $G(x_1, \dots, x_m) = F_1(x_1, \dots, x_m) \cdot F_2(x_1, \dots, x_m)$ , то

$$H(b_1, \dots, b_m) = F_1(b_1, \dots, b_m) + F_2(b_1, \dots, b_m)$$

и

$$G(b_1, \dots, b_m) = F_1(b_1, \dots, b_m) \cdot F_2(b_1, \dots, b_m).$$

**3. Теорема о тождестве.** Если  $A$  — область целостности, содержащая бесконечно много элементов, то верна следующая теорема о тождестве.

**Теорема 2.** *Если два полинома  $F_1(x_1, \dots, x_m)$  и  $F_2(x_1, \dots, x_m)$  равны тождественно в  $A$  (т. е. принимают одинаковые значения при одинаковых наборах значений букв), то они равны формально.*

Для доказательства достаточно установить справедливость леммы:

**Лемма.** *Если полином  $H(x_1, \dots, x_m) \in A[x_1, \dots, x_m]$  тождественно равен нулю в  $A$  (т. е. все его значения равны нулю), то он равен нулю формально.*

Действительно, достаточно перейти от многочленов  $F_1$  и  $F_2$  к их разности  $H = F_1 - F_2$ .

**Доказательство леммы.** Мы докажем равносильное лемме предложение: *если полином  $H$  формально отличен от нуля, то найдутся значения  $x_1^*, \dots, x_m^*$  для букв  $x_1, \dots, x_m$ , при которых  $H$  принимает значение, отличное от нуля.*

Применим метод математической индукции по числу букв  $m$ . При  $m = 1$  теорема была доказана. Пусть  $m > 1$ ,  $H(x_1, \dots, x_m) \neq 0$ . Запишем  $H(x_1, \dots, x_m)$  как полином от  $x_1$  с коэффициентами из  $A[x_2, \dots, x_m]$ :

$$H(x_1, \dots, x_m) = \\ = a_0(x_2, \dots, x_m)x_1^n + a_1(x_2, \dots, x_m)x_1^{n-1} + \dots + a_n(x_2, \dots, x_m).$$

Можно считать, что  $a_0(x_2, \dots, x_m) \neq 0$ . В силу индуктивного предположения для  $x_2, \dots, x_m$  найдется набор значений  $x_2^*, \dots, x_m^*$  такой, что  $a_0^* = a_0(x_2^*, \dots, x_m^*) \neq 0$ . Тогда

$$H(x_1, x_2^*, \dots, x_m^*) = \\ = a_0(x_2^*, \dots, x_m^*)x_1^n + a_1(x_2^*, \dots, x_m^*)x_1^{n-1} + \dots + a_n(x_2^*, \dots, x_m^*) = \\ = a_0^*x_1^n + a_1^*x_1^{n-1} + \dots + a_n^*$$

при  $a_0^* \neq 0$ . В силу теоремы для  $m = 1$  найдется  $x_1^* \in A$  такое, что

$$H(x_1^*, x_2^*, \dots, x_m^*) = a_0^*x_1^{*n} + a_1^*x_1^{*(n-1)} + \dots + a_n^* \neq 0,$$

что и требовалось доказать.

#### 4. Теорема о несуществовании алгебраических неравенств.

**Теорема 3.** Пусть  $A$  — область целостности, содержащая бесконечно много элементов, и пусть  $F_1$  и  $F_2$  — два полинома из  $A[x_1, \dots, x_m]$ , принимающие одинаковые значения  $F_1(x_1^*, \dots, x_m^*) = F_2(x_1^*, \dots, x_m^*)$  всюду, где выполнены неравенства  $H_1(x_1^*, \dots, x_m^*) \neq 0, \dots, H_k(x_1^*, \dots, x_m^*) \neq 0$ , где  $H_1, \dots, H_k$  — некоторые отличные от нуля полиномы из  $A[x_1, \dots, x_m]$ . Тогда полиномы  $F_1$  и  $F_2$  равны формально.

**Доказательство.** Рассмотрим полином  $(F_1 - F_2)H_1 \dots H_k$ . Он равен нулю при всех наборах переменных, так как там, где  $H_1 \neq 0, \dots, H_k \neq 0$ , обращается в нуль первый множитель. В силу теоремы о тождестве  $(F_1 - F_2)H_1 \dots H_k = 0$  (формальное равенство). Но  $A[x_1, \dots, x_m]$  есть область целостности и  $H_1 \neq 0, \dots, H_k \neq 0$ . Следовательно,  $F_1 - F_2 = 0$ , т. е.  $F_1 = F_2$ , что и требовалось доказать.

Установленная теорема оказывается полезной в довольно часто встречающейся ситуации, когда равенство значений двух полиномов удастся установить в предположении о необращении в нуль одного или нескольких полиномов. В силу доказанной теоремы после установления равенства поставленные ограничения автоматически снимаются.

# МАТРИЦЫ И ОПРЕДЕЛИТЕЛИ

## § 1. Матрицы и действия над ними

**1. Определение матрицы.** *Матрицей* называется прямоугольная таблица, заполненная некоторыми математическими объектами. По большей части мы будем рассматривать матрицы с элементами из некоторого поля, хотя многие предложения сохраняют силу, если в качестве элементов матриц рассматривать элементы ассоциативного (не обязательно коммутативного) кольца.

Чаще всего элементы матрицы обозначаются одной буквой с двумя индексами, указывающими «адрес» элемента — первый индекс дает номер строки, содержащей элемент, второй — номер столбца. Таким образом, матрица (*размеров*  $m \times n$ ) записывается в форме

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Матрицы, составленные из чисел, естественно возникают при рассмотрении систем линейных уравнений

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1, \\ \dots & \dots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n &= b_n. \end{aligned}$$

Входные данные для этой задачи — это множество коэффициентов, естественно составляющих матрицу

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

и совокупность свободных членов, образующих матрицу  $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ ,

имеющую лишь один столбец. Искомым является набор значений неизвестных, который, как оказывается, удобно пред-



число называется *порядком* квадратной матрицы. Вместо того чтобы говорить «матрица, состоящая из одной строки», и «матрица, состоящая из одного столбца», говорят короче: *строка, столбец*.

2. **Сложение матриц и умножение матрицы на число.** Введем в рассмотрение алгебраические действия над матрицами. Рассматриваем матрицы с элементами из некоторого поля  $K$ . При этом две матрицы считаются *равными*, если у них совпадают элементы, стоящие на одинаковых местах.

Определим *произведение элемента*  $c \in K$  *на матрицу*  $A =$   
 $= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ :

$$cA \stackrel{\text{def}}{=} \begin{pmatrix} ca_{11} & \dots & ca_{1n} \\ \dots & \dots & \dots \\ ca_{m1} & \dots & ca_{mn} \end{pmatrix}$$

(для матриц над некоммутативным ассоциативным кольцом следует различать два произведения  $cA$  и  $Ac$ ).

Для матриц одинакового строения, т. е. имеющих одинаковое число строк и столбцов, определяется *сложение* по правилу: если

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{pmatrix},$$

то

$$A + B \stackrel{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \dots & \dots & \dots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix},$$

т. е. элементами *суммы* двух матриц является сумма соответствующих элементов слагаемых матриц.

Отметим некоторые свойства действий.

1.  $(A + B) + C = A + (B + C)$  — ассоциативность сложения.

2.  $A + B = B + A$  — коммутативность сложения.

3. Матрица 0, состоящая из нулей, играет роль нуля:  $A + 0 = A$  при любой  $A$ .

4. Для любой матрицы  $A$  существует противоположная  $-A$  такая, что  $A + (-A) = 0$ . (В качестве матрицы  $-A$ , очевидно, следует взять матрицу  $(-1)A$ , элементы которой отличаются от элементов  $A$  знаком.)

5.  $(c_1 + c_2)A = c_1A + c_2A$ .

6.  $c(A_1 + A_2) = cA_1 + cA_2$ .

7.  $c_1(c_2A) = (c_1c_2)A$ .

8.  $1 \cdot A = A$ .

Все перечисленные свойства непосредственно следуют из определений и свойств действий в поле (или в кольце).

Система математических объектов, в которой определено действие сложения и действие умножения на элементы поля  $K$ , причем



называется число  $a_1b_1 + a_2b_2 + \dots + a_nb_n$  (или элемент кольца, которому принадлежат элементы рассматриваемых матриц).

Для прямоугольных матриц  $A$  и  $B$  произведение определено, если длины строк первого сомножителя  $A$  равны длинам столбцов второго сомножителя  $B$ , т. е. если число столбцов  $A$  равно числу строк  $B$ . Именно, произведение  $AB$  матриц  $A$  и  $B$  составляется из произведений строк  $A$  на столбцы  $B$ , при их естественном расположении в матрицу. Точнее: произведением  $AB$  матрицы  $A$  на матрицу  $B$ , где

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kn} \end{pmatrix},$$

называется матрица  $C$ , элемент  $c_{ij}$   $i$ -й строки и  $j$ -го столбца которой равен произведению  $i$ -й строки  $A$  на  $j$ -й столбец  $B$ , т. е. равен сумме произведений элементов  $i$ -й строки матрицы  $A$  на элементы  $j$ -го столбца матрицы  $B$ . Таким образом,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj} = \sum_{\alpha=1}^k a_{i\alpha}b_{\alpha j}.$$

Рассмотрим примеры:

1.  $(1, 2) \begin{pmatrix} 3 \\ 4 \end{pmatrix} = 1 \cdot 3 + 2 \cdot 4 = 11.$
2.  $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 5 & 1 \cdot 2 + 2 \cdot 3 \\ 3 \cdot 1 + 4 \cdot 5 & 3 \cdot 2 + 4 \cdot 3 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 23 & 18 \end{pmatrix}.$
3.  $\begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 3 & 1 \cdot 2 + 2 \cdot 4 \\ 5 \cdot 1 + 3 \cdot 3 & 5 \cdot 2 + 3 \cdot 4 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 14 & 22 \end{pmatrix}.$

Последние два примера поучительны тем, что в них рассматриваются произведения одинаковых сомножителей, но в разных порядках. Результаты получились различными. Следовательно, свойство коммутативности при умножении даже квадратных матриц не имеет места.

Условие, когда произведение матриц определено, а также размеры произведения двух матриц удобно изобразить при помощи схематического рисунка:

$$\begin{array}{c} \begin{array}{c} k \\ \boxed{A} \\ m \end{array} \cdot \begin{array}{c} n \\ \boxed{B} \\ k \end{array} = \begin{array}{c} \boxed{AB} \\ n \\ m \end{array}$$

Ясно, что если определены произведения  $AB$  и  $BA$ , то число строк  $A$  равно числу столбцов  $B$  и число строк  $B$  — числу столбцов  $A$ . Оба произведения  $AB$  и  $BA$  будут квадратными матрицами, но разных размеров, если  $A$  и  $B$  не квадратные. Если  $A$  и  $B$



Таким образом,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj},$$

так что матрица коэффициентов в выражениях  $y_1, \dots, y_m$  через  $t_1, \dots, t_n$  действительно равна  $AB$ . Итак, последовательному проведению («суперпозиции») двух линейных подстановок соответствует произведение их матриц.

Заметим, что линейную подстановку

$$y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k,$$

$$y_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k,$$

$$\dots \dots \dots$$

$$y_m = a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mk}x_k$$

можно записать в матричных обозначениях  $Y = AX$ , где

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}, \quad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}.$$

Соответственно, подстановка

$$x_1 = b_{11}t_1 + b_{12}t_2 + \dots + b_{1n}t_n,$$

$$x_2 = b_{21}t_1 + b_{22}t_2 + \dots + b_{2n}t_n,$$

$$\dots \dots \dots$$

$$x_k = b_{k1}t_1 + b_{k2}t_2 + \dots + b_{kn}t_n$$

записывается в виде  $X = BT$ , где  $B$  — матрица коэффициентов,  $T$  — столбец из  $t_j$ .

Поэтому суперпозицию этих подстановок можно записать в виде  $Y = A(BT)$ . Вместе с тем матрица суперпозиции равна  $AB$ , и этот факт записывается так:  $Y = (AB)T$ . Таким образом, верно следующее соотношение ассоциативности:

$$A(BT) = (AB)T,$$

где  $T$  — столбец.

Рассмотрим теперь свойства действия умножения матриц:

$$1. (cA)B = A(cB) = cAB.$$

$$2. (A_1 + A_2)B = A_1B + A_2B.$$

$$3. A(B_1 + B_2) = AB_1 + AB_2.$$

Эти свойства непосредственно следуют из того, что элементы произведения выражаются как через элементы  $A$ , так и через элементы  $B$  в виде линейных однородных полиномов.

$$4. (AB)C = A(BC) \text{ (ассоциативность умножения).}$$

Это свойство трактуется таким образом, что если одна из частей равенства имеет смысл, то имеет смысл и другая, и они равны.

Пусть  $(AB)C$  имеет смысл и пусть  $m$  есть число строк матрицы  $A$ ,  $k$  — число ее столбцов. Тогда  $B$  имеет  $k$  строк, ибо  $AB$  имеет смысл. Пусть матрица  $B$  имеет  $l$  столбцов. Тогда и  $AB$  имеет  $l$  столбцов, так что для осмысленности  $(AB)C$  нужно, чтобы  $C$  имела  $l$  строк. Итак, для осмысленности  $(AB)C$  необходимо и достаточно, чтобы число столбцов матрицы  $A$  равнялось числу строк матрицы  $B$ , а число столбцов матрицы  $B$  равнялось числу строк матрицы  $C$ . Аналогично прослеживается, что те же условия необходимы и достаточны для осмысленности  $A(BC)$ . Остается доказать равенство  $(AB)C = A(BC)$ . Введем в рассмотрение матрицы  $F = AB$ ,  $G = (AB)C$ ,  $D = BC$  и  $H = A(BC)$ , обозначая их элементы соответствующими малыми буквами.

Имеем:  $f_{i\beta} = \sum_{\alpha=1}^k a_{i\alpha} b_{\alpha\beta}$ ; далее,

$$g_{ij} = \sum_{\beta=1}^l f_{i\beta} c_{\beta j} = \sum_{\beta=1}^l \sum_{\alpha=1}^k a_{i\alpha} b_{\alpha\beta} c_{\beta j},$$

$$d_{\alpha j} = \sum_{\beta=1}^l b_{\alpha\beta} c_{\beta j},$$

$$h_{ij} = \sum_{\alpha=1}^k a_{i\alpha} d_{\alpha j} = \sum_{\alpha=1}^k \sum_{\beta=1}^l a_{i\alpha} b_{\alpha\beta} c_{\beta j}.$$

Мы видим, что  $g_{ij} = h_{ij}$ , ибо эти элементы представлены в виде сумм одинаковых слагаемых, только расположенных в различных порядках.

Равенство  $(AB)C = A(BC)$  можно доказать менее вычислительно, воспользовавшись следующим простым замечанием. Пусть  $P$  и  $Q$  — две матрицы такие, что  $PQ$  имеет смысл. Пусть  $Q_1, Q_2, \dots, Q_k$  — столбцы матрицы  $Q$ . Тогда столбцами матрицы  $PQ$  являются  $PQ_1, PQ_2, \dots, PQ_k$ , что непосредственно следует из определения. Это обстоятельство можно записать в виде

$$P(Q_1, Q_2, \dots, Q_k) = (PQ_1, PQ_2, \dots, PQ_k).$$

Обозначим через  $C_1, C_2, \dots, C_l$  столбцы матрицы  $C$ . Тогда  $(AB)C = ((AB)C_1, (AB)C_2, \dots, (AB)C_l)$ . Далее,  $BC = (BC_1, BC_2, \dots, BC_l)$  и  $A(BC) = (A(BC_1), A(BC_2), \dots, A(BC_l))$ . Но, как было установлено выше,  $(AB)C_1 = A(BC_1)$ ,  $(AB)C_2 = A(BC_2)$ ,  $\dots$ ,  $(AB)C_l = A(BC_l)$ , ибо  $C_1, C_2, \dots, C_l$  — столбцы. Таким образом,

$$(AB)C = A(BC).$$

Особую роль при умножении матриц играют единичные матрицы. Это квадратные матрицы, у которых элементы главной диагонали равны 1, а все остальные элементы равны 0. Обозначать единичные матрицы будем  $E_n$  (если нужно указать порядок) или

просто  $E$ . Из правила умножения матриц непосредственно следует, что  $AE = A$  и  $EA = A$ , если произведения определены.

Ясно, что единичной матрице соответствует единичная подстановка переменных:

$$\begin{array}{ccccccc} y_1 & = & x_1, & & & & \\ & y_2 & = & x_2, & & & \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & y_n & = & x_n, & & & \end{array}$$

сводящаяся просто к переименованию переменных. На языке подстановок переменных свойства единичных матриц становятся совершенно очевидными.

Отметим еще, что представляют собой субматрицы произведения двух матриц. Пусть

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \cdot & \cdot & \cdot \\ c_{m1} & \dots & c_{mn} \end{pmatrix} = AB.$$

Субматрица, образованная строками с номерами  $\alpha_1, \alpha_2, \dots, \alpha_k$  и столбцами с номерами  $\beta_1, \beta_2, \dots, \beta_l$ , равна произведению субматрицы матрицы  $A$ , составленной из строк  $\alpha_1, \alpha_2, \dots, \alpha_k$ , на субматрицу матрицы  $B$ , составленную из столбцов  $\beta_1, \beta_2, \dots, \beta_l$ . Это непосредственно следует из того, что  $C_{\alpha_i \beta_j}$  есть произведение  $\alpha_i$ -й строки матрицы  $A$  на  $\beta_j$ -й столбец матрицы  $B$ .

**4. Транспонирование матриц.** Замена строк матрицы на ее столбцы, а столбцов — на строки называется *транспонированием* матрицы. Так, если

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

то транспонированная с ней матрица

$$A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}.$$

Ясно, что дважды транспонировать — значит вернуться к исходной матрице:  $(A^T)^T = A$ . Ясно также, что  $(A + B)^T = A^T + B^T$  и  $(cA)^T = cA^T$ .

Несколько сложнее дело обстоит с транспонированием произведения. Именно:

Матрица, транспонированная с произведением двух матриц, равна произведению транспонированных, взятых в обратном порядке.

В буквенной записи

$$(AB)^T = B^T A^T,$$

Докажем это. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mk} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & b_{kn} \end{pmatrix}.$$

Положим

$$A^T = C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1m} \\ c_{21} & c_{22} & \dots & c_{2m} \\ \dots & \dots & \dots & \dots \\ c_{k1} & c_{k2} & \dots & c_{km} \end{pmatrix}, \quad B^T = D = \begin{pmatrix} d_{11} & d_{12} & \dots & d_{1k} \\ d_{21} & d_{22} & \dots & d_{2k} \\ \dots & \dots & \dots & \dots \\ d_{n1} & d_{n2} & \dots & d_{nk} \end{pmatrix},$$

так что  $c_{ji} = a_{ij}$ ,  $d_{\beta\alpha} = b_{\alpha\beta}$ . Пусть, далее,

$$AB = F = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{pmatrix}, \quad B^T A^T = G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1m} \\ g_{21} & g_{22} & \dots & g_{2m} \\ \dots & \dots & \dots & \dots \\ g_{n1} & g_{n2} & \dots & g_{nm} \end{pmatrix}.$$

Тогда  $f_{ij} = \sum_{\alpha=1}^k a_{i\alpha} b_{\alpha j}$ ,

$$g_{ji} = \sum_{\alpha=1}^k d_{j\alpha} c_{\alpha i} = \sum_{\alpha=1}^k b_{\alpha j} a_{i\alpha} = \sum_{\alpha=1}^k a_{i\alpha} b_{\alpha j} = f_{ij}.$$

Итак,  $g_{ji} = f_{ij}$  при всех  $i = 1, 2, \dots, m$  и  $j = 1, 2, \dots, n$ , а это и значит, что  $G = F^T$ , т. е.  $B^T A^T = (AB)^T$ , что и требовалось доказать.

**5. Обзор действий над матрицами.** Над матрицами определены четыре действия: сложение, умножение на элементы основного поля (или кольца), умножение матрицы на матрицу и транспонирование.

Условие применимости и размеры результата поясняются следующими схемами:

$$A+B: \begin{matrix} m \\ \boxed{\phantom{000}} \\ n \end{matrix} + \begin{matrix} m \\ \boxed{\phantom{000}} \\ n \end{matrix} = \begin{matrix} \phantom{m} \\ \boxed{\phantom{000}} \\ n \end{matrix}$$

$$cA: \begin{matrix} m \\ \boxed{\phantom{000}} \\ n \end{matrix} \longrightarrow \begin{matrix} \phantom{m} \\ \boxed{\phantom{000}} \\ n \end{matrix} m$$

$$AB: \begin{matrix} m \\ \boxed{\phantom{000}} \\ k \end{matrix} \cdot \begin{matrix} \phantom{m} \\ \boxed{\phantom{000}} \\ n \end{matrix} k = \begin{matrix} \phantom{m} \\ \boxed{\phantom{000}} \\ n \end{matrix} m$$

$$A^T: \begin{matrix} m \\ \boxed{\phantom{000}} \\ n \end{matrix} \longrightarrow \begin{matrix} \phantom{m} \\ \boxed{\phantom{000}} \\ m \end{matrix} n$$

Эти действия обладают свойствами:

1.  $(A + B) + C = A + (B + C)$ .
2.  $A + B = B + A$ .
3. Существует  $0$ :  $A + 0 = 0 + A = A$ .
4. Для  $A$  существует  $-A$ :  $A + (-A) = 0$ .
5.  $(c_1 + c_2)A = c_1A + c_2A$ .
6.  $c(A_1 + A_2) = cA_1 + cA_2$ .
7.  $c_1(c_2A) = (c_1c_2)A$ .
8.  $1 \cdot A = A$ .

Это — свойства векторного пространства, так что матрицы фиксированных размеров образуют векторное пространство.

9.  $(AB)C = A(BC)$ .
10.  $A(B_1 + B_2) = AB_1 + AB_2$ .
11.  $(A_1 + A_2)B = A_1B + A_2B$ .
12.  $(cA)B = A(cB) = cAB$ .

13. Существуют единицы, именно, если  $A = \begin{bmatrix} & \\ & \end{bmatrix}_n^m$ , то

$$E_m A = A E_n = A.$$

14.  $(A^T)^T = A$ .
15.  $(A + B)^T = A^T + B^T$ .
16.  $(cA)^T = cA^T$ .
17.  $(AB)^T = B^T A^T$ .

Для квадратных матриц фиксированного порядка  $n$  действия сложения и умножения определены всегда, и их результатами являются квадратные матрицы того же порядка. Таким образом, квадратные матрицы фиксированного порядка образуют кольцо. Кольцо, наделенное структурой векторного пространства, т. е. система объектов, обладающих свойствами 1—12, называется *алгеброй* над основным полем. Таким образом, квадратные матрицы с элементами из поля  $K$  составляют алгебру над этим полем.

Само поле  $K$  изоморфно вкладывается в алгебру квадратных матриц при помощи отображения  $c \mapsto cE$ ,  $c \in K$ .

В соответствии с тем, что было изложено в гл. III о значениях полинома, в алгебре квадратных матриц естественным образом определяются степени  $A^n$  матрицы с натуральными показателями и значения полиномов, именно, если  $f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_n \in K[t]$ , то  $f(A) = a_0 A^n + a_1 A^{n-1} + \dots + a_{n-1} A + a_n E$ . Значения полиномов от одной и той же матрицы коммутируют.

## § 2. Теория определителей

С линейными задачами, использующими теорию матриц, связан аппарат так называемых определителей, очень ценный по широте приложений к теоретическим вопросам.

**1. Наводящие соображения.** Рассмотрим в общем виде систему двух линейных уравнений с двумя неизвестными

$$\begin{aligned} a_1x + b_1y &= c_1, \\ a_2x + b_2y &= c_2. \end{aligned} \quad (1)$$

Допустим, что система имеет решение и пара  $x, y$  составляет решение, так что оба уравнения уже обратились в верные равенства. Умножим обе части первого равенства на  $b_2$ , второго на  $b_1$  и вычтем. Получим

$$(a_1b_2 - a_2b_1)x = c_1b_2 - c_2b_1.$$

Теперь первое равенство умножим на  $-a_2$ , второе на  $a_1$  и сложим. Получим

$$(a_1b_2 - a_2b_1)y = a_1c_2 - a_2c_1.$$

Предположим, что  $a_1b_2 - a_2b_1 \neq 0$ . Тогда

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1}, \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}. \quad (2)$$

Таким образом, предположив, что решение существует, мы смогли его найти. Теперь перед нами альтернатива — либо решение существует и тогда оно дается формулами (2), либо решение не существует. Для того чтобы отделаться от второй возможности, нужно только установить, что формулы (2) действительно дают решение системы, для чего следует подставить  $x$  и  $y$  из (2) в систему (1). Сделаем это:

$$\begin{aligned} a_1 \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} + b_1 \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1} &= \\ &= \frac{a_1c_1b_2 - a_1c_2b_1 + a_1b_1c_2 - a_2b_1c_1}{a_1b_2 - a_2b_1} = \frac{c_1(a_1b_2 - a_2b_1)}{a_1b_2 - a_2b_1} = c_1, \\ a_2 \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} + b_2 \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1} &= \frac{c_2(a_1b_2 - a_2b_1)}{a_1b_2 - a_2b_1} = c_2. \end{aligned}$$

Мы видим, что оба уравнения превратились в верные равенства.

Если  $a_1b_2 - a_2b_1 = 0$ , то наши рассуждения не приводят к законченному результату, и мы оставим этот случай пока в стороне.

В формулах (2) знаменатель  $a_1b_2 - a_2b_1$  один и тот же. Числители же очень похожи по форме записи на знаменатель.

Для выражения  $a_1b_2 - a_2b_1$  существует специальное название *определителя* матрицы  $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$  и специальное обозначение:

$$a_1b_2 - a_2b_1 = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}.$$

С помощью обозначений для определителей формулы (2) записываются в виде

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}, \quad y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}.$$

Применяя, например, эти формулы к решению системы

$$2x - 3y = 5,$$

$$3x + 4y = 7,$$

получим

$$x = \frac{\begin{vmatrix} 5 & -3 \\ 7 & 4 \end{vmatrix}}{\begin{vmatrix} 2 & -3 \\ 3 & 4 \end{vmatrix}} = \frac{41}{17}, \quad y = \frac{\begin{vmatrix} 2 & 5 \\ 3 & 7 \end{vmatrix}}{\begin{vmatrix} 2 & -3 \\ 3 & 4 \end{vmatrix}} = -\frac{1}{17}.$$

Разумеется, понятие определителя было бы не нужным, если бы шла речь только о системах двух уравнений с двумя неизвестными. Результат может быть обобщен на линейные системы  $n$  уравнений с  $n$  неизвестными.

Рассмотрим еще случай  $n = 3$ . Пусть дана система

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1, \\ a_2x + b_2y + c_2z &= d_2, \\ a_3x + b_3y + c_3z &= d_3. \end{aligned} \quad (3)$$

Исключим сразу неизвестные  $y$  и  $z$ . С этой целью умножим первое уравнение на  $b_2c_3 - b_3c_2$ , второе на  $b_3c_1 - b_1c_3$ , третье на  $b_1c_2 - b_2c_1$  и сложим. Получим

$$\begin{aligned} & (a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1)x + \\ & + (b_1b_2c_3 - b_1b_3c_2 + b_2b_3c_1 - b_2b_1c_3 + b_3b_1c_2 - b_3b_2c_1)y + \\ & + (c_1b_2c_3 - c_1b_3c_2 + c_2b_3c_1 - c_2b_1c_3 + c_3b_1c_2 - c_3b_2c_1)z = \\ & = d_1b_2c_3 - d_1b_3c_2 + d_2b_3c_1 - d_2b_1c_3 + d_3b_1c_2 - d_3b_2c_1. \end{aligned}$$

Ясно, что коэффициенты при  $y$  и  $z$  равны нулю.

Коэффициент при  $x$  играет здесь такую же роль, как  $a_1b_2 - a_2b_1$  для систем второго порядка. Он называется *определителем матрицы*

$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$  и обозначается:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}.$$

В этих обозначениях, если определитель не равен нулю,

$$x = \frac{\begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}.$$

Аналогично,

$$y = \frac{\begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}, \quad z = \frac{\begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}}.$$

Наш вывод имеет смысл при предположении, что решение существует. Однако, если подставить найденные выражения для  $x$ ,  $y$ ,  $z$  в исходную систему, можно убедиться в том, что все три уравнения обратятся в верные равенства.

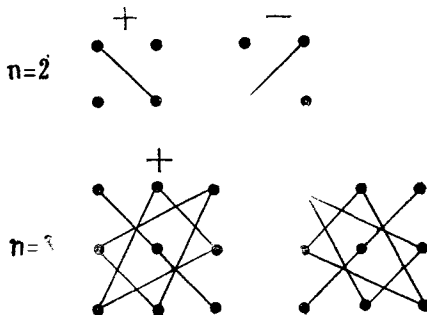
Итак, мы показали, что формулы для решения в общем виде линейных систем уравнений при  $n=2$  и  $n=3$  имеют сходную структуру и основную роль в них играют определители второго порядка

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1 b_2 - a_2 b_1$$

и третьего порядка

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 b_2 c_3 - a_1 b_3 c_2 + a_2 b_3 c_1 - a_2 b_1 c_3 + a_3 b_1 c_2 - a_3 b_2 c_1.$$

Оба эти выражения представляют собой алгебраические суммы произведений элементов матриц, причем эти произведения составляются по одному элементу из каждой строки и по одному из каждого столбца. Все такие произведения входят в состав определителя. Произведения снабжаются знаками  $+$  и  $-$  по правилам:



На этих рисунках соединены линиями элементы матрицы, составляющие произведения, входящие в определитель со знаками  $+$  и  $-$ .

Обратимся теперь к обобщению определителя для квадратных матриц любого порядка  $n$ , исходя из формы этих выражений для  $n = 2$  и  $n = 3$ .

Здесь удобно обозначать элементы матрицы одной буквой, приписывая ей два индекса — номер строки и номер столбца. Дадим формальное определение определителя для квадратной матрицы порядка  $n$  следующим образом:

*Определителем* квадратной матрицы порядка  $n$  (или *определителем порядка  $n$* ) называется алгебраическая сумма всевозможных произведений элементов матрицы, взятых по одному из каждой строки, по одному из каждого столбца и снабженных знаками «плюс» и «минус» по некоторому определенному правилу.

К вопросу о том, что это за правило, мы обратимся в ближайшее время, а пока попытаемся записать символически сформулированное выше определение. В каждом слагаемом определителя мы будем записывать сомножители в порядке следования строк. Номера столбцов будут составлять в совокупности все числа от 1 до  $n$ , в различных порядках, причем во всех возможных порядках, так как определитель, согласно данному определению, составлен из всех произведений элементов, взятых по одному из каждой строки и по одному из каждого столбца. В буквенных обозначениях:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum \pm a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n}.$$

Здесь индексы  $\alpha_1, \alpha_2, \dots, \alpha_n$  пробегают все возможные перестановки чисел 1, 2,  $\dots, n$ . Все перестановки должны быть разбиты на два класса так, чтобы одному классу соответствовали слагаемые со знаком «плюс», другому — со знаком «минус».

**2. Элементарные сведения теории перестановок.** Сейчас мы рассмотрим некоторые простейшие свойства совокупности перестановок  $n$  элементов. Переставляемыми элементами мы будем считать числа натурального ряда.

Предложение 1. Число всех перестановок  $n$  элементов равно  $n! = 1 \cdot 2 \cdot \dots \cdot n$ .

**Доказательство.** Применим метод индукции. Для  $n = 1$  предложение очевидно. Пусть оно верно для  $n - 1$ . Совокупность перестановок  $n$  элементов разобьем на  $n$  частей, по положению элемента  $n$  на первом, втором,  $\dots, n$ -м месте. В каждой части будет  $(n - 1)!$  перестановок, так как их число равно числу расположений элементов 1, 2,  $\dots, n - 1$  на  $n - 1$  незанятых местах. Следовательно, число перестановок равно  $n \cdot (n - 1)! = n!$ , что и требовалось доказать.

Теперь разобьем все  $n!$  перестановок  $n$  элементов на два класса, по признаку, кажущемуся довольно искусственным, но именно это разбиение будет нужно для разумного правила расстановки знаков в определителе.

Пусть  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  — некоторая перестановка чисел  $1, 2, \dots, n$ . Скажем, что пара элементов  $(\alpha_i, \alpha_j)$ ,  $i < j$ , образует *инверсию*, если  $\alpha_i > \alpha_j$ . Число всех пар элементов перестановки, образующих инверсию, называется числом инверсий в перестановке и обозначается  $\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Так,  $\text{inv}(3, 5, 1, 4, 2, 6, 8, 7) = 7$  (инверсии образуют пары  $(3, 1)$ ,  $(3, 2)$ ,  $(5, 1)$ ,  $(5, 4)$ ,  $(5, 2)$ ,  $(4, 2)$ ,  $(8, 7)$ ).

Перестановки, содержащие четное число инверсий, называются *четными*, содержащие нечетное число инверсий — *нечетными*.

*Подстановкой* на множестве  $\{1, 2, \dots, n\}$  называется взаимно однозначное отображение множества на себя. Удобно задавать подстановку прямым указанием замен для каждого элемента, посредством записи образа под прообразом. Так, запись  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$  задает подстановку, которая заменяет элементы  $1, 2, 3, 4, 5$ , соответственно, на  $5, 1, 3, 2, 4$ ; порядок расположения ее столбцов безразличен. В такой записи в «числителе» и в «знаменателе» оказываются перестановки. Удобно в «числителе» записывать элементы в натуральном расположении.

Последовательное применение двух подстановок приводит к подстановке, называемой их *произведением*. Так,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 4 & 2 \end{pmatrix}$$

(мы считаем первой действующей ту подстановку, которая записана слева). Почти очевидно, что при умножении подстановок имеет место ассоциативность. Действительно, пусть  $\sigma$ ,  $\tau$  и  $\varphi$  — подстановки на множестве  $\{1, 2, \dots, n\}$ . Сделать  $(\sigma\tau)\varphi$  — все равно, что сначала сделать  $\sigma$ , потом  $\tau$ , затем  $\varphi$ ; сделать же  $\sigma(\tau\varphi)$  — все равно, что сначала сделать  $\sigma$ , потом  $\tau\varphi$ , т. е. к результату применения  $\sigma$  применить  $\tau$  и затем  $\varphi$ .

Тождественная подстановка, при которой каждому элементу сопоставляется он сам, играет роль единицы в этом умножении. Если запись подстановки  $\sigma$  перевернуть, т. е. ее числитель сделать знаменателем, а знаменатель числителем, мы придем к обратной подстановке  $\sigma^{-1}$ , произведение которой на  $\sigma$  как в одном, так и в обратном порядке, дает единичную подстановку. Умножение подстановок, вообще говоря, некоммутативно, например,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \text{ а } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Число всех возможных подстановок на множестве из  $n$  элементов равно  $n!$ , ибо таково число возможных знаменателей при фиксированном числителе.

Подстановка называется *транспозицией*, если она  $n-2$  элемента оставляет на местах, а остальные два элемента переставляет местами. Вместо того чтобы записывать, например, транспозицию  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix}$ , пишут кратко  $(2, 5)$ .

**Предложение 2.** Пусть в некоторой перестановке сделана транспозиция. Она равна произведению нечетного числа транспозиций соседних элементов.

**Доказательство.** Пусть дана перестановка

$$(a, b, \dots, c, d, e, \dots, f, g, h, \dots, k, l),$$

и транспозиция меняет местами  $c$  и  $h$ . Обозначим через  $m$  число элементов  $d, e, \dots, f, g$ , лежащих между  $c$  и  $h$ . Переставим местами  $c$  с  $d$ , затем  $c$  с  $e, \dots, c$  с  $f, c$  с  $g$ . После этого мы придем к перестановке

$$(a, b, \dots, d, e, \dots, f, g, c, h, \dots, k, l).$$

Мы сделали последовательно  $m$  транспозиций. Теперь переставим  $c$  и  $h$ . Придем к

$$(a, b, \dots, d, e, \dots, f, g, h, c, \dots, k, l).$$

Теперь «перегоним»  $h$  на место, которое занимало  $c$ , переставив  $h$  по очереди с  $g, c, f, \dots, c, e, c, d$ . Мы придем к перестановке

$$(a, b, \dots, h, d, e, \dots, f, g, c, \dots, k, l),$$

т. е. как будто мы сделали одну транспозицию  $(c, h)$ . Всего мы сделали  $m + 1 + m = 2m + 1$  транспозиций соседних элементов. Таким образом, транспозиция  $(c, h)$  равна произведению  $2m + 1$  транспозиций соседних элементов. Все это рассуждение равносильно одному равенству:

$$(c, h) = (c, d)(c, e) \dots (c, f)(c, g)(c, h)(g, h)(f, h) \dots (e, h)(d, h).$$

**Предложение 3.** При транспозиции соседних элементов число инверсий в перестановке меняется на одну единицу.

**Доказательство.** Нам нужно сравнить число инверсий в перестановках

$$(a, b, \dots, c, d, e, f, \dots, k, l)$$

и

$$(a, b, \dots, c, e, d, f, \dots, k, l).$$

Обозначим через  $i_1$  и  $i'_1$  число инверсий в парах, не содержащих элементов  $d$  и  $e$ , в обеих перестановках соответственно; через  $i_2$  и  $i'_2$  — число инверсий в парах, содержащих один из элементов  $d$  и  $e$ ; через  $i_3$  и  $i'_3$  — число инверсий в паре  $d, e$  и через  $i$  и  $i'$  — полное число инверсий. Ясно, что  $i = i_1 + i_2 + i_3$ ,  $i' = i'_1 + i'_2 + i'_3$ .

Далее, очевидно, что  $i_1 = i'_1$ . Число  $i_2$  тоже равно  $i'_2$ , так как каждый из элементов  $d$  и  $e$  расположен относительно остальных элементов одинаковым образом в обеих перестановках. На-

конец, если  $i_3 = 0$ , то  $i'_3 = 1$ , и если  $i_3 = 1$ , то  $i'_3 = 0$ . Поэтому  $i' - i = i'_1 + i'_2 + i'_3 - i_1 - i_2 - i_3 = i'_3 - i_3 = \pm 1$ , что и требовалось доказать.

**Следствие 1.** *Если в перестановке сделать транспозицию соседних элементов, то четность перестановки изменится на противоположную.*

**Следствие 2.** *Любая транспозиция изменяет четность перестановки на противоположную.*

Действительно, любая транспозиция равносильна нечетному числу транспозиций соседних элементов.

**Предложение 4.** *Число четных перестановок  $n$  элементов равно числу нечетных перестановок.*

**Доказательство.** Пусть число четных перестановок равно  $a$ , число нечетных равно  $b$ . Рассмотрим множество всех четных перестановок. Сделаем в них одну и ту же транспозицию, например,  $(1, 2)$ . Мы получим нечетные перестановки, попарно различные, в количестве  $a$  штук. Так как число всех нечетных перестановок равно  $b$ , заключаем, что  $a \leq b$ . Теперь рассмотрим множество всех нечетных перестановок и сделаем в них транспозицию  $(1, 2)$ . Мы получим  $b$  четных перестановок и, следовательно,  $b \leq a$ . Из установленных неравенств следует, что  $a = b$ , что и требовалось доказать.

Попутно мы получили, что если во всех четных перестановках сделать одну и ту же транспозицию, то мы получили все нечетные перестановки.

**Предложение 5.** *Любая перестановка может быть получена из любой другой посредством нескольких транспозиций.*

**Доказательство.** Применим индукцию. Для  $n = 2$  утверждение тривиально. Пусть  $n > 2$  и для перестановок  $n - 1$  элемента предложение доказано. Пусть  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  и  $(\beta_1, \beta_2, \dots, \beta_n)$  — две данные перестановки. Если  $\beta_1 = \alpha_1$ , то  $(\alpha_2, \dots, \alpha_n)$  и  $(\beta_2, \dots, \beta_n)$  отличаются только порядком и, в силу индукционного предположения, посредством нескольких транспозиций можно перейти от  $(\alpha_2, \dots, \alpha_n)$  к  $(\beta_2, \dots, \beta_n)$  и, следовательно, от  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  к  $(\beta_1, \beta_2, \dots, \beta_n)$ . Пусть теперь  $\beta_1 \neq \alpha_1$ . Тогда  $\beta_1 = \alpha_i$  при некотором  $i \neq 1$ . Сделав в  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  транспозицию  $(\alpha_1, \alpha_i)$ , мы придем к новой перестановке, у которой на первом месте находится  $\alpha_i = \beta_1$ . В силу доказанного эта перестановка превращается в  $\beta_1, \beta_2, \dots, \beta_n$  посредством нескольких транспозиций. Следовательно, от  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  к  $(\beta_1, \beta_2, \dots, \beta_n)$  можно перейти посредством нескольких транспозиций, что и требовалось доказать.

В терминах подстановок предложение можно переформулировать так: любая подстановка может быть представлена в виде произведения транспозиций.

Переход от одной перестановки к другой посредством транспозиций совершенно не однозначен. Однако в силу предложения 3

четность или нечетность числа транспозиций для такого перехода инвариантна. Именно, для перехода от перестановки к другой перестановке той же четности число транспозиций обязательно четное, ибо каждая транспозиция меняет четность перестановки на противоположную. Аналогично, для перехода от перестановки к другой перестановке противоположной четности требуется нечетное число транспозиций.

**3. Определитель порядка  $n$ . Определение.** В п. 1 была дана предварительная формулировка для определителя. В ней не хватало правила расстановки знаков слагаемых, но было указано, что это правило должно быть связано с разбиением перестановок на два класса. В п. 2 было описано разбиение перестановок на два класса — четных и нечетных перестановок. Это разбиение и положим в основу правила расстановки знаков в определителе. Таким образом, приходим к следующей полной формулировке.

Определителем квадратной матрицы называется алгебраическая сумма всевозможных произведений элементов этой матрицы, взятых по одному из каждой строки и по одному из каждого столбца. Сомножители в каждом слагаемом записываются в порядке следования строк, тогда номера столбцов образуют перестановки; слагаемые, соответствующие четным перестановкам, берутся со знаком «плюс», соответствующие нечетным — со знаком «минус».

Легко проследить, что расстановка знаков в определителях второго и третьего порядков соответствует сформулированному правилу.

Настоятельно рекомендую читателю не пожалеть времени и выписать в развернутой форме определитель четвертого порядка.

В символической записи определитель можно записать так:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)} a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n},$$

где  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  пробегает все перестановки чисел  $1, 2, \dots, n$ ; далее, множитель  $(-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)}$  равен  $+1$ , если  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  — четная перестановка, и равен  $-1$ , если нечетная.

Ясно, что понятие определителя имеет смысл для матриц с элементами из любого ассоциативного коммутативного кольца и, в частности, из любого поля.

#### 4. Свойства определителя.

**1. Общее правило знаков.** Для дальнейшего будет полезно узнать, с каким знаком входит в определитель

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \text{ слагаемое } a_{\alpha_1\beta_1} a_{\alpha_2\beta_2} \dots a_{\alpha_n\beta_n}, \text{ где } (\alpha_1, \alpha_2, \dots, \alpha_n)$$

и  $(\beta_1, \beta_2, \dots, \beta_n)$  — две перестановки чисел  $1, 2, \dots, n$ . Для того

чтобы узнать это, следует расположить сомножители в порядке следования строк. Заметим, что если поменять местами два сомножителя, то происходит транспозиция как в первых, так и во вторых индексах, так что число инверсий в первых индексах и число инверсий во вторых индексах меняются на нечетные числа, и потому их сумма меняется на четное число. Поэтому  $(-1)^{\text{inv}(a_1, a_2, \dots, a_n) + \text{inv}(\beta_1, \beta_2, \dots, \beta_n)}$  не изменяется при перемещении мест двух сомножителей, а следовательно, и при любом изменении порядка сомножителей, ибо любое изменение порядка равносильно нескольким попарным перемещениям мест. Отсюда следует, что знак, с которым входит слагаемое  $a_{a_1\beta_1} a_{a_2\beta_2} \dots a_{a_n\beta_n}$  в определитель, есть  $(-1)^{\text{inv}(a_1, a_2, \dots, a_n) + \text{inv}(\beta_1, \beta_2, \dots, \beta_n)}$ . Действительно, пусть  $\gamma_1, \gamma_2, \dots, \gamma_n$  — последовательность номеров столбцов после приведения сомножителей в порядок следования строк, так что  $a_{a_1\beta_1} a_{a_2\beta_2} \dots a_{a_n\beta_n} = a_{1\gamma_1} a_{2\gamma_2} \dots a_{n\gamma_n}$ . Тогда

$$\begin{aligned} (-1)^{\text{inv}(a_1, a_2, \dots, a_n) + \text{inv}(\beta_1, \beta_2, \dots, \beta_n)} &= \\ &= (-1)^{\text{inv}(1, 2, \dots, n) + \text{inv}(\gamma_1, \gamma_2, \dots, \gamma_n)} = (-1)^{\text{inv}(\gamma_1, \gamma_2, \dots, \gamma_n)}, \end{aligned}$$

а это и есть множитель  $\pm 1$ , с которым интересующее нас слагаемое входит в состав определителя.

2. *Определитель транспонированной матрицы равен определителю исходной.* Другими словами — определитель не меняется при транспонировании матрицы.

Действительно, брать произведения элементов по одному из каждой строки и по одному из каждого столбца исходной матрицы — то же самое, что делать это по отношению к транспонированной матрице. Далее, номера строк для исходной — это номера столбцов для транспонированной, а номера столбцов исходной суть номера строк транспонированной. Поэтому каждое слагаемое  $a_{a_1\beta_1} a_{a_2\beta_2} \dots a_{a_n\beta_n}$  входит в состав определителя исходной матрицы и определителя транспонированной с одним и тем же множителем  $(-1)^{\text{inv}(a_1, a_2, \dots, a_n) + \text{inv}(\beta_1, \beta_2, \dots, \beta_n)}$ .

Установленные два свойства указывают, что в определителе строки и столбцы совершенно равноправны. Поэтому все дальнейшие свойства, устанавливаемые для строк, остаются справедливыми и для столбцов.

Следующие два свойства означают *линейность* определителя относительно элементов любой его строки.

3. *Если элементы какой-либо строки представлены в виде суммы двух слагаемых, то определитель равен сумме двух определителей, в первом из которых элементы отмеченной строки равны первым слагаемым, во втором — вторым.*

Это свойство становится прозрачнее, если от словесной формулировки перейти к формуле:

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ b_{i1} + c_{i1} & \dots & b_{in} + c_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ b_{i1} & \dots & b_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ c_{i1} & \dots & c_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Доказательство.

$$\begin{aligned} \Delta &= \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots (b_{i\alpha_i} + c_{i\alpha_i}) \dots a_{n\alpha_n} = \\ &= \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots b_{i\alpha_i} \dots a_{n\alpha_n} + \\ &\quad + \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots c_{i\alpha_i} \dots a_{n\alpha_n}. \end{aligned}$$

Ясно, что первая сумма равна  $\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ b_{i1} & \dots & b_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$ , а вторая равна

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ c_{i1} & \dots & c_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Доказанное свойство естественным образом обобщается на случай, когда элементы строки представлены в виде суммы нескольких слагаемых.

4. Если все элементы какой-либо строки определителя имеют общий множитель, то этот общий множитель можно вынести за знак определителя.

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ ma_{i1} & \dots & ma_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = m \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Действительно,

$$\begin{aligned} \Delta &= \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots ma_{i\alpha_i} \dots a_{n\alpha_n} = \\ &= m \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{n\alpha_n} = \\ &= m \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}. \end{aligned}$$

5. *Определитель с двумя одинаковыми строками равен нулю.*

6. *Если в матрице поменять местами две строки, то ее определитель изменит знак на обратный.*

Эти два свойства тесно связаны и играют особо важную роль в теории определителей.

Докажем сначала 5-е свойство, потом 6-е.

Пусть дан определитель с двумя одинаковыми строками:

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} =$$

$$= \sum_{(\alpha_1, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_n)} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n},$$

причем  $a_{i1} = a_{k1}$ ,  $a_{i2} = a_{k2}$ , ...,  $a_{in} = a_{kn}$ .

Разобьем сумму на две части, соответствующие четным и нечетным перестановкам:

$$\Delta = \sum_{\substack{(\alpha_1, \dots, \alpha_n) \\ \text{четн.}}} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n} -$$

$$- \sum_{\substack{(\alpha_1, \dots, \alpha_n) \\ \text{нечетн.}}} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n}.$$

Вспомним, что все нечетные перестановки получаются, если во всех четных перестановках  $(\alpha_1, \dots, \alpha_i, \dots, \alpha_k, \dots, \alpha_n)$  сделать одну и ту же транспозицию  $(\alpha_i, \alpha_k)$ . Поэтому

$$\Delta = \sum_{\substack{(\alpha_1, \dots, \alpha_i, \dots, \alpha_k, \dots, \alpha_n) \\ \text{четн.}}} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n} -$$

$$- \sum_{\substack{(\alpha_1, \dots, \alpha_i, \dots, \alpha_k, \dots, \alpha_n) \\ \text{нечетн.}}} a_{1\alpha_1} \dots a_{i\alpha_k} \dots a_{k\alpha_i} \dots a_{n\alpha_n}.$$

Но  $a_{i\alpha_i} = a_{k\alpha_i}$  и  $a_{k\alpha_k} = a_{i\alpha_k}$ . Поэтому для каждого слагаемого первой суммы найдется равное ему слагаемое во второй, так что  $\Delta = 0$ , что и требовалось доказать.

Обратимся теперь к доказательству 6-го свойства, причем позволим себе обозначить переставляемые строки просто I и II. Нам нужно сравнить определители

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \text{I} & & \\ \dots & \dots & \dots \\ \text{II} & & \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} \quad \text{и} \quad \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \text{II} & & \\ \dots & \dots & \dots \\ \text{I} & & \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

С этой целью рассмотрим вспомогательный определитель, заведомо равный нулю:

$$\begin{aligned}
 0 &= \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ I + II & & \\ \dots & \dots & \dots \\ I + II & & \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ I & & \\ \dots & \dots & \dots \\ I + II & & \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ II & & \\ \dots & \dots & \dots \\ I + II & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \\
 &= \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ I & & \\ \dots & \dots & \dots \\ I & & \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ I & & \\ \dots & \dots & \dots \\ II & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ II & & \\ I & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ II & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.
 \end{aligned}$$

Мы два раза воспользовались свойством 3.

Первое и четвертое слагаемые равны нулю. Следовательно, сумма второго и третьего равна нулю, что и требовалось доказать.

Рассмотрим другой путь доказательства свойств 5 и 6. Начнем с шестого. Пусть

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} \quad \text{и} \quad \Delta' = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}; \quad i < k.$$

Возьмем какое-либо слагаемое из второго определителя, записанное в порядке следования его строк:

$$a_{1\alpha_1} \dots a_{k\alpha_k} \dots a_{i\alpha_i} \dots a_{n\alpha_n}.$$

Оно входит в состав  $\Delta'$  с множителем  $(-1)^{\text{inv}(a_1, \dots, a_i, \dots, a_k, \dots, a_n)}$ . Но  $a_{1\alpha_1} \dots a_{k\alpha_k} \dots a_{i\alpha_i} \dots a_{n\alpha_n} = a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{k\alpha_k} \dots a_{n\alpha_n}$ , так что в  $\Delta$  оно входит с множителем  $(-1)^{\text{inv}(a_1, \dots, a_k, \dots, a_i, \dots, a_n)}$ . Ясно, что  $(-1)^{\text{inv}(a_1, \dots, a_k, \dots, a_i, \dots, a_n)} = -(-1)^{\text{inv}(a_1, \dots, a_i, \dots, a_k, \dots, a_n)}$ , так что каждое слагаемое из  $\Delta'$  входит в  $\Delta$  с противоположным знаком, т. е.  $\Delta' = -\Delta$ .

Теперь для доказательства свойства 5 рассмотрим определитель с двумя одинаковыми строками и переменим местами эти строки. С одной стороны, он при этом изменит знак, но вместе с тем он не изменится. Следовательно,  $\Delta = -\Delta$ ,  $2\Delta = 0$  и  $\Delta = 0$ .

Однако это рассуждение применимо, только если в кольце возможно деление на 2, так что из  $2\Delta = 0$  следует  $\Delta = 0$ . В поле

вычетов по модулю 2 мы не могли бы сделать такого вывода. В этом состоит небольшой недостаток второго доказательства сравнительно с первым.

7. *Определитель с двумя пропорциональными строками равен нулю.*

Действительно, если, согласно свойству 4, вынести за знак определителя коэффициент пропорциональности, то остается определитель с равными строками, который равен нулю.

8. *Определитель не меняется, если к какой-либо его строке прибавить числа, пропорциональные другой строке.*

Действительно,

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} + ma_{k1} & \dots & a_{in} + ma_{kn} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ ma_{k1} & \dots & ma_{kn} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Свойство 8 особенно важно, так как оно дает ключ к вычислению определителей.

Рассмотрим небольшой пример.

Пусть требуется вычислить определитель

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix}.$$

Прибавим ко второй строке первую, умноженную на  $-1$ , затем к третьей прибавим первую, умноженную на  $-1$ , и затем к четвертой прибавим первую, умноженную на  $-1$ . Получим равный определитель

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & -2 \\ 0 & -2 & 0 & -2 \\ 0 & -2 & -2 & 0 \end{vmatrix}.$$

Теперь прибавим к четвертой строке третью, умноженную на  $-1$ , и к четвертой — вторую, умноженную на  $-1$ . Получим равный

определитель

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & -2 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & 0 & 4 \end{vmatrix}.$$

Теперь оказывается, что из 24 слагаемых определителя отлично от нуля только одно:  $a_{11}a_{23}a_{32}a_{44} = 1 \cdot (-2) \cdot (-2) \cdot 4 = 16$ . Перестановка (1, 3, 2, 4) нечетная, следовательно, определитель равен  $-16$ .

**5. Алгебраические дополнения и миноры.** Пусть дан определитель

$$\begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{i1} & \dots & a_{ik} & \dots & a_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix}.$$

Рассмотрим определитель

$$\begin{vmatrix} a_{11} & \dots & 0 & \dots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \dots & 0 & \dots & a_{nn} \end{vmatrix},$$

матрица которого получается из матрицы исходного определителя посредством замены элемента  $a_{ik}$  на 1 и всех остальных элементов  $i$ -й строки и  $k$ -го столбца на нули.

Так построенный определитель называется *алгебраическим дополнением* элемента  $a_{ik}$ . Для него принято обозначение  $A_{ik}$ . Заметим, что  $A_{ik}$  не зависит от элементов  $i$ -й строки и  $k$ -го столбца исходного определителя.

**9. Определитель равен сумме произведений элементов какой-либо строки на их алгебраические дополнения.**

Для доказательства запишем данный определитель в виде

$$\begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{i1} & \dots & a_{ik} & \dots & a_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} \cdot & \cdot & a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{i1} + 0 + \dots + 0 & \dots & 0 + \dots + a_{ik} + \dots + 0 & \dots & 0 + 0 + \dots + a_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix},$$

где каждый элемент  $i$ -й строки имеет  $n$  слагаемых. Теперь воспользуемся свойством линейности. Определитель равен сумме

следующих  $n$  определителей:

$$\begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} + \dots + \begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & a_{ik} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} + \dots$$

$$\dots + \begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix}.$$

В каждом из них вынесем в качестве множителя ненулевой элемент  $i$ -й строки:

$$a_{i1} \begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} + \dots + a_{ik} \begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} + \dots$$

$$\dots + a_{in} \begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix}.$$

Теперь вычтем из первой строки первого определителя  $i$ -ю, умноженную на  $a_{i1}$ , из второй —  $i$ -ю, умноженную на  $a_{21}$ , ..., из  $n$ -й вычтем  $i$ -ю, умноженную на  $a_{n1}$ . Все элементы не изменятся, кроме элементов первого столбца, которые заменятся на нули. Поэтому первый определитель равен

$$\begin{vmatrix} 0 & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} = A_{i1}.$$

Аналогично, остальные определители равны соответствующим алгебраическим дополнениям, так что действительно

$$\begin{vmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ik} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{vmatrix} = a_{i1}A_{i1} + \dots + a_{ik}A_{ik} + \dots + a_{in}A_{in}.$$

Это свойство носит название *разложения определителя по элементам строки*. Разумеется, существуют аналогичные разложения по элементам столбцов.

Следующие два свойства являются непосредственными следствиями из разложения по элементам строки.

10. Пусть в определителе  $\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$  выбрана строка с номером  $i$  и даны  $n$  чисел  $b_1, \dots, b_n$ . Сумма произведений этих чисел на алгебраические дополнения элементов  $i$ -й строки равна определителю, в матрице которого на месте  $a_{i1}, \dots, a_{in}$  стоят  $b_1, \dots, b_n$ :

$$b_1 A_{i1} + \dots + b_n A_{in} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ b_1 & \dots & b_n \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Действительно,

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ b_1 & \dots & b_n \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = b_1 A'_{i1} + \dots + b_n A'_{in},$$

где  $A'_{i1}, \dots, A'_{in}$  — алгебраические дополнения элементов  $i$ -й строки этого определителя. Но алгебраические дополнения не зависят от элементов  $i$ -й строки, так что они совпадают с алгебраическими дополнениями  $A_{i1}, \dots, A_{in}$  исходного определителя.

11. Сумма произведений элементов какой-либо строки на алгебраические дополнения элементов другой строки равна нулю (свойство ортогональности строк и алгебраических дополнений).

Действительно, пусть дан определитель

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Тогда, по предыдущему свойству,

$$a_{k1} A_{i1} + a_{k2} A_{i2} + \dots + a_{kn} A_{in} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = 0,$$

ибо получился определитель с двумя одинаковыми строками.

Следующее свойство касается вычисления алгебраических дополнений.

*Минором* порядка  $n - 1$  для данного определителя называется определитель матрицы, получающейся из матрицы исходного определителя посредством вычеркивания одной строки и одного столбца. Минор, получающийся вычеркиванием строки и столбца, содержащих  $a_{ik}$ , обозначается через  $\Delta_{ik}$ .

12. *Алгебраическое дополнение*  $A_{ik}$  отличается от соответствующего минора  $\Delta_{ik}$  лишь на множитель  $(-1)^{i+k}$  (т. е.  $A_{ik} = \Delta_{ik}$  или  $A_{ik} = -\Delta_{ik}$  в зависимости от того, четно или нечетно число  $i + k$ ).

При доказательстве рассмотрим два случая. Сначала положим  $i = k = 1$ :

$$A_{11} = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Согласно определению

$$A_{11} = \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)} a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n},$$

причем нужно положить  $a_{11} = 1$ ,  $a_{1k} = 0$  при  $k = 2, \dots, n$  и  $a_{i1} = 0$  при  $i = 2, 3, \dots, n$ . Поэтому в сумме нужно сохранить только слагаемые при  $\alpha_1 = 1$  и  $(\alpha_2, \dots, \alpha_n)$ , пробегающей все перестановки чисел  $2, 3, \dots, n$ , причем положить  $a_{11} = 1$ . Получаем

$$A_{11} = \sum_{(\alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(1, \alpha_2, \dots, \alpha_n)} a_{2\alpha_2} \dots a_{n\alpha_n}.$$

Ясно, что  $\text{inv}(1, \alpha_2, \dots, \alpha_n) = \text{inv}(\alpha_2, \dots, \alpha_n)$ , ибо 1 на первом месте не образует инверсий с другими элементами. Поэтому

$$A_{11} = \sum_{(\alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_2, \dots, \alpha_n)} a_{2\alpha_2} \dots a_{n\alpha_n} = \begin{vmatrix} a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Для того чтобы установить последнее равенство, достаточно воспользоваться определением определителя для  $\begin{vmatrix} a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n2} & \dots & a_{nn} \end{vmatrix}$ , учи-

тывая, что вторые индексы на единицу больше номеров столбцов в этом определителе, так что  $\text{inv}(\alpha_2, \dots, \alpha_n)$  равно числу инверсий в номерах столбцов. Итак,  $A_{11} = \Delta_{11}$ .

Теперь пусть  $i$  и  $k$  любые:

$$A_{ik} = \begin{vmatrix} a_{11} & \dots & a_{1, k-1} & 0 & a_{1, k+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i-1, 1} & \dots & a_{i-1, k-1} & 0 & a_{i-1, k+1} & \dots & a_{i-1, n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1, 1} & \dots & a_{i+1, k-1} & 0 & a_{i+1, k+1} & \dots & a_{i+1, n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n, k-1} & 0 & a_{n, k+1} & \dots & a_{nn} \end{vmatrix}.$$

Переместим 1 в левый верхний угол, сохранив порядок остальных строк и столбцов. С этой целью поменяем местами  $i$ -ю строку последовательно со всеми предыдущими, а затем то же сделаем с  $k$ -м столбцом. Определитель при этом приобретет множитель  $(-1)^{i-1+k-1}$ , так что

$$A_{ik} = (-1)^{i+k} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_{11} & \dots & a_{1, k-1} & a_{1, k+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{i-1, 1} & \dots & a_{i-1, k-1} & a_{i-1, k+1} & \dots & a_{i-1, n} \\ 0 & a_{i+1, 1} & \dots & a_{i+1, k-1} & a_{i+1, k+1} & \dots & a_{i+1, n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{n1} & \dots & a_{n, k-1} & a_{n, k+1} & \dots & a_{nn} \end{vmatrix}.$$

В силу рассмотренного ранее случая  $i = k = 1$  заключаем, что

$$A_{ik} = (-1)^{i+k} \begin{vmatrix} a_{11} & \dots & a_{1, k-1} & a_{1, k+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i-1, 1} & \dots & a_{i-1, k-1} & a_{i-1, k+1} & \dots & a_{i-1, n} \\ a_{i+1, 1} & \dots & a_{i+1, k-1} & a_{i+1, k+1} & \dots & a_{i+1, n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n, k-1} & a_{n, k+1} & \dots & a_{nn} \end{vmatrix} = (-1)^{i+k} \Delta_{ik},$$

что и требовалось доказать.

**6. Вычисление определителей.** Для того чтобы вычислить определитель, пользуясь определением этого выражения, нужно вычислить  $n!$  произведений  $n$  сомножителей, каждое из которых равносильно  $n - 1$  попарных умножений чисел. Таким образом, для вычисления определителя этим способом требуется  $n!(n - 1)$  попарных умножений и много сложений, которых мы не учитываем как значительно менее трудоемкую операцию. Так, при  $n = 100$  число умножений равно  $100!99 > 10^{153}$ . Никакая самая мощная вычислительная машина не в состоянии справиться с таким числом операций.

Теперь посмотрим, как можно воспользоваться свойствами определителя. Разложение по строке (или по столбцу) показывает, что вычисление определителя порядка  $n$  в основном сводится к вычислению  $n$  определителей порядка  $n - 1$ . Но если в строке есть нули, то нужно столько определителей порядка  $n - 1$ , сколько имеется отличных от нуля элементов в строке (в столбце). Но при помощи добавления к строкам чисел, пропорциональных другим строкам, можно получать нули в столбцах.

Проследим за этим. Пусть нам нужно вычислить определитель

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Положим для простоты, что  $a_{11} \neq 0$ . Вынесем из первой строки  $a_{11}$  за знак определителя:

$$a_{11} \begin{vmatrix} 1 & \frac{a_{12}}{a_{11}} & \dots & \frac{a_{1n}}{a_{11}} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

При этом нам нужно выполнить  $n - 1$  деление (деление и умножение считаются одинаковыми по сложности операциями).

Далее, прибавим ко второй строке первую, умноженную на  $-a_{21}$ , к третьей — первую, умноженную на  $-a_{31}$ , и т. д. При этом нужно сделать  $(n - 1)^2$  умножений и столько же сложений. Получится определитель вида

$$a_{11} \begin{vmatrix} 1 & \frac{a_{12}}{a_{11}} & \dots & \frac{a_{1n}}{a_{11}} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a'_{n2} & \dots & a'_{nn} \end{vmatrix}.$$

Для этого перехода нужно  $n - 1 + (n - 1)^2 = n(n - 1)$  умножений и делений и  $(n - 1)^2$  сложений.

Но теперь разложение по первому столбцу сводит задачу к вычислению одного определителя  $(n - 1)$ -го порядка, и процесс нужно продолжить дальше. Всего для перехода к определителю первого порядка, т. е. к одному числу, нужно  $n(n - 1) + \dots + 2 \cdot 1 = \frac{n^3 - n}{3}$  умножений и делений и  $(n - 1)^2 + \dots + 1^2 = \frac{n(n - 1)(2n - 1)}{6}$  сложений.

После этого нужно последнее число (определитель первого порядка) умножить на  $n - 1$  множителей, которые выносились за знак определителя. Это требует еще  $n - 1$  попарных умножений.

Всего при  $n = 100$  нужно  $\frac{100^3 - 100}{3} + 99 = 333\,399$  умножений и делений и  $\frac{100 \cdot 99 \cdot 199}{6} = 328\,350$  сложений.

Современная ЭВМ, способная производить несколько миллионов операций в секунду, легко справится с таким вычислением.

При практических вычислениях все может проходить не так благополучно, как в теоретическом описании. Возможно, что в левом верхнем углу очередной матрицы окажется нуль или число, близкое к нулю. Это обстоятельство заставляет выбирать так называемый ведущий элемент — по возможности, наибольший в строке или во всей матрице, на который производится деление строки. Но это значительно усложняет программу при машинном проведении вычислений.

Мы не будем приводить примеров вычисления численно заданных определителей типа таких, которые могут встретиться в приложениях, например,

$$\begin{vmatrix} 1,325 & 2,427 & 1,215 & -0,647 \\ 2,354 & -1,621 & 3,514 & 0,812 \\ -1,117 & -2,311 & 1,511 & -1,212 \\ 2,123 & 1,427 & -1,211 & 2,531 \end{vmatrix}.$$

Ясно, что для вычисления такого определителя нужны хотя бы несложные вычислительные средства.

Мы рассмотрим примеры другого рода, не требующие вычислительных средств, но нуждающиеся в проявлении известной сообразительности при применении свойств определителей.

**Пример 1.** Вычислить

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{vmatrix}.$$

Квадратная матрица, в которой все элементы ниже главной диагонали равны нулю, называется *верхней* (или *правой*) *треугольной*. (Заметим, что главной диагональю квадратной матрицы называется последовательность элементов, стоящих в позициях  $(1, 1)$ ,  $(2, 2)$ , ...,  $(n, n)$ .)

Ясно, что определитель треугольной матрицы равен произведению  $a_{11}a_{22} \dots a_{nn}$  элементов ее главной диагонали, ибо это произведение есть единственное слагаемое, отличное от нуля.

**Пример 2.** Вычислить

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & a_2 & 1 & \dots & 1 \\ 1 & 1 & a_3 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & a_n \end{vmatrix}.$$

Здесь естественно ко всем строкам прибавить первую, умноженную на  $-1$ . Тогда получится определитель:

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & a_2 - 1 & 0 & \dots & 0 \\ 0 & 0 & a_3 - 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_n - 1 \end{vmatrix} = (a_2 - 1)(a_3 - 1) \dots (a_n - 1).$$

**Пример 3.** Вычислить определитель порядка  $n$

$$\Delta_n = \begin{vmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix}.$$

Если бы вместо 0 в левом верхнем углу находилась 1, мы легко вычислили бы определитель, подобно примеру 2. Прибавим все строки к первой. Получим

$$\Delta_n = \begin{vmatrix} n-1 & n-1 & n-1 & \dots & n-1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix} = (n-1) \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix}.$$

Остается вычесть первую строку из всех остальных. Получим:

$$\Delta_n = (n-1) \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 \end{vmatrix} = (-1)^{n-1} (n-1).$$

Пример 4. Вычислить

$$\Delta_n = \begin{vmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \\ n-1 & n & 1 & \dots & n-2 \\ \dots & \dots & \dots & \dots & \dots \\ 2 & 3 & 4 & \dots & 1 \end{vmatrix}.$$

В строках циклически передвигаются 1, 2, 3, ..., n. Прибавим к последней строке все предшествующие. Получим:

$$\Delta_n = \frac{n(n+1)}{2} \begin{vmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \\ n-1 & n & 1 & \dots & n-2 \\ \dots & \dots & \dots & \dots & \dots \\ 3 & 4 & 5 & \dots & 2 \\ 1 & 1 & 1 & \dots & 1 \end{vmatrix}.$$

Теперь получим нули в последней строке, вычитая из каждого столбца предыдущий (из последнего предпоследний, из предпоследнего предшествующий и т. д.):

$$\begin{aligned} \Delta_n &= \frac{n(n+1)}{2} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ n & 1-n & 1 & \dots & 1 \\ n-1 & 1 & 1-n & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 3 & 1 & 1 & \dots & 1-n & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{vmatrix} = \\ &= \frac{n(n+1)}{2} (-1)^{n+1} \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1-n & 1 & \dots & 1 \\ 1 & 1-n & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1-n & 1 \end{vmatrix}. \end{aligned}$$

Теперь вычтем первую строку из всех последующих:

$$\Delta_n = \frac{n(n+1)}{2} (-1)^{n+1} \begin{vmatrix} 1 & 1 & \dots & 1 \\ -n & 0 & \dots & 0 \\ 0 & -n & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -n & 0 \end{vmatrix}.$$

Разложение по последнему столбцу дает

$$\begin{aligned} \Delta_n &= \frac{n(n+1)}{2} (-1)^{n+1} (-1)^n \begin{vmatrix} -n & 0 & \dots & 0 \\ 0 & -n & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -n \end{vmatrix} = \\ &= \frac{n(n+1)}{2} (-1)^{n+1+n+n-2} n^{n-2} = (-1)^{n-1} \frac{n^{n-1}(n+1)}{2}. \end{aligned}$$

При решении последних примеров мы довольно смело составляли линейные комбинации строк. Однако при этом важно следить, чтобы не прибавлять в неизменном виде строку, изменившуюся в процессе предыдущих преобразований. Иначе можно, например, «доказать», что любой определитель равен нулю. Вот это «доказательство»: дан определитель. Прибавим первую строку ко второй и вторую к первой. Получим определитель с двумя одинаковыми строками, а он равен нулю. Ошибка в этом «доказательстве» состоит именно в том, что вторая строка уже изменилась после прибавления к ней первой строки, и прибавлять ее к первой можно только в этом измененном виде — только тогда можно говорить о сохранении величины определителя.

### 7. Определитель Вандермонда. Определитель вида

$$\Delta_n(x_1, x_2, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}$$

называется *определителем Вандермонда* и имеет некоторое теоретическое значение, так как возникает в различных ситуациях.

Подсчитаем определитель Вандермонда для  $n=2$  и  $n=3$ . Имеем

$$\Delta_2(x_1, x_2) = \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1.$$

При подсчете определителя третьего порядка

$$\Delta_3(x_1, x_2, x_3) = \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix}$$

вычтем из третьего столбца второй, умноженный на  $x_1$ , из второго — первый, умноженный на  $x_1$ . Получим:

$$\begin{aligned}\Delta_3(x_1, x_2, x_3) &= \begin{vmatrix} 1 & 0 & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_2 x_1 \\ 1 & x_3 - x_1 & x_3^2 - x_3 x_1 \end{vmatrix} = \\ &= \begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) \end{vmatrix} = (x_2 - x_1)(x_3 - x_1) \begin{vmatrix} 1 & x_2 \\ 1 & x_3 \end{vmatrix} = \\ &= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).\end{aligned}$$

Очевидно, что аналогичные рассуждения можно проводить и при больших  $n$ , и это дает основание сформулировать гипотезу:

$$\begin{aligned}\Delta_n(x_1, x_2, \dots, x_n) &= \\ &= (x_2 - x_1)(x_3 - x_1) \dots (x_n - x_1)(x_3 - x_2) \dots (x_n - x_2) \dots (x_n - x_{n-1}) = \\ &= \prod_{n \geq i > j \geq 1} (x_i - x_j).\end{aligned}$$

Докажем эту гипотезу методом математической индукции. Пусть она доказана для определителя порядка  $n-1$ . В определителе порядка  $n$  вычтем из каждого столбца предшествующий, умноженный на  $x_1$ :

$$\begin{aligned}\Delta_n(x_1, x_2, \dots, x_n) &= \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_2 x_1 & \dots & x_2^{n-1} - x_2^{n-2} x_1 \\ 1 & x_3 - x_1 & x_3^2 - x_3 x_1 & \dots & x_3^{n-1} - x_3^{n-2} x_1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n - x_1 & x_n^2 - x_n x_1 & \dots & x_n^{n-1} - x_n^{n-2} x_1 \end{vmatrix} = \\ &= (x_2 - x_1)(x_3 - x_1) \dots (x_n - x_1) \begin{vmatrix} 1 & x_2 & \dots & x_2^{n-2} \\ 1 & x_3 & \dots & x_3^{n-2} \\ \dots & \dots & \dots & \dots \\ 1 & x_n & \dots & x_n^{n-2} \end{vmatrix} = \\ &= (x_2 - x_1)(x_3 - x_1) \dots (x_n - x_1) \Delta_{n-1}(x_2, x_3, \dots, x_n).\end{aligned}$$

Мы можем применить предположение индукции:

$$\begin{aligned}\Delta_n(x_1, x_2, \dots, x_n) &= \\ &= (x_2 - x_1)(x_3 - x_1) \dots (x_n - x_1) \prod_{n \geq i > j \geq 2} (x_i - x_j) = \prod_{n \geq i > j \geq 1} (x_i - x_j).\end{aligned}$$

Формула доказана.

**8. Система  $n$  уравнений с  $n$  неизвестными с ненулевым определителем матрицы коэффициентов.** Дана система  $n$  линейных

уравнений с  $n$  неизвестными

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1,$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2,$$

$$\dots \dots \dots$$

$$a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n$$

с числовыми коэффициентами (результаты остаются в силе для системы уравнений с коэффициентами из любого поля).

Предполагаем, что  $D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \neq 0.$

Сначала допустим, что уравнение имеет решение и что  $x_1, x_2, \dots, x_n$  составляют решение, так что уравнения уже превратились в верные равенства. Обозначим через  $A_{ij}$  алгебраические дополнения  $a_{ij}$  в  $D$ .

Умножим первое из равенств системы на  $A_{11}$ , второе на  $A_{21}, \dots, n$ -е на  $A_{n1}$  и сложим. Получим

$$\begin{aligned} (a_{11}A_{11} + a_{21}A_{21} + \dots + a_{n1}A_{n1})x_1 + \\ + (a_{12}A_{11} + a_{22}A_{21} + \dots + a_{n2}A_{n1})x_2 + \dots \\ \dots + (a_{1n}A_{11} + a_{2n}A_{21} + \dots + a_{nn}A_{n1})x_n = \\ = b_1A_{11} + b_2A_{21} + \dots + b_nA_{n1}. \end{aligned}$$

Коэффициент при  $x_1$  есть определитель  $D$ , представленный в разложении по элементам первого столбца. Коэффициенты же при  $x_2, \dots, x_n$  все равны нулю, так как они суть суммы произведений алгебраических дополнений элементов первого столбца на элементы других столбцов. Таким образом, мы пришли к равенству

$$Dx_1 = b_1A_{11} + b_2A_{21} + \dots + b_nA_{n1}.$$

Таким же образом, умножив исходные равенства на алгебраические дополнения второго столбца, получим

$$Dx_2 = b_1A_{12} + b_2A_{22} + \dots + b_nA_{n2}$$

и т. д. Из этих равенств получим

$$x_1 = \frac{1}{D}(b_1A_{11} + b_2A_{21} + \dots + b_nA_{n1}),$$

$$x_2 = \frac{1}{D}(b_1A_{12} + b_2A_{22} + \dots + b_nA_{n2}),$$

$$\dots \dots \dots$$

$$x_n = \frac{1}{D}(b_1A_{1n} + b_2A_{2n} + \dots + b_nA_{nn}).$$

Тем самым мы показали, что если решение существует, то оно единственно и дается формулами, которые мы установили.

Теперь нужно доказать, что решение существует, т. е. что формулы для  $x_1, x_2, \dots, x_n$  действительно дают решение.

Имеем

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1(a_{11}A_{11} + a_{12}A_{12} + \dots + a_{1n}A_{1n}) + \\ &+ b_2(a_{11}A_{21} + a_{12}A_{22} + \dots + a_{1n}A_{2n}) + \dots \\ &\dots + b_n(a_{11}A_{n1} + a_{12}A_{n2} + \dots + a_{1n}A_{nn}). \end{aligned}$$

Здесь коэффициент при  $b_1$  равен  $D$  в форме разложения по элементам первой строки, коэффициенты же при  $b_2, \dots, b_n$  равны нулю как суммы элементов первой строки на алгебраические дополнения других строк.

Аналогичным образом, с использованием тех же свойств определителя, проверяется, что найденные  $x_1, x_2, \dots, x_n$  удовлетворяют и всем остальным уравнениям.

Тем самым мы доказали теорему о существовании и единственности решения системы  $n$  линейных уравнений с  $n$  неизвестными с ненулевым определителем матрицы коэффициентов. Эта теорема носит название *теоремы Крамера*.

Формулы для решения можно преобразовать, учитывая, что

$$b_1A_{11} + b_2A_{12} + \dots + b_nA_{1n} = \begin{vmatrix} b_1 & a_{12} & \dots & a_{1n} \\ b_2 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ b_n & a_{n2} & \dots & a_{nn} \end{vmatrix},$$

и аналогично преобразовать остальные числители. Получим

$$x_1 = \frac{D_1}{D}, \quad x_2 = \frac{D_2}{D}, \quad \dots, \quad x_n = \frac{D_n}{D},$$

где  $D_i$  есть определитель, матрица которого отличается от матрицы определителя  $D$  только  $i$ -м столбцом, в который помещены  $b_1, b_2, \dots, b_n$ . Эти формулы носят название *формул Крамера*. Раньше мы их получили для  $n = 2$  и  $n = 3$ .

### 9. Некоторые следствия из теоремы Крамера.

**Следствие 1.** Если известно, что система  $n$  линейных уравнений с  $n$  неизвестными не имеет решений, то определитель матрицы из коэффициентов системы равен нулю.

Действительно, если бы определитель был отличен от нуля, то система имела бы решение.

**Следствие 2.** Если система  $n$  линейных уравнений с  $n$  неизвестными имеет более чем одно решение, то определитель матрицы из ее коэффициентов равен нулю.

Действительно, иначе система имела бы единственное решение.

Система линейных уравнений называется *однородной*, если все ее свободные члены равны нулю. Однородная система (независимо от числа уравнений) всегда имеет решение, состоящее из нулевых значений для всех неизвестных. Для однородных систем представ-

ляет интерес вопрос о том, является ли нулевое решение единственным или кроме него существуют другие, нетривиальные, решения.

**Следствие 3.** *Для того чтобы система  $n$  линейных однородных уравнений с  $n$  неизвестными имела нетривиальные решения, необходимо, чтобы определитель матрицы из ее коэффициентов был равен нулю.*

Действительно, если хотя бы одно нетривиальное решение имеется, то система имеет более чем одно решение, так как нулевое всегда есть. Следовательно, определитель матрицы из коэффициентов системы равен нулю.

### § 3. Линейная зависимость и линейная независимость строк (столбцов)

**1. Определение и простейшие свойства.** Напоминаем, что *линейной комбинацией* строк (или вообще матриц)  $u_1, u_2, \dots, u_m$  называется строка (матрица)  $c_1u_1 + c_2u_2 + \dots + c_mu_m$ , где  $c_i$  — числа (элементы основного поля). Ясно, что если все коэффициенты равны нулю, то линейная комбинация равна нулевой строке.

Совокупность строк  $u_1, u_2, \dots, u_m$  называется *линейно зависимой*, если существуют коэффициенты  $c_1, c_2, \dots, c_m$ , не равные нулю одновременно, такие, что  $c_1u_1 + c_2u_2 + \dots + c_mu_m = 0$  (здесь 0 обозначает нулевую строку). Если же такие коэффициенты не существуют, т. е. из равенства  $c_1u_1 + c_2u_2 + \dots + c_mu_m = 0$  следует, что все коэффициенты  $c_1, c_2, \dots, c_m$  равны нулю, то совокупность строк называется *линейно независимой*.

Так, например, строки  $u_1 = (1, 1, 1)$ ,  $u_2 = (-1, 2, 1)$ ,  $u_3 = (1, 4, 3)$  линейно зависимы, ибо  $2u_1 + u_2 - u_3 = (0, 0, 0)$ . А строки  $u_1 = (1, 1)$ ,  $u_2 = (-1, 2)$  линейно независимы, ибо из  $c_1u_1 + c_2u_2 = 0$  следует

$$\begin{aligned} c_1 - c_2 &= 0, \\ c_1 + 2c_2 &= 0, \end{aligned}$$

откуда  $c_1 = c_2 = 0$ .

**Предложение 1.** *Для того чтобы совокупность строк была линейно зависимой, необходимо и достаточно, чтобы хотя бы одна из строк была линейной комбинацией остальных.*

Действительно, пусть совокупность строк  $u_1, u_2, \dots, u_m$  линейно зависима. Это значит, что существуют  $c_1, c_2, \dots, c_m$ , не равные одновременно нулю, такие, что  $c_1u_1 + c_2u_2 + \dots + c_mu_m = 0$ . Пусть  $c_i \neq 0$ . Тогда

$$u_i = -\frac{c_1}{c_i}u_1 - \dots - \frac{c_{i-1}}{c_i}u_{i-1} - \frac{c_{i+1}}{c_i}u_{i+1} - \dots - \frac{c_m}{c_i}u_m.$$

Необходимость доказана.

Пусть теперь  $u_i = c_1u_1 + \dots + c_{i-1}u_{i-1} + c_{i+1}u_{i+1} + \dots + c_mu_m$ . Тогда  $c_1u_1 + \dots + c_{i-1}u_{i-1} + (-1)u_i + c_{i+1}u_{i+1} + \dots + c_mu_m = 0$ , т. е. совокупность  $u_1, \dots, u_m$  линейно зависима.

Другая формулировка этого предложения:

*Для того чтобы совокупность строк была линейно независима, необходимо и достаточно, чтобы ни одна из строк не была линейной комбинацией остальных.*

Отметим еще некоторые очевидные предложения, касающиеся свойств линейной зависимости и независимости.

Ясно, что *любая совокупность строк, содержащая нулевую строку, линейно зависима*. Действительно, нулевая строка есть линейная комбинация остальных строк с нулевыми коэффициентами. Столь же ясно, что *всякая совокупность строк, содержащая две равные или две пропорциональные строки, линейно зависима*. Далее, *если совокупность строк линейно зависима, то всякая большая совокупность будет тоже линейно зависима*. Наконец, *если совокупность строк линейно независима, то и всякая ее часть линейно независима*.

**Предложение 2.** Пусть строки  $u_1, \dots, u_m$  составляют линейно независимую совокупность, а строки  $u_1, \dots, u_m, u_{m+1}$  — линейно зависимую. Тогда  $u_{m+1}$  есть линейная комбинация  $u_1, \dots, u_m$ .

Действительно, в равенстве  $c_1 u_1 + \dots + c_m u_m + c_{m+1} u_{m+1} = 0$  с не равными одновременно нулю коэффициентами коэффициент  $c_{m+1}$  отличен от 0, так как иначе совокупность  $u_1, \dots, u_m$  была бы линейно зависимой. Следовательно,

$$u_{m+1} = -\frac{c_1}{c_{m+1}} u_1 - \dots - \frac{c_m}{c_{m+1}} u_m.$$

Строку  $\tilde{u} = (a_1, \dots, a_k)$  будем называть *отрезком строки*  $u = (a_1, \dots, a_k, \dots, a_n)$ .

**Предложение 3.** Если между строками  $u_1, \dots, u_m$  имеется линейная зависимость, то такая же зависимость имеет место и для их отрезков  $\tilde{u}_1, \dots, \tilde{u}_m$  фиксированной длины.

Действительно, равенство  $c_1 u_1 + \dots + c_m u_m = 0$  означает, что все компоненты строки  $c_1 u_1 + \dots + c_m u_m$  равны нулю, а равенство  $c_1 \tilde{u}_1 + \dots + c_m \tilde{u}_m = 0$  означает то же самое для компонент, входящих в отрезки.

Отсюда непосредственно следует, что если некоторые отрезки строк  $u_1, \dots, u_m$  линейно независимы, то и сами строки  $u_1, \dots, u_m$  составляют линейно независимую совокупность.

**2. Линейные зависимости столбцов матрицы с линейно зависимыми строками.**

**Предложение 4.** Пусть  $u_1, \dots, u_m$  — строки матрицы

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix},$$

причем строки  $u_{k+1}, \dots, u_m$  являются линейными комбинациями строк  $u_1, \dots, u_k$ . Пусть, далее,  $v_1, \dots, v_n$  — столбцы матрицы  $A$ ,





**Теорема 6.** *Все строки данного конечного или бесконечного множества строк длины  $n$  являются линейными комбинациями строк любого максимального линейно независимого подмножества.*

**Доказательство.** Пусть  $u_1, \dots, u_m$  — строки, образующие максимальное линейно независимое подмножество, и пусть  $u$  — какая-либо строка исходного множества. Тогда совокупность  $u_1, \dots, u_m, u$  линейно зависима и, как мы видели выше,  $u$  есть линейная комбинация  $u_1, \dots, u_m$ .

Линейно независимая совокупность строк, линейными комбинациями которых являются все строки рассматриваемого множества, называется *базисной* или *фундаментальной* совокупностью, короче, *базисом* данного множества строк.

**Предложение 7.** *Число строк, составляющих базис, не зависит от его выбора.*

Действительно, пусть  $u_1, \dots, u_m$  и  $v_1, \dots, v_k$  — два базиса одного и того же множества строк. Так как  $v_1, \dots, v_k$  — линейно независимая совокупность строк, являющихся линейными комбинациями строк  $u_1, \dots, u_m$ , должно быть  $k \leq m$ . По тем же соображениям  $m \leq k$ , так что  $m = k$ , что и требовалось доказать.

Число строк, составляющих базис данной совокупности строк, называется *рангом* этой совокупности.

Разумеется, тот же термин применяется к совокупностям столбцов.

**Предложение 8.** *Даны две совокупности строк такие, что вторая из них содержит первую. Если их ранги одинаковы, то все строки второй совокупности являются линейными комбинациями строк первой совокупности.*

Действительно, выберем базис первой совокупности. Так как ранги равны, выбранные строки образуют базис и для второй совокупности, и все ее строки являются линейными комбинациями этого базиса.

**5. Линейно эквивалентные совокупности строк.** Две совокупности строк  $u_1, \dots, u_m$  и  $v_1, \dots, v_k$  называются *линейно эквивалентными*, если каждая строка первой совокупности есть линейная комбинация строк второй совокупности и каждая строка второй совокупности есть линейная комбинация строк первой.

**Предложение 9.** *Ранги линейно эквивалентных совокупностей строк равны.*

**Доказательство.** Пусть  $r$  — ранг второй совокупности. Это значит, что все строки второй совокупности являются линейными комбинациями базиса, состоящего из  $r$  строк. Но тогда и строки первой совокупности, будучи линейными комбинациями линейных комбинаций этих  $r$  строк, сами являются их линейными комбинациями. Следовательно, ранг первой совокупности не больше  $r$ , т. е. ранга второй совокупности. По аналогичной причине ранг второй совокупности не больше ранга первой. Следовательно эти ранги равны.

**6. Ранг матрицы.** С данной прямоугольной матрицей связывается множество ее строк и множество ее столбцов. Каждое из них имеет ранг. Замечательно то, что эти ранги равны.

**Теорема 10.** *Ранг множества строк прямоугольной матрицы равен рангу множества ее столбцов.*

**Доказательство.** Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Пусть ранг множества ее строк равен  $k$ . Тогда найдется базис из  $k$  строк, т. е. такое линейно независимое множество строк, что все остальные строки являются их линейными комбинациями. Для упрощения записи будем считать, что это первые  $k$  строк, иначе мы изменили бы нумерацию. Введем в рассмотрение матрицу из этих строк

$$\tilde{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}.$$

Столбцы матрицы  $\tilde{A}$  являются отрезками столбцов матрицы  $A$ .

Выберем базис столбцов матрицы  $\tilde{A}$ . Пусть число столбцов, составляющих базис, равно  $r$ . Все столбцы матрицы  $\tilde{A}$  являются их линейными комбинациями. Ясно, что  $r \leq k$ . Пополним выбранные базисные столбцы до полных столбцов матрицы  $A$ . Получившиеся столбцы линейно независимы, и, в силу предложения 4, все столбцы матрицы  $A$  являются их линейными комбинациями. Таким образом, мы построили базис множества столбцов матрицы  $A$ , состоящий из  $r$  столбцов, причем  $r \leq k$ . Итак, ранг  $r$  множества столбцов матрицы  $A$  не превосходит ранга  $k$  множества ее строк. Но по тем же соображениям ранг  $k$  множества строк не превосходит ранга  $r$  множества столбцов. Следовательно, эти ранги равны. Их величина называется *рангом* матрицы.

**7. Условие линейной зависимости множества строк квадратной матрицы.**

**Теорема 11.** *Для линейной зависимости множества строк квадратной матрицы необходимо и достаточно обращение в нуль ее определителя.*

**Доказательство.** **Необходимость.** Допустим, что  $\det A \neq 0$ , где

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$





Матрица вида

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1k} & c_{1,k+1} & \dots & c_{1n} \\ 0 & c_{22} & \dots & c_{2k} & c_{2,k+1} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_{kk} & c_{k,k+1} & \dots & c_{kn} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

при  $c_{11} \neq 0, c_{22} \neq 0, \dots, c_{kk} \neq 0$  называется *верхней трапецевидной*. Легко видеть, что ранг трапецевидной матрицы равен  $k$ . Действительно, минор

$$\begin{vmatrix} c_{11} & c_{12} & \dots & c_{1k} \\ 0 & c_{22} & \dots & c_{2k} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_{kk} \end{vmatrix} = c_{11}c_{22} \dots c_{kk}$$

отличен от нуля, все же миноры порядка  $k+1$  и выше равны нулю, так как у них имеется хотя бы одна нулевая строка.

**Предложение 14.** *Любая матрица за счет элементарных преобразований над строками и, быть может, перестановок столбцов может быть преобразована в трапецевидную.*

**Доказательство.** Если матрица не нулевая, она содержит ненулевой элемент, который посредством перестановок строк и столбцов можно перевести в левый верхний угол.

Итак, пусть матрица имеет вид

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \text{ причем } a_{11} \neq 0.$$

Теперь сделаем элементарные преобразования: ко второй строке прибавим первую, умноженную на  $-a_{21}/a_{11}$ , к третьей — первую, умноженную на  $-a_{31}/a_{11}$ , и т. д. После этих преобразований придём к матрице

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix}.$$

Если матрица  $\begin{pmatrix} a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots \\ a'_{m2} & \dots & a'_{mn} \end{pmatrix}$  равна нулю, процесс окончен

Если нет — то сначала за счет перестановок строк и столбцов добьемся того, чтобы элемент в позиции  $a'_{22}$  стал отличен от нуля.







Две системы линейных уравнений называются *линейно эквивалентными*, если каждое уравнение первой системы есть линейная комбинация уравнений второй системы и каждое уравнение второй системы есть линейная комбинация уравнений первой системы. Линейно эквивалентные системы эквивалентны и в обычном смысле — они одновременно совместны или несовместны и, в случае совместности, имеют одинаковые множества решений.

*Элементарными преобразованиями* системы линейных уравнений называем умножение уравнения на отличное от нуля число, перестановку уравнений местами и прибавление к одному уравнению другого, умноженного на некоторое число. Ясно, что элементарные преобразования переводят систему в линейно эквивалентную.

**Теорема 6.** *Любая система линейных уравнений приводится посредством элементарных преобразований и, быть может, изменения нумерации неизвестных к системе с трапецевидной матрицей. В частности, для системы  $n$  уравнений с  $n$  неизвестными с не равным нулю определителем матрицы коэффициентов система приводится к системе с треугольной матрицей.*

**Доказательство.** Сделаем последовательность элементарных преобразований так, чтобы матрица коэффициентов привелась к трапецевидной форме. Возможно, что при этом придется изменить нумерацию неизвестных (и соответствующих столбцов матрицы коэффициентов). Если ранг  $r$  матрицы коэффициентов меньше числа уравнений  $m$ , то система примет вид:

$$\begin{array}{ccccccccccc} c_{11}x_1 + \dots + c_{1r}x_r + c_{1,r+1}x_{r+1} + \dots + c_{1n}x_n & = & d_1, \\ \dots & & \dots \\ c_{rr}x_r + c_{r,r+1}x_{r+1} + \dots + c_{rn}x_n & = & d_r, \\ & 0 & = & d_{r+1}, \\ & \dots & & \dots \\ & 0 & = & d_m. \end{array}$$

Равенства, следующие за  $r$ -м уравнением, могут быть противоречивы, если хотя бы одно из чисел  $d_{r+1}, \dots, d_m$  отлично от нуля. Если же все они равны нулю, то последние  $m - r$  равенств не несут никакой информации и могут быть отброшены. Тогда, если  $r < n$ , то неизвестным  $x_{r+1}, \dots, x_n$  можно придавать произвольные значения. Неизвестные  $x_1, \dots, x_r$  найдутся из решения системы с

треугольной матрицей  $\begin{pmatrix} c_{11} & \dots & c_{1r} \\ \dots & \dots & \dots \\ 0 & \dots & c_{rr} \end{pmatrix}$ . Эту систему удобно ре-

шать, определив из  $r$ -го уравнения  $x_r$ , затем из  $(r-1)$ -го  $x_{r-1}$  и т. д. Если сохранить за неизвестными  $x_{r+1}, \dots, x_n$  буквенные

обозначения, мы можем выразить через них  $x_1, \dots, x_r$  и получить общее решение системы. Если  $r = n$ , то система (в случае совместности) имеет единственное решение.

Если  $r = m = n$ , т. е. если матрица коэффициентов системы квадратная с не равным нулю определителем, этим способом решение системы сводится к решению системы с треугольной матрицей

$$\begin{array}{ccccccc} c_{11}x_1 + & \dots & + c_{1n}x_n = d_1, \\ & \dots & & & & & \\ & & & & & & c_{nn}x_n = d_n \end{array}$$

при  $c_{11} \neq 0, \dots, c_{nn} \neq 0$ . Обычно добиваются того, чтобы  $c_{11} = \dots = c_{rr} = 1$ . Для этого каждый раз, прежде чем добавлять с нужными множителями уравнение к последующим, делят обе части уравнения на коэффициент при исключаемой неизвестной (схема единственного деления метода Гаусса). Преобразование системы к системе с треугольной матрицей называется *прямым ходом* метода Гаусса. Последовательное вычисление неизвестных в порядке  $x_n, x_{n-1}, \dots, x_1$  называется *обратным ходом*. Легко подсчитать, что число арифметических действий при применении метода Гаусса ненамного больше числа арифметических действий для вычисления одного определителя. Метод Гаусса до настоящего времени остается одним из лучших методов решения систем линейных уравнений.

## § 5. Дальнейшие свойства определителей

**1. Теорема Лапласа.** Теорема, о которой будет идти речь в этом пункте, является глубоким обобщением разложения определителя по элементам строки. Пусть  $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$  — квадратная матрица порядка  $n$ .

Напомним, что минором порядка  $k$  для этой матрицы называется определитель матрицы, составленной из элементов, находящихся на пересечении некоторых выбранных  $k$  строк и  $k$  столбцов. В общем виде минор порядка  $k$  можно записать в форме

$$\begin{vmatrix} a_{\alpha_1\beta_1} & \dots & a_{\alpha_1\beta_k} \\ \dots & \dots & \dots \\ a_{\alpha_k\beta_1} & \dots & a_{\alpha_k\beta_k} \end{vmatrix}.$$

Здесь  $\alpha_1, \dots, \alpha_k$  — номера выбранных строк  $\alpha_1 < \alpha_2 < \dots < \alpha_k$ , и  $\beta_1, \dots, \beta_k$  — номера выбранных столбцов,  $\beta_1 < \beta_2 < \dots < \beta_k$ .

Минором, *дополнительным* к данному минору порядка  $k$ , называется минор порядка  $n - k$ , матрица которого получается из исходной посредством вычеркивания строк и столбцов, содержа-

щих данный минор. *Алгебраическим дополнением* к данному минору называется дополнительный минор с множителем  $(-1)^{\alpha_1+\dots+\alpha_k+\beta_1+\dots+\beta_k}$ .

**Теорема 1 (теорема Лапласа).** Пусть в матрице определителя выбраны  $k$  строк. Определитель равен сумме произведений всех миноров порядка  $k$ , составленных из этих строк, на их алгебраические дополнения.

Например, если для определителя

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix}$$

выбрать первые две строки, теорема Лапласа дает

$$\Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \cdot \begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix} - \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} a_{32} & a_{34} \\ a_{42} & a_{44} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{14} \\ a_{21} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{32} & a_{33} \\ a_{42} & a_{43} \end{vmatrix} + \\ + \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{34} \\ a_{41} & a_{44} \end{vmatrix} - \begin{vmatrix} a_{12} & a_{14} \\ a_{22} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{33} \\ a_{41} & a_{43} \end{vmatrix} + \begin{vmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{vmatrix}.$$

Доказательство теоремы Лапласа довольно громоздко. В конце курса, в главе, посвященной внешней алгебре, теорема Лапласа появится как почти очевидное утверждение.

Мы ограничимся доказательством важного частного случая, именно, формулой для определителя ступенчатой матрицы. *Ступенчатая* матрица устроена так:

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1m} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2m} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} & 0 & \dots & 0 \\ a_{m+1,1} & a_{m+1,2} & \dots & a_{m+1,m} & a_{m+1,m+1} & \dots & a_{m+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} & a_{n,m+1} & \dots & a_{nn} \end{vmatrix}.$$

Если к определителю ступенчатой матрицы применить теорему Лапласа, исходя из первых  $m$  строк, то лишь один минор будет отличен от нуля, именно, левый верхний, и его алгебраическим дополнением будет минор, составленный из последних  $n - m$  строк и столбцов.

Согласно теореме Лапласа

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{vmatrix} \cdot \begin{vmatrix} a_{m+1,m+1} & \dots & a_{m+1,n} \\ \dots & \dots & \dots \\ a_{n,m+1} & \dots & a_{nn} \end{vmatrix}.$$

Этот частный случай теоремы мы сейчас докажем. При  $m = 1$  утверждение теоремы очевидно. Далее проведем индукцию по порядку  $m$  минора из левого верхнего угла, допустив, что для левого верхнего углового минора порядка  $m - 1$  теорема верна. Введем следующие обозначения. Через  $\alpha_{11}, \alpha_{12}, \dots, \alpha_{1m}$  обозначим алгебраические дополнения элементов первой строки определителя

$\begin{vmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mm} \end{vmatrix}$ , через  $\delta_{11}, \delta_{12}, \dots, \delta_{1m}$  — соответствующие миноры.

Далее, через  $A_{11}, A_{12}, \dots, A_{1n}$  обозначим алгебраические дополнения элементов первой строки в определителе  $\det A$  и через  $\Delta_{11}, \Delta_{12}, \dots, \Delta_{1n}$  — соответствующие миноры.

Разложим определитель  $\det A$  по элементам первой строки. Получим

$$\det A = a_{11}A_{11} + \dots + a_{1m}A_{1m} = \\ = a_{11}\Delta_{11} - a_{12}\Delta_{12} + \dots + (-1)^{m+1}a_{1m}\Delta_{1m} = \sum_{k=1}^m (-1)^{k+1} a_{1k}\Delta_{1k}.$$

Присмотримся к тому, что представляет собой минор  $\Delta_{1k}$ . Его матрица получается вычеркиванием первой строки и  $k$ -го столбца из матрицы  $A$ . Останется снова ступенчатая матрица. Ее левый верхний угловой минор имеет порядок  $m - 1$ , и его матрица есть результат вычеркивания первой строки и  $k$ -го столбца из матрицы

$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mm} \end{pmatrix}$ . Правый нижний угловой минор такой же, как у матрицы  $A$ . В силу индуктивного предположения

$$\Delta_{1k} = \delta_{1k} \begin{vmatrix} a_{m+1, m+1} & \dots & a_{m+1, n} \\ \dots & \dots & \dots \\ a_{n, m+1} & \dots & a_{nn} \end{vmatrix}.$$

Поэтому

$$\det A = \sum_{k=1}^m (-1)^{k+1} a_{1k} \delta_{1k} \begin{vmatrix} a_{m+1, m+1} & \dots & a_{m+1, n} \\ \dots & \dots & \dots \\ a_{n, m+1} & \dots & a_{nn} \end{vmatrix} = \\ = \sum_{k=1}^m a_{1k} \alpha_{1k} \begin{vmatrix} a_{m+1, m+1} & \dots & a_{m+1, n} \\ \dots & \dots & \dots \\ a_{n, m+1} & \dots & a_{nn} \end{vmatrix} = \\ = \begin{vmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mm} \end{vmatrix} \cdot \begin{vmatrix} a_{m+1, m+1} & \dots & a_{m+1, n} \\ \dots & \dots & \dots \\ a_{n, m+1} & \dots & a_{nn} \end{vmatrix},$$

что и требовалось доказать.

Для приложений теории определителей теорема Лапласа, в основном, нужна именно в частном случае определителя ступенчатой матрицы.

Пример.

$$\begin{vmatrix} 1 & 2 & 0 & 0 & 0 & 0 \\ 3 & 4 & 0 & 0 & 0 & 0 \\ 5 & 6 & 1 & 2 & 3 & 0 & 0 \\ 7 & 8 & 2 & 3 & 4 & 0 & 0 \\ \pi & e & 3 & 1 & 2 & 0 & 0 \\ x & y & e^{-1} & c & d & 2 & 5 \\ u & v & \pi^2 & p & q & 3 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & 3 & 0 & 0 \\ 2 & 3 & 4 & 0 & 0 \\ 3 & 1 & 2 & 0 & 0 \\ e^{-1} & c & d & 2 & 5 \\ \pi^2 & p & q & 3 & 7 \end{vmatrix} = \\
 = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 1 & 2 \end{vmatrix} \cdot \begin{vmatrix} 2 & 5 \\ 3 & 7 \end{vmatrix} = (-2) \cdot (-3) \cdot (-1) = -6.$$

Мы дважды применили теорему об определителе ступенчатой матрицы.

2. Умножение матриц, разбитых на клетки. Пусть матрица разбита на части горизонтальными и вертикальными линиями, идущими через всю матрицу. Получившиеся части называются *блоками* или *клетками*, а исходная матрица называется *блочной* или *клеточной*. Блочную матрицу можно рассматривать как матрицу, элементами которой являются матрицы.

Оказывается, что основные действия над клеточными матрицами можно производить по тем же правилам, что и над матрицами из чисел (или из элементов данного поля). Но, разумеется, должны быть выполнены надлежащие требования на разбиения, чтобы все нужные действия имели смысл.

Если  $A$  и  $B$  — две матрицы одинакового строения и они разбиты на клетки одинаковым образом, то их можно складывать по клеткам. Это очевидно. Пусть теперь  $A$  есть  $m \times k$ -матрица,  $B$  есть  $k \times n$ -матрица,  $C = AB$ ,  $k = k_1 + \dots + k_s$ . Матрица  $A$  разбита на клетки  $A_{\alpha\beta}$ ,  $\alpha = 1, \dots, p$ ,  $\beta = 1, \dots, s$ , так, что ширины горизонтальных полос (в числе  $p$ ) безразличны, вертикальные же полосы имеют ширины  $k_1, \dots, k_s$ ; соответственно  $B$  разбита на клетки  $B_{\gamma\delta}$ ,  $\gamma = 1, \dots, s$ ,  $\delta = 1, \dots, q$ , ширины горизонтальных полос которых равны  $k_1, \dots, k_s$ , ширины вертикальных (в числе  $q$ ) безразличны. Матрицу  $C$  разобьем на клетки  $C_{\alpha\gamma}$  так, что горизонтальные полосы по ширине такие же, как соответствующие горизонтальные полосы матрицы  $A$ , а вертикальные полосы — как соответствующие вертикальные полосы матрицы  $B$ . В этих предположениях  $A_{\alpha\beta}B_{\beta\gamma}$  имеет смысл при любых  $\alpha, \beta, \gamma$  и  $C_{\alpha\gamma} = \sum_{\beta=1}^s A_{\alpha\beta}B_{\beta\gamma}$ .

Для доказательства рассмотрим два крайних случая. Сначала допустим, что матрица  $A$  разбита только на горизонтальные полосы  $A_1, \dots, A_p$ , матрица  $B$  — только на вертикальные полосы  $B_1, \dots, B_q$  и матрица  $C$  — соответственно на  $p$  полос по горизонтали и  $q$  полос по вертикали. В этом случае субматрица  $C_{\alpha\gamma}$  матрицы  $C$  есть произведение полосы  $A_\alpha$  на полосу  $B_\gamma$ .

Теперь допустим, что  $A$  разбита только на вертикальные полосы  $A_1, \dots, A_s$  ширины  $k_1, \dots, k_s$  соответственно и  $B$  разбита только на горизонтальные полосы  $B_1, \dots, B_s$  ширины  $k_1, \dots, k_s$  соответственно. В этой ситуации матрица  $C$  на клетки не разбивается. Имеем:

$$c_{ij} = (a_{i1}b_{1j} + \dots + a_{ik_1}b_{k_1j}) + (a_{i,k_1+1}b_{k_1+1,j} + \dots + a_{i,k_1+k_2}b_{k_1+k_2,j}) + \dots$$

Слагаемые в скобках суть элементы в позиции  $(i, j)$  матриц  $A_1B_1, A_2B_2, \dots$ . Поэтому  $C = A_1B_1 + A_2B_2 + \dots + A_sB_s$ .

Справедливость общего утверждения теперь получается непосредственно. Сначала нужно разбить  $A$  на горизонтальные полосы и  $B$  на вертикальные. Соответствующие клетки матрицы  $C$  равны произведениям горизонтальных полос матрицы  $A$  на вертикальные полосы матрицы  $B$ . Каждое такое произведение вычисляется согласно второму частному случаю как сумма произведений клеток матрицы  $A$ , на которые разбиты горизонтальные ее полосы, на клетки матрицы  $B$ , на которые разбиты ее вертикальные полосы.

3. Умножение матрицы на вспомогательную матрицу как линейное преобразование строк (столбцов). Рассмотрим произведение  $C = AB$  двух матриц  $A$  и  $B$ . Разобьем матрицу  $B$  на клетки, считая клетками столбцы  $B$ , матрицу  $A$  рассмотрим как состоящую из одной клетки. Соответствующими клетками их произведения  $C$  будут столбцы. Получим  $A(B_1, B_2, \dots, B_n) = (AB_1, AB_2, \dots, AB_n)$ . Здесь  $B_1, B_2, \dots, B_n$  — столбцы  $B$  и, соответственно,  $AB_1, AB_2, \dots, AB_n$  — столбцы  $C$ . С таким представлением произведения мы уже встречались.

Теперь примем за клетки  $B$  ее строки:

$$B = \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_k \end{bmatrix},$$

а за клетки  $A$  — ее элементы:  $A = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mk} \end{pmatrix}$ . В этом представлении

$$AB = \begin{bmatrix} a_{11}B_1 + \dots + a_{1k}B_k \\ a_{21}B_1 + \dots + a_{2k}B_k \\ \vdots \\ a_{m1}B_1 + \dots + a_{mk}B_k \end{bmatrix},$$

так что строками матрицы  $AB$  оказываются линейные комбинации строк  $B$ .

Аналогично, расщепление  $A$  на строки дает:

$$\begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} B = \begin{pmatrix} A_1 B \\ \vdots \\ A_m B \end{pmatrix},$$

расщепление же  $A$  на столбцы дает

$$(A_1, \dots, A_k) \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \dots & \vdots \\ b_{k1} & \dots & b_{kn} \end{pmatrix} = \\ = (b_{11}A_1 + \dots + b_{k1}A_k, \dots, b_{1n}A_1 + \dots + b_{kn}A_k).$$

Таким образом, умножение матрицы на некоторую вспомогательную матрицу слева равносильно линейному комбинированию строк матрицы, умножение справа — линейному комбинированию столбцов.

Рассмотрим матрицу  $e_{ij}$ ,  $i \neq j$ , элементами которой являются 1 на месте  $(i, j)$  и нули на остальных местах. Умножение слева некоторой матрицы на  $e_{ij}$  переставляет  $j$ -ю строку матрицы на  $i$ -е место, а все остальные строки заменяет нулями. Квадратная матрица  $E + ce_{ij}$  называется *матрицей трансвекции* или *матрицей элементарного преобразования*. Умножение слева на  $E + ce_{ij}$  равносильно прибавлению к  $i$ -й строке  $j$ -й строки, умноженной на  $c$ , с сохранением всех остальных строк. Такие преобразования неоднократно применялись нами по различным поводам. Умножение на  $e_{ij}$  справа переставляет  $i$ -й столбец на  $j$ -е место, заменяя нулями остальные столбцы. Умножение справа на  $E + ce_{ij}$  равносильно добавлению к  $i$ -му столбцу  $j$ -го, умноженного на  $c$ .

Треугольная матрица называется *унитреугольной*, если все элементы ее главной диагонали равны 1. Выясним, как изменяются строки матрицы  $A$  при умножении ее слева на правую унитреугольную матрицу  $C$ . Пусть

$$C = \begin{pmatrix} 1 & c_{12} & \dots & c_{1m} \\ 0 & 1 & \dots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \text{ и } A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}.$$

Здесь  $A_1, \dots, A_m$  — строки матрицы  $A$ .

Имеем:

$$CA = \begin{pmatrix} A_1 + c_{12}A_2 + \dots + c_{1m}A_m \\ A_2 + \dots + c_{2m}A_m \\ \vdots \\ A_m \end{pmatrix},$$

так что первая строка получена из первой строки  $A$  прибавлением последующих строк, умноженных на  $c_{12}, \dots, c_{1m}$ , вторая — из

второй прибавлением последующих строк с соответствующими множителями и т. д., последняя остается без изменения.

Если  $A$  — квадратная матрица, то при всех описанных преобразованиях определитель матрицы не изменяется, так что  $\det CA = \det A$ .

Если  $C$  — левая унитреугольная матрица

$$C = \begin{pmatrix} 1 & 0 & \dots & 0 \\ c_{21} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & 1 \end{pmatrix},$$

то

$$CA = \begin{pmatrix} A_1 \\ c_{21}A_1 + A_2 \\ \dots \\ c_{m1}A_1 + c_{m2}A_2 + \dots + A_m \end{pmatrix},$$

и здесь описание преобразований удобно начинать с конца: к последней строке прибавляются предшествующие, умноженные на  $c_{m1}, c_{m2}, \dots, c_{m, m-1}$ , к предпоследней — предшествующие, умноженные на соответствующие элементы матрицы  $C$ , и т. д.; ко второй строке прибавляется первая, умноженная на  $c_{21}$ , и первая остается без изменения. Поэтому и в этом случае  $\det CA = \det A$ .

При правом умножении на унитреугольную матрицу  $C$  происходят аналогичные преобразования столбцов, поэтому также  $\det AC = \det A$ .

**4. Определитель произведения двух квадратных матриц.** Имеет место следующая замечательная теорема:

**Теорема 2.** *Определитель произведения двух квадратных матриц равен произведению определителей сомножителей.*

Теорема эта представляет собой глубокое тождество, непосредственная проверка которого требует некоторых усилий даже для  $n = 2$ . Выполним эту проверку. Пусть  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ .

Тогда  $AB = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}$  и

$$\begin{aligned} \det AB &= (ax + bz)(cy + dt) - (ay + bt)(cx + dz) = \\ &= axcy + axdt + bzcy + bzdt - aycx - aydz - btcx - bdtz = \\ &= adxt + bcyz - adyz - bcxt = (ad - bc)(xt - yz) = \det A \det B. \end{aligned}$$

О непосредственной проверке теоремы даже для  $n = 3$  страшно подумать. Тем не менее, у нас уже имеется достаточно сведений об определителях и матрицах для того, чтобы дать краткое косвенное доказательство теоремы.

**Доказательство.** Пусть  $A$  и  $B$  — две квадратные матрицы порядка  $n$ . Рассмотрим матрицу  $\begin{pmatrix} A & 0 \\ -E & B \end{pmatrix}$  порядка  $2n$ . По

теореме об определителе ступенчатой матрицы  $\det \begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \det A \det B$ . Умножим теперь эту матрицу слева на унитреугольную матрицу  $\begin{pmatrix} E & A \\ 0 & E \end{pmatrix}$ . При этом определитель не изменится. Таким образом,

$$\det A \det B = \det \begin{pmatrix} E & A \\ 0 & E \end{pmatrix} \begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \det \begin{pmatrix} 0 & AB \\ -E & B \end{pmatrix}.$$

В последнем определителе поменяем местами первый столбец с  $(n+1)$ -м; второй с  $(n+2)$ -м и т. д. Это равносильно перестановке блоков-столбцов. Определитель приобретет множитель  $(-1)^n$ . Итак,

$$\det A \det B = (-1)^n \det \begin{pmatrix} AB & 0 \\ B & -E \end{pmatrix}.$$

Применив еще раз теорему об определителе ступенчатой матрицы, получим

$$\det A \det B = (-1)^n \det AB \det (-E) = \det AB,$$

что и требовалось доказать.

**5. Примеры применения теоремы об определителе произведения квадратных матриц к вычислению определителей.** Собственно говоря, те приемы вычисления определителей, которые мы рассматривали раньше, можно рассматривать как левые умножения (при комбинировании строк) или правые умножения (при комбинировании столбцов) на вспомогательные матрицы, именно, матрицы трансвекций. Мы должны были внимательно следить за тем, чтобы не прибавить уже измененную строку (или столбец) при линейном комбинировании. Теорема об определителе произведения дает большую свободу для линейного комбинирования строк (или столбцов) за счет умножения на подходящие вспомогательные матрицы. Определитель при этом может меняться, но мы в состоянии учесть это изменение, именно, определитель приобретает множителем определитель вспомогательной матрицы. Остается следить только за тем, чтобы не умножить на матрицу с нулевым определителем.

**Пример 1.** Найти  $\det A$ , если

$$A = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}.$$

Здесь напрашивается несколько способов линейного комбинирования строк. Хорошо сложить все строки. Не менее хорошо сложить первые две и вычесть третью и четвертую, сложить первую с третьей и вычесть вторую и четвертую и, наконец, сложить первую с четвертой и вычесть вторую и третью. Все эти преобра-

зования выполняться одновременно, если исходную матрицу умножить слева на матрицу

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Действительно

$$CA = \begin{pmatrix} a+b+c+d & a+b+c+d & a+b+c+d & a+b+c+d \\ a+b-c-d & a+b-c-d & -a-b+c+d & -a-b+c+d \\ a-b+c-d & -a+b-c+d & a-b+c-d & -a+b-c+d \\ a-b-c+d & -a+b+c-d & -a+b+c-d & a-b-c+d \end{pmatrix}$$

и

$$\begin{aligned} \det CA &= \det C \det A = (a+b+c+d)(a+b-c-d) \times \\ &\times (a-b+c-d)(a-b-c+d) \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} = \\ &= (a+b+c+d)(a+b-c-d)(a-b+c-d)(a-b-c+d) \det C. \end{aligned}$$

Остается убедиться, что  $\det C \neq 0$ . Мы его вычисляли выше, он равен  $-16$ . Но легко также убедиться в справедливости неравенства  $\det C \neq 0$ , учитывая, что

$$C^2 = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad \text{так что} \quad (\det C)^2 = 256.$$

Этот пример несколько искусственный, но он есть частный случай более общей ситуации — группового определителя конечной абелевой группы.

Подчеркнем еще раз важность того, что  $\det C \neq 0$ . Если за этим не проследить, можно получить неверный результат. Например, для той же матрицы  $A$  возьмем в качестве вспомогательной

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Тогда

$$CA = \begin{pmatrix} a+b+c+d & a+b+c+d & a+b+c+d & a+b+c+d \\ a+b+c+d & a+b+c+d & a+b+c+d & a+b+c+d \\ a+b+c+d & a+b+c+d & a+b+c+d & a+b+c+d \\ a+b+c+d & a+b+c+d & a+b+c+d & a+b+c+d \end{pmatrix}$$

и

$$\det CA = \det C \det A = (a+b+c+d)^4 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{vmatrix} = \\ = (a+b+c+d)^4 \det C.$$

«Сократив» на  $\det C$ , получим неверный результат:

$$\det A = (a+b+c+d)^4.$$

Но на самом деле  $\det C = 0$ , и сокращение на  $\det C$  недопустимо.

Пример 2. Найти  $\Delta = \det A$ , где

$$A = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}.$$

Пример очень похож на предыдущий, но здесь линейное комбинирование строк малополезно. Хорошо возвести  $\Delta$  в квадрат:

$$\Delta^2 = \det A^T A = \\ = \begin{vmatrix} a^2 + b^2 + c^2 + d^2 & 0 & 0 & 0 \\ 0 & a^2 + b^2 + c^2 + d^2 & 0 & 0 \\ 0 & 0 & a^2 + b^2 + c^2 + d^2 & 0 \\ 0 & 0 & 0 & a^2 + b^2 + c^2 + d^2 \end{vmatrix} = \\ = (a^2 + b^2 + c^2 + d^2)^4.$$

Следовательно, или  $\Delta = (a^2 + b^2 + c^2 + d^2)^2$ , или  $\Delta = -(a^2 + b^2 + c^2 + d^2)^2$ , или при одних значениях  $a, b, c, d$  одно, при других — другое. Разберемся в этом вопросе. Мы имеем равенство полиномов от  $a, b, c, d$ :  $\Delta^2 = (a^2 + b^2 + c^2 + d^2)^4$ , или

$$(\Delta - (a^2 + b^2 + c^2 + d^2)^2)(\Delta + (a^2 + b^2 + c^2 + d^2)^2) = 0.$$

Но кольцо полиномов есть область целостности. Следовательно, равен нулю один из сомножителей. Равенство нулю второго приводит к

$$\Delta = -(a^2 + b^2 + c^2 + d^2)^2,$$

что не имеет места при следующих значениях букв:  $a = 1, b = c = d = 0$ . Следовательно,

$$\Delta = (a^2 + b^2 + c^2 + d^2)^2.$$

**6. Теорема Бине — Коши.** Пусть произведение двух прямоугольных матриц есть матрица квадратная. Это будет в том и только в том случае, когда не только число столбцов первой ма-

трицы равно числу строк второй, но и число строк первой равно числу столбцов второй:

$$\begin{matrix} m \\ \boxed{A} \\ n \end{matrix} \cdot \begin{matrix} \boxed{B} \\ m \end{matrix} = \begin{matrix} \boxed{AB} \\ m \end{matrix}$$

В этой ситуации имеет место следующая теорема, называемая теоремой Бине — Коши.

**Теорема 3.** *Определитель матрицы  $AB$  равен нулю, если  $m > n$ , и равен сумме произведений всех миноров  $m$ -го порядка матрицы  $A$  на соответствующие миноры  $m$ -го порядка матрицы  $B$ , если  $m \leq n$ .*

Соответствие миноров понимается здесь в следующем смысле: номера столбцов матрицы  $A$ , составляющие минор, совпадают с номерами строк матрицы  $B$ , из которых составляется соответствующий минор.

В формульной записи:

$$\det AB = \sum_{\gamma_1 < \gamma_2 < \dots < \gamma_m} A_{\gamma_1, \gamma_2, \dots, \gamma_m} B_{\gamma_1, \gamma_2, \dots, \gamma_m},$$

где  $A_{\gamma_1, \gamma_2, \dots, \gamma_m}$  — минор матрицы  $A$ , составленный из столбцов с номерами  $\gamma_1, \gamma_2, \dots, \gamma_m$ , и  $B_{\gamma_1, \gamma_2, \dots, \gamma_m}$  — минор матрицы  $B$ , составленный из строк с номерами  $\gamma_1, \gamma_2, \dots, \gamma_m$ .

Теорему Бине — Коши можно доказать аналогично доказательству теоремы об определителе произведения двух квадратных матриц (которая, конечно, есть частный случай теоремы Бине — Коши). Однако при этом пришлось бы воспользоваться теоремой Лапласа в общей формулировке.

Приведем доказательство, основанное на другой идее. Запишем подробно

$$\det AB =$$

$$= \begin{vmatrix} a_{11}b_{11} + a_{12}b_{21} + \dots + a_{1n}b_{n1} & \dots & a_{11}b_{1m} + a_{12}b_{2m} + \dots + a_{1n}b_{nm} \\ \dots & \dots & \dots \\ a_{m1}b_{11} + a_{m2}b_{21} + \dots + a_{mn}b_{n1} & \dots & a_{m1}b_{1m} + a_{m2}b_{2m} + \dots + a_{mn}b_{nm} \end{vmatrix}.$$

Теперь применим свойство линейности определителя к первому столбцу. Получим

$$\begin{aligned} \det AB &= \begin{vmatrix} a_{11}b_{11} & \dots \\ \dots & \dots \\ a_{m1}b_{11} & \dots \end{vmatrix} + \begin{vmatrix} a_{12}b_{21} & \dots \\ \dots & \dots \\ a_{m2}b_{21} & \dots \end{vmatrix} + \begin{vmatrix} a_{1n}b_{n1} & \dots \\ \dots & \dots \\ a_{mn}b_{n1} & \dots \end{vmatrix} = \\ &= \sum_{\alpha_1=1}^n \begin{vmatrix} a_{1\alpha_1}b_{\alpha_1 1} & \dots \\ \dots & \dots \\ a_{m\alpha_1}b_{\alpha_1 1} & \dots \end{vmatrix}. \end{aligned}$$

где у всех определителей столбцы, начиная со второго, такие же, как у  $\det AB$  в исходной форме. Применим теперь свойство линейности ко вторым столбцам определителей, составляющих эту сумму. Получим

$$\det AB = \sum_{\alpha_1, \alpha_2} \begin{vmatrix} a_{1\alpha_1} b_{\alpha_1 1} & a_{1\alpha_2} b_{\alpha_2 2} & \cdots \\ \vdots & \vdots & \ddots \\ a_{m\alpha_1} b_{\alpha_1 1} & a_{m\alpha_2} b_{\alpha_2 2} & \cdots \end{vmatrix},$$

где индексы  $\alpha_1$  и  $\alpha_2$  пробегают независимо значения 1, 2, ...,  $n$ . Здесь у всех определителей столбцы, начиная с третьего, такие же, как в исходной форме у  $\det AB$ .

Тем же способом продолжаем разложение определителя  $\det AB$  на сумму определителей, применяя свойство линейности к третьим, ...,  $m$ -м столбцам. Получим в результате

$$\det AB = \sum_{\alpha_1, \alpha_2, \dots, \alpha_m} \begin{vmatrix} a_{1\alpha_1} b_{\alpha_1 1} & a_{1\alpha_2} b_{\alpha_2 2} & \cdots & a_{1\alpha_m} b_{\alpha_m m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\alpha_1} b_{\alpha_1 1} & a_{m\alpha_2} b_{\alpha_2 2} & \cdots & a_{m\alpha_m} b_{\alpha_m m} \end{vmatrix},$$

где индексы  $\alpha_1, \alpha_2, \dots, \alpha_m$  принимают независимо друг от друга все значения от 1 до  $n$ . Здесь всего  $n^m$  слагаемых. Вынесем из каждого столбца общий множитель. Получим

$$\det AB = \sum b_{\alpha_1 1} b_{\alpha_2 2} \cdots b_{\alpha_m m} \begin{vmatrix} a_{1\alpha_1} & a_{1\alpha_2} & \cdots & a_{1\alpha_m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\alpha_1} & a_{m\alpha_2} & \cdots & a_{m\alpha_m} \end{vmatrix}.$$

Если  $m > n$ , то индексам  $\alpha_1, \alpha_2, \dots, \alpha_m$  будет «настолько тесно», что среди их значений будет находиться хотя бы одна пара равных. Но тогда все определители, входящие в слагаемые  $\det AB$ , будут равны нулю как имеющие равные столбцы. Поэтому  $\det AB = 0$  при  $m > n$ .

Пусть теперь  $m \leq n$ . Если среди значений индексов найдется хотя бы одна пара равных, то соответствующее слагаемое равно нулю. Все такие слагаемые можно отбросить и останется сумма, распространенная на попарно различные значения индексов  $\alpha_1, \alpha_2, \dots, \alpha_m$ . Наборы таких значений могут отличаться как составом значений, так и порядком, если состав один и тот же. Такие наборы носят название *размещений*. Обозначим через  $\gamma_1, \gamma_2, \dots, \gamma_m$  набор значений индексов  $\alpha_1, \alpha_2, \dots, \alpha_m$ , расположенных в порядке возрастания:  $\gamma_1 < \gamma_2 < \dots < \gamma_m$ , так что при одном и том же составе значения индексов  $\alpha_1, \alpha_2, \dots, \alpha_m$  будут образовывать перестановки элементов  $\gamma_1, \gamma_2, \dots, \gamma_m$ .

Проведем сначала суммирование по всевозможным наборам  $\alpha_1, \alpha_2, \dots, \alpha_m$  одинакового состава, т. е. по перестановкам элементов  $\gamma_1, \gamma_2, \dots, \gamma_m$ , а затем сложим получившиеся суммы по возможным составам.

Получим

$$\det AB =$$

$$= \sum_{1 \leq \gamma_1 < \dots < \gamma_m \leq n} \sum_{(\alpha_1, \alpha_2, \dots, \alpha_m)} b_{\alpha_1 1} b_{\alpha_2 2} \dots b_{\alpha_m m} \begin{vmatrix} a_{1\alpha_1} & a_{1\alpha_2} & \dots & a_{1\alpha_m} \\ \dots & \dots & \dots & \dots \\ a_{m\alpha_1} & a_{m\alpha_2} & \dots & a_{m\alpha_m} \end{vmatrix},$$

где во внутренней сумме суммирование ведется по всем наборам  $(\alpha_1, \alpha_2, \dots, \alpha_m)$ , составляющим перестановки чисел  $\gamma_1, \gamma_2, \dots, \gamma_m$ .

В пределах внутренней суммы определители отличаются только порядком столбцов. Приведя столбцы в порядок возрастания значений индексов, получим:

$$\begin{vmatrix} a_{1\alpha_1} & a_{1\alpha_2} & \dots & a_{1\alpha_m} \\ \dots & \dots & \dots & \dots \\ a_{m\alpha_1} & a_{m\alpha_2} & \dots & a_{m\alpha_m} \end{vmatrix} = (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_m)} \begin{vmatrix} a_{1\gamma_1} & a_{1\gamma_2} & \dots & a_{1\gamma_m} \\ \dots & \dots & \dots & \dots \\ a_{m\gamma_1} & a_{m\gamma_2} & \dots & a_{m\gamma_m} \end{vmatrix},$$

так что

$$\det AB =$$

$$= \sum_{1 \leq \gamma_1 < \dots < \gamma_m \leq n} \sum_{(\alpha_1, \dots, \alpha_m)} b_{\alpha_1 1} b_{\alpha_2 2} \dots b_{\alpha_m m} (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_m)} \times \\ \times \begin{vmatrix} a_{1\gamma_1} & a_{1\gamma_2} & \dots & a_{1\gamma_m} \\ \dots & \dots & \dots & \dots \\ a_{m\gamma_1} & a_{m\gamma_2} & \dots & a_{m\gamma_m} \end{vmatrix}.$$

Во все слагаемые внутренней суммы входит сомножителем один и тот же определитель. Его можно вынести за знак суммы:

$$\det AB =$$

$$= \sum_{\gamma_1 < \dots < \gamma_m} \begin{vmatrix} a_{1\gamma_1} & \dots & a_{1\gamma_m} \\ \dots & \dots & \dots \\ a_{m\gamma_1} & \dots & a_{m\gamma_m} \end{vmatrix} \sum_{(\alpha_1, \alpha_2, \dots, \alpha_m)} b_{\alpha_1 1} b_{\alpha_2 2} \dots b_{\alpha_m m} (-1)^{\text{inv}(\alpha_1, \dots, \alpha_m)}.$$

После вынесения минора матрицы  $A$  за знак внутренней суммы осталось драгоценное наследство в виде множителя  $(-1)^{\text{inv}(\alpha_1, \dots, \alpha_m)}$ , наличие которого позволяет заключить, что внутренняя сумма равна определителю

$$\begin{vmatrix} b_{\gamma_1 1} & b_{\gamma_1 2} & \dots & b_{\gamma_1 m} \\ \dots & \dots & \dots & \dots \\ b_{\gamma_m 1} & b_{\gamma_m 2} & \dots & b_{\gamma_m m} \end{vmatrix}.$$

Действительно, она есть сумма всевозможных произведений элементов матрицы этого определителя, взятых по одному из каждой строки (ведь  $(\alpha_1, \alpha_2, \dots, \alpha_m)$  пробегает всевозможные перестановки чисел  $\gamma_1, \gamma_2, \dots, \gamma_m$ ) и по одному из каждого столбца.

Сомножители записаны в порядке следования столбцов, а  $\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_m)$  есть число инверсий в номерах строк. Итак,  $\det AB =$

$$= \sum_{1 \leq \nu_1 < \dots < \nu_m \leq n} \begin{vmatrix} a_{1\nu_1} & a_{1\nu_2} & \dots & a_{1\nu_m} \\ \dots & \dots & \dots & \dots \\ a_{m\nu_1} & a_{m\nu_2} & \dots & a_{m\nu_m} \end{vmatrix} \cdot \begin{vmatrix} b_{\nu_1 1} & b_{\nu_1 2} & \dots & b_{\nu_1 m} \\ \dots & \dots & \dots & \dots \\ b_{\nu_m 1} & b_{\nu_m 2} & \dots & b_{\nu_m m} \end{vmatrix},$$

что и требовалось доказать.

Приведем один интересный пример. Пусть

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}, \quad B = \begin{pmatrix} \bar{a}_1 & \bar{b}_1 \\ \bar{a}_2 & \bar{b}_2 \\ \dots & \dots \\ \bar{a}_n & \bar{b}_n \end{pmatrix}.$$

Здесь  $a_i, b_i$  — комплексные числа,  $\bar{a}_i, \bar{b}_i$  — сопряженные с ними. Имеем:

$$AB = \begin{vmatrix} a_1 \bar{a}_1 + a_2 \bar{a}_2 + \dots + a_n \bar{a}_n & a_1 \bar{b}_1 + a_2 \bar{b}_2 + \dots + a_n \bar{b}_n \\ \bar{a}_1 b_1 + \bar{a}_2 b_2 + \dots + \bar{a}_n b_n & \bar{b}_1 b_1 + \bar{b}_2 b_2 + \dots + \bar{b}_n b_n \end{vmatrix}.$$

Вспомним, что произведение комплексного числа на сопряженное равно квадрату его модуля, и заметим, что элементы побочной диагонали  $AB$  комплексно сопряжены. Поэтому

$$\det AB = (|a_1|^2 + \dots + |a_n|^2)(|b_1|^2 + \dots + |b_n|^2) - \\ - |a_1 \bar{b}_1 + a_2 \bar{b}_2 + \dots + a_n \bar{b}_n|^2.$$

По теореме Бине — Коши

$$\det AB = \sum_{i < j} \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} \cdot \begin{vmatrix} \bar{a}_i & \bar{b}_i \\ \bar{a}_j & \bar{b}_j \end{vmatrix} = \sum_{i < j} |a_i b_j - a_j b_i|^2.$$

Сравнивая результаты, получаем тождество

$$(|a_1|^2 + \dots + |a_n|^2)(|b_1|^2 + \dots + |b_n|^2) - |a_1 \bar{b}_1 + \dots + a_n \bar{b}_n|^2 = \\ = \sum_{i < j} |a_i b_j - a_j b_i|^2,$$

откуда следует известное неравенство Коши:

$$|a_1 \bar{b}_1 + \dots + a_n \bar{b}_n|^2 \leq (|a_1|^2 + \dots + |a_n|^2)(|b_1|^2 + \dots + |b_n|^2),$$

причем равенство возможно, только если  $a_i b_j - a_j b_i = 0$  для всех  $i$  и  $j$ , т. е. если строки матрицы  $A$  пропорциональны.

## § 6. Обращение квадратных матриц

**1. Условие существования обратной матрицы.** Для данной квадратной матрицы  $A$  *правой обратной* называется такая матрица  $B$ , что  $AB = E$ . Соответственно, матрица  $C$  называется *левой обрат-*

ной для  $A$ , если  $CA = E$ . Матрица называется *обратной* для  $A$ , если она одновременно левая и правая обратная.

**Теорема 1.** Для того чтобы матрица  $A$  с элементами из поля имела обратную, необходимо и достаточно, чтобы ее определитель был отличен от нуля.

**Доказательство.** Необходимость. Пусть для матрицы  $A$  существует правая обратная  $B$ , так что  $AB = E$ . Применяя теорему об определителе произведения квадратных матриц, получим:  $\det A \det B = \det E = 1$ , откуда следует, что  $\det A \neq 0$ . То же условие, очевидно, необходимо и для существования левой обратной.

**Достаточность.** Требование  $AB = E$  означает, в частности, что произведение  $i$ -й строки матрицы  $A$  на  $j$ -й столбец матрицы  $B$  при  $i \neq j$  равно нулю. Этому свойству, согласно свойствам определителя, удовлетворяет матрица  $\tilde{A}$ , транспонированная к матрице, составленной из алгебраических дополнений элементов определителя  $\det A$  в их естественном расположении.

Матрица  $\tilde{A}$  носит название матрицы, *союзной* с матрицей  $A$ . Легко видеть, что

$$\begin{aligned} A\tilde{A} &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} = \\ &= \begin{pmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \det A \end{pmatrix} = \det A \cdot E. \end{aligned}$$

Действительно, на диагональных позициях оказываются суммы произведений элементов строки на их алгебраические дополнения, а каждая такая сумма есть определитель  $\det A$ , представленный в виде разложения по элементам строки. На недиагональных позициях оказываются суммы произведений элементов строки на алгебраические дополнения элементов другой строки, а все такие суммы равны нулю.

Применяя те же свойства к столбцам определителя  $\det A$ , получим, что

$$\tilde{A}A = \det A \cdot E.$$

Поэтому, если  $\det A \neq 0$ , то матрица  $\frac{1}{\det A} \cdot \tilde{A}$  есть правая и левая обратная для матрицы  $A$ , т. е. обратная для  $A$ . Она обозначается  $A^{-1}$ .

Заметим еще, что кроме  $A^{-1}$  не существует ни правых, ни левых обратных матриц для  $A$ . Действительно, если  $AB = E$ , то  $A^{-1}(AB) = A^{-1}$ , но  $A^{-1}(AB) = (A^{-1}A)B = B$ , так что  $B = A^{-1}$ . Аналогично, если  $CA = E$ , то  $(CA)A^{-1} = A^{-1}$ , откуда  $C = A^{-1}$ .

Квадратная матрица  $A$ , у которой  $\det A \neq 0$ , называется *неособенной* или *невырожденной*. В противном случае матрица называется *вырожденной*.

Для матриц с элементами из коммутативного ассоциативного кольца (не обязательно поля) те же рассуждения дают следующее условие обратимости:

*Для того чтобы матрица  $A$  с элементами из коммутативного ассоциативного кольца  $\Lambda$  была обратима над тем же кольцом, необходимо и достаточно, чтобы определитель матрицы был обратимым в кольце  $\Lambda$  элементом.*

Действительно, необходимость следует из равенства

$$\det A \det A^{-1} = 1,$$

а определитель матрицы с элементами из  $\Lambda$  принадлежит  $\Lambda$ . Для достаточности нужно заметить, что элементы союзной матрицы  $\tilde{A}$  принадлежат кольцу  $\Lambda$  и, если  $\det A$  обратим в  $\Lambda$ , то матрица  $(\det A)^{-1}\tilde{A}$  будет обратной, и ее элементы принадлежат  $\Lambda$ .

Например, для целочисленной обратимости матрицы с целыми элементами необходимо и достаточно, чтобы ее определитель был равен  $\pm 1$ . Для обратимости матрицы над кольцом полиномов необходимо и достаточно, чтобы ее определитель был не равной нулю константой, и т. п.

## 2. Некоторые свойства обратной матрицы.

1.  $\det A^{-1} = (\det A)^{-1}$ .

Действительно,  $AA^{-1} = E$ , следовательно,  $\det A \det A^{-1} = \det E = 1$ , откуда  $(\det A)^{-1} = \det A^{-1}$ .

2. Если  $A$  и  $B$  невырождены, то их произведение  $AB$  тоже невырожденно и  $(AB)^{-1} = B^{-1}A^{-1}$ , т. е. матрица, обратная к произведению, равна произведению обратных, взятых в обратном порядке.

Действительно,

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = E,$$

откуда следует, что  $B^{-1}A^{-1} = (AB)^{-1}$ .

3.  $(A^{-1})^{-1} = A$ .

Действительно,  $(A^{-1})^{-1}$  есть такая единственная матрица, произведение которой на  $A^{-1}$  равно  $E$ . Этим свойством обладает  $A$ .

4.  $(A^T)^{-1} = (A^{-1})^T$ .

Действительно, переходя в равенстве  $AA^{-1} = E$  к транспонированным матрицам, получим  $(A^{-1})^T A^T = E$ , откуда и следует, что  $(A^{-1})^T = (A^T)^{-1}$ .

3. Решение линейных систем с невырожденной матрицей в терминах обратной матрицы. Пусть дана система линейных уравнений

$$Ax = b,$$

где  $A$  — невырожденная квадратная матрица,  $x$  — столбец из неизвестных,  $b$  — столбец свободных членов.

Допустим, что система имеет решение и  $x$  уже есть решение, так что  $Ax = b$  — верное равенство. Умножим обе части его на  $A^{-1}$ . Получим  $A^{-1}Ax = A^{-1}b$ , откуда  $x = A^{-1}b$ . Теперь докажем, что  $A^{-1}b$  действительно есть решение:  $A(A^{-1}b) = (AA^{-1})b = b$ .

Мы находились в условиях теоремы Крамера, и приведенные несколько строк представляют собой доказательство теоремы Крамера. Легко проследить, что то доказательство, которое было приведено, в точности совпадает с данным сейчас, но было осуществлено в развернутой записи. Именно, умножение уравнений системы на алгебраические дополнения и сложение представляло собой не что иное, как умножение слева на союзную матрицу. Вторая часть, проверка, представляла собой подстановку  $A^{-1}b$  вместо  $x$ , но в развернутой записи. Ясно также, что равенство  $x = A^{-1}b = \frac{1}{\det A} \tilde{A}b$  есть матричная запись формул Крамера.

Столь же кратко записывается решение матричного уравнения  $AX = B$ , где  $A$  — невырожденная матрица порядка  $n$ ,  $X$  — неизвестная  $n \times k$ -матрица,  $B$  — данная  $n \times k$ -матрица. Именно,  $X = A^{-1}B$ . Запись  $AX = B$  равносильна  $k$  системам линейных уравнений с одной и той же матрицей коэффициентов  $A$ , с неизвестными, составляющими столбцы матрицы  $X$ , и со свободными членами, составляющими столбцы матрицы  $B$ .

**4. Обращение ступенчатой матрицы.** Пусть  $\begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$  — невырожденная ступенчатая матрица с квадратными блоками  $A$  и  $D$ . Из невырожденности следует, что  $\det A \neq 0$  и  $\det D \neq 0$ . Пусть  $\begin{pmatrix} X & Y \\ U & V \end{pmatrix}$  — обратная матрица, разбитая на блоки в соответствии с разбиением исходной матрицы. Из равенства  $\begin{pmatrix} A & 0 \\ C & D \end{pmatrix} \begin{pmatrix} X & Y \\ U & V \end{pmatrix} = \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}$  следуют уравнения  $AX = E$ ,  $AY = 0$ ,  $CX + DU = 0$ ,  $CY + DV = E$ .

Находим из первого уравнения  $X = A^{-1}$ , из второго  $Y = 0$ , из четвертого  $V = D^{-1}$  и, наконец, из третьего  $U = -D^{-1}CA^{-1}$ . Итак,

$$\begin{pmatrix} A & 0 \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & 0 \\ -D^{-1}CA^{-1} & D^{-1} \end{pmatrix}.$$

$$\text{Аналогично, } \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{pmatrix}.$$

**5. Вычисление определителя матрицы, разбитой на четыре клетки, и обращение такой матрицы.** Пусть дана матрица  $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$  с квадратными клетками  $A$  и  $D$ , причем предполагается, что

матрица  $A$  невырождена. Умножим матрицу слева на матрицу  $\begin{pmatrix} A^{-1} & 0 \\ -CA^{-1} & E \end{pmatrix}$ . Получим

$$\begin{pmatrix} A^{-1} & 0 \\ -CA^{-1} & E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} E & A^{-1}B \\ 0 & -CA^{-1}B + D \end{pmatrix}. \quad (*)$$

Переходя к определителям, получим

$$\det A^{-1} \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (D - CA^{-1}B)$$

и

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det A \det (D - CA^{-1}B).$$

Матрица  $D - CA^{-1}B$  называется *шуровским дополнением* к субматрице  $A$  матрицы  $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ .

Перейдем теперь в равенстве (\*) к обратным матрицам. Получим

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} \begin{pmatrix} A^{-1} & 0 \\ -CA^{-1} & E \end{pmatrix}^{-1} = \begin{pmatrix} E & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix}^{-1}.$$

откуда

$$\begin{aligned} \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} &= \begin{pmatrix} E & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix}^{-1} \begin{pmatrix} A^{-1} & 0 \\ -CA^{-1} & E \end{pmatrix} = \\ &= \begin{pmatrix} E & -A^{-1}B(D - CA^{-1}B)^{-1} \\ 0 & (D - CA^{-1}B)^{-1} \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ -CA^{-1} & E \end{pmatrix} = \\ &= \begin{pmatrix} A^{-1} + A^{-1}B(D - CA^{-1}B)^{-1}CA^{-1} & -A^{-1}B(D - CA^{-1}B)^{-1} \\ -(D - CA^{-1}B)^{-1}CA^{-1} & (D - CA^{-1}B)^{-1} \end{pmatrix}. \end{aligned}$$

Заметим еще, что если  $A, B, C, D$  — квадратные матрицы одинакового порядка, то формулу для определителя можно преобразовать к виду

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (AD - ACA^{-1}B),$$

и если  $A$  и  $C$  коммутируют, то

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (AD - CB).$$

Аналогично, записав  $\det A$  правым множителем, получим

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (DA - CA^{-1}BA)$$

и, если  $A$  и  $B$  коммутируют,

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (DA - CB).$$

**6. Ортогональные и унитарные матрицы.** Вещественная матрица называется *ортогональной*, если ее обратная совпадает с транспонированной. В формульной записи:  $P$  ортогональна, если  $PP^T = E$ .

Запишем это матричное равенство в развернутой форме. Пусть

$$P = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \dots & \dots & \dots & \dots \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix}.$$

Тогда

$$P^T = \begin{pmatrix} p_{11} & p_{21} & \dots & p_{n1} \\ p_{12} & p_{22} & \dots & p_{n2} \\ \dots & \dots & \dots & \dots \\ p_{1n} & p_{2n} & \dots & p_{nn} \end{pmatrix}$$

и

$$PP^T = \begin{pmatrix} p_{11}^2 + p_{12}^2 + \dots + p_{1n}^2 & p_{11}p_{21} + p_{12}p_{22} + \dots + p_{1n}p_{2n} & \dots \\ \dots & \dots & \dots \end{pmatrix}.$$

На главной диагонали матрицы  $PP^T$  находятся суммы квадратов элементов строк матрицы  $P$ . На остальных позициях находятся суммы произведений соответствующих элементов двух различных строк. Поэтому равенство  $PP^T = E$ , характеризующее ортогональные матрицы, записывается как

$$\sum_{j=1}^n p_{ij}^2 = 1, \quad i = 1, \dots, n,$$

$$\sum_{j=1}^n p_{ij}p_{kj} = 0, \quad i, k = 1, \dots, n, \quad i \neq k.$$

Вещественная строка называется *нормированной*, если сумма квадратов ее элементов равна 1, и две вещественные строки называются *ортогональными*, если сумма произведений соответствующих элементов равна нулю. Таким образом, условие  $PP^T = E$  равносильно тому, что строки матрицы  $P$  нормированны и попарно ортогональны.

Из равенства  $PP^T = E$  следует  $P^TP = E$ , или  $P^T(P^T)^T = E$ . Таким образом, из ортогональности матрицы  $P$  следует ортогональность транспонированной с ней матрицы  $P^T$  и обратно. Однако развернутая запись равенства  $P^TP = E$  полностью отлична от записи  $PP^T = E$ , именно, имеет вид нормированности и попарной ортогональности столбцов матрицы  $P$ . Таким образом, мы

получаем нетривиальное обстоятельство — из нормированности и попарной ортогональности строк матрицы следует нормированность и попарная ортогональность ее столбцов.

Отметим некоторые свойства ортогональных матриц.

1. Ортогональность  $P$  влечет ортогональность  $P^{-1}$ .

Действительно,  $P^{-1} = P^T$ , а ортогональность  $P^T$  уже установлена.

2. Произведение ортогональных матриц есть ортогональная матрица.

Действительно,  $P_1 P_2 (P_1 P_2)^T = P_1 P_2 P_2^T P_1^T = P_1 E P_1^T = P_1 P_1^T = E$ .

3. Единичная матрица ортогональна.

Действительно,  $EE^T = EE = E$ .

Эти свойства означают, что ортогональные матрицы образуют группу.

4. Определитель ортогональной матрицы равен  $\pm 1$ .

Действительно,  $\det PP^T = (\det P)^2 = \det E = 1$ , откуда  $\det P = \pm 1$ .

Ортогональные матрицы разбиваются на два класса — собственно ортогональные с определителем 1, и несобственно ортогональные с определителем  $-1$ .

В дальнейшем мы увидим различие в геометрическом смысле собственно и несобственно ортогональных матриц.

Среди матриц с комплексными элементами существенную роль играют так называемые унитарные матрицы. Матрица  $A^*$ , комплексно сопряженная с транспонированной к  $A$ , называется *сопряженной* с  $A$ , т. е.  $A^* = \bar{A}^T$ , где черточка наверху — знак комплексного сопряжения. Матрица  $Q$  называется *унитарной*, если обратная к ней совпадает с сопряженной. Записав равенство  $QQ^* = E$  в развернутой форме, получим

$$\sum_{j=1}^n q_{ij} \bar{q}_{ij} = \sum_{j=1}^n |q_{ij}|^2 = 1, \quad i = 1, \dots, n,$$

$$\sum_{j=1}^n q_{ij} \bar{q}_{kj} = 0, \quad i, k = 1, \dots, n, \quad i \neq k.$$

Строка из комплексных чисел называется *нормированной*, если сумма квадратов модулей ее элементов равна 1. Две комплексные строки называются *ортогональными*, если сумма произведений элементов одной строки на числа, сопряженные с соответствующими элементами второй строки, равна 0.

Таким образом, равенство  $QQ^* = E$  обозначает, что строки матрицы  $Q$  нормированны и попарно ортогональны. Равносильное равенство  $Q^*Q = E$  дает, что столбцы матрицы  $Q$  нормированны и попарно ортогональны.

Отметим свойства унитарных матриц, аналогичные свойствам ортогональных матриц.

1. Унитарность  $Q$  влечет унитарность  $Q^{-1}$ .

Действительно,  $Q^{-1} = Q^*$ , а унитарность  $Q^*$  следует из равенства  $Q^*Q = E$ .

2. Произведение унитарных матриц есть унитарная матрица.

Действительно,  $Q_1Q_2(Q_1Q_2)^* = Q_1Q_2Q_2^*Q_1^* = Q_1Q_1^* = E$ .

3. Единичная матрица унитарна.

Действительно,  $EE^* = EE = E$ .

Эти свойства означают, что унитарные матрицы образуют группу.

4. Модуль определителя унитарной матрицы равен 1.

Действительно,  $\det QQ^* = \det Q \det Q^* = \det Q \det Q = |\det Q|^2 = 1$ .

## § 7. Характеристический полином матрицы

1. Определение характеристического полинома. Сопоставим квадратной матрице с элементами из поля  $K$  матрицу  $tE - A$ , элементы которой принадлежат кольцу полиномов  $K[t]$ . Матрица  $tE - A$  называется *характеристической матрицей* для  $A$ , а ее определитель  $f(t) = \det(tE - A)$  называется *характеристическим полиномом* матрицы  $A$ .

Если

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

то  $f(t) = t^n - b_1 t^{n-1} + b_2 t^{n-2} + \dots + (-1)^n b_n$  с коэффициентами из  $K$ . Вычислим  $b_1$  и  $b_n$ . Заметим, что  $b_1$  есть коэффициент при  $t^{n-1}$  в определителе

$$\begin{vmatrix} t - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & t - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & t - a_{nn} \end{vmatrix}.$$

Буква  $t$  входит, причем в первой степени, только в диагональные элементы матрицы  $tE - A$ . Следовательно, каждое слагаемое определителя, содержащее  $t^{n-1}$ , имеет в числе сомножителей по крайней мере  $n-1$  диагональных элементов, но тогда и последний сомножитель тоже диагональный. Таким образом, коэффициент при  $t^{n-1}$  равен коэффициенту при  $t^{n-1}$  в полиноме  $(t - a_{11}) \times \dots \times (t - a_{nn})$ , т. е. равен  $-(a_{11} + a_{22} + \dots + a_{nn})$ . Таким образом,  $b_1 = a_{11} + a_{22} + \dots + a_{nn}$ . Это выражение имеет специальное название — *след* матрицы  $A$  и обозначается  $\text{Sp } A$  или  $\text{Tr } A$  (от *Spur* — нем., *Trace* — англ.).

Для подсчета свободного члена положим  $t = 0$ . Получим  $(-1)^n b_n = \det(-A) = (-1)^n \det A$ , откуда  $b_n = \det A$ .

Остальные коэффициенты тоже можно подсчитать, но это несколько сложнее.



Квадратичная форма может быть записана более компактно, если использовать матричные обозначения. Вынося  $x_1$  из первой







примет канонический вид:

$$\alpha_{11}z_1^2 + \alpha_2z_2^2 + \dots + \alpha_nz_n^2.$$

Несколько невырожденных линейных преобразований можно заменить одним невырожденным, ибо композиции преобразований соответствует умножение матриц, а произведение невырожденных матриц невырожденно. Теорема доказана.

Заметим, что хотя мы теорему сформулировали для вещественных квадратичных форм и вещественных преобразований — именно этот случай наиболее интересен для приложений — теорема остается верной для квадратичных форм с коэффициентами из любого поля  $K$ , характеристика которого не равна 2, при преобразованиях над тем же полем  $K$ .

Рассуждение посредством метода математической индукции есть, по существу, краткая запись единообразного процесса, состоящего в повторении индуктивного перехода. Поэтому данное доказательство дает и способ преобразования квадратичной формы к каноническому виду. Рассмотрим один пример.

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1^2 + x_1x_2 - x_1x_3 + 2x_1x_4 + \\ &+ x_2x_1 + x_2^2 + 3x_2x_4 - \\ &- x_3x_1 + x_3^2 - 2x_3x_4 + \\ &+ 2x_4x_1 + 3x_4x_2 - 2x_4x_3 + 4x_4^2 = \\ &= x_1^2 + 2x_1x_2 - 2x_1x_3 + 4x_1x_4 + x_2^2 + 6x_2x_4 + x_3^2 - 4x_3x_4 + 4x_4^2 = \\ &= (x_1 + x_2 - x_3 + 2x_4)^2 - (x_2 - x_3 + 2x_4)^2 + x_2^2 + 6x_2x_4 + x_3^2 - 4x_3x_4 + 4x_4^2 = \\ &= (x_1 + x_2 - x_3 + 2x_4)^2 + 2x_2x_3 + 2x_2x_4. \end{aligned}$$

Положим

$$\begin{aligned} x_1 + x_2 - x_3 + 2x_4 &= y_1, \\ x_2 &= y_2, \\ x_3 &= y_3, \\ x_4 &= y_4, \end{aligned}$$

т. е. сделаем подстановку

$$\begin{aligned} x_1 &= y_1 - y_2 + y_3 - 2y_4, \\ x_2 &= y_2, \\ x_3 &= y_3, \\ x_4 &= y_4. \end{aligned}$$

Придем к форме  $y_1^2 + \Phi(y_2, y_3, y_4)$ , где  $\Phi(y_2, y_3, y_4) = 2y_2y_3 + 2y_2y_4$ .  
Здесь нужно вспомогательное преобразование:

$$\begin{aligned}y_1 &= z_1, \\y_2 &= z_2, \\y_3 &= z_2 + z_3, \\y_4 &= z_4,\end{aligned}$$

после которого

$$\begin{aligned}\Phi(y_2, y_3, y_4) &= 2z_2^2 + 2z_2z_3 + 2z_2z_4 = \\&= 2\left(z_2 + \frac{z_3}{2} + \frac{z_4}{2}\right)^2 - 2\left(\frac{z_3}{2} + \frac{z_4}{2}\right)^2 = 2\left(z_2 + \frac{z_3}{2} + \frac{z_4}{2}\right)^2 - \\&\quad - \frac{1}{2}z_3^2 - z_3z_4 - \frac{1}{2}z_4^2.\end{aligned}$$

Теперь делается замена

$$\begin{aligned}z_1 &= u_1, \\z_2 &= u_2 - \frac{u_3}{2} - \frac{u_4}{2}, \\z_3 &= u_3, \\z_4 &= u_4,\end{aligned}$$

после которой придем к равенству

$$\Phi(y_2, y_3, y_4) = 2u_2^2 + \Phi_1(u_3, u_4),$$

где

$$\Phi_1(u_3, u_4) = -\frac{1}{2}u_3^2 - u_3u_4 - \frac{1}{2}u_4^2 = -\frac{1}{2}(u_3 + u_4)^2.$$

Очередная замена:

$$\begin{aligned}u_1 &= v_1, \\u_2 &= v_2, \\u_3 &= v_3 - v_4, \\u_4 &= v_4,\end{aligned}$$

которая дает  $\Phi_1(u_3, u_4) = -\frac{1}{2}v_3^2$ . Итак!

$$\begin{aligned}f = y_1^2 + \Phi(y_2, y_3, y_4) &= z_1^2 + 2z_2^2 + 2z_2z_3 + 2z_2z_4 = \\&= u_1^2 + 2u_2^2 + \Phi_1(u_3, u_4) = v_1^2 + 2v_2^2 - \frac{1}{2}v_3^2.\end{aligned}$$

Резльтирующая подстановка:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 1 & -2 \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & -\frac{1}{2} & -\frac{1}{2} \\ & & 1 & \\ & & & 1 \end{pmatrix} \times \\ \times \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & -1 \\ & & & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = \begin{bmatrix} 1 & 0 & 1 & -3 \\ 0 & 1 & -\frac{1}{2} & 0 \\ 0 & 1 & \frac{1}{2} & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix}.$$

В этом примере перед вторым шагом мы «споткнулись» о вспомогательное преобразование.

**4. Ранг квадратичной формы.** В терминах матриц теорема о приведении квадратичной формы к каноническому виду означает, что для данной симметричной матрицы  $A$  существует такая невырожденная матрица  $B$ , что  $B^T A B = D$ , где  $D$  — диагональная матрица. Обозначив  $C = B^{-1}$ , получим  $A = C^T D C$ .

Из доказательства теоремы ясно, что приведение квадратичной формы к каноническому виду может осуществляться бесконечным множеством способов — например, можно сделать произвольную линейную подстановку, а затем приступить к «выделению квадратов». Поэтому матрицы  $B$  и  $D$  определяются неоднозначно. Однако число ненулевых элементов матрицы  $D$  однозначно определено, именно, оно равно рангу матрицы  $A$ . Этот ранг называется *рангом* квадратичной формы.

Для доказательства установим сначала справедливость следующих предложений.

**Предложение 2.** *Ранг произведения двух матриц (не обязательно квадратных) не превосходит ранга каждого из сомножителей.*

**Доказательство.** Столбцы матрицы  $AB$  являются линейными комбинациями столбцов матрицы  $A$ . Поэтому ранг  $AB$ , равный максимальному числу линейно независимых столбцов, не превосходит ранга  $A$ . С другой стороны, строки  $AB$  являются линейными комбинациями строк  $B$ , поэтому ранг  $AB$  не превосходит ранга  $B$ .

**Предложение 3.** *Если один из сомножителей есть квадратная невырожденная матрица, то ранг произведения равен рангу другого сомножителя.*

Действительно, пусть  $C = AB$  и  $B$  — невырожденная квадратная матрица. Тогда ранг  $C$  не превосходит ранга  $A$ . Но  $A = CB^{-1}$ , так что ранг  $A$  не превосходит ранга  $C$ . Следовательно, эти

ранги равны. Аналогичное рассуждение применимо к случаю, если левый сомножитель есть квадратная невырожденная матрица.

Из предложения 3 непосредственно следует: если  $F = BAC$ , где  $B$  и  $C$  — невырожденные квадратные матрицы, то ранги матриц  $F$  и  $A$  совпадают.

Применяя это к матричному равенству

$$D = C^T A C,$$

где  $C$  — невырожденная квадратная матрица, получим, что ранги  $D$  и  $A$  совпадают. Но ранг диагональной матрицы  $D$ , очевидно, равен числу ее ненулевых элементов. Итак, число ненулевых коэффициентов после приведения квадратичной формы к каноническому виду не зависит от способа приведения и равен рангу матрицы квадратичной формы.

**5. Преобразование квадратичной формы к каноническому виду посредством унитарного преобразования переменных.** Вернемся еще раз к доказательству теоремы о приведении квадратичной формы к каноническому виду. Если на каждом шагу индуктивного рассуждения «выделение квадрата» происходит без вспомогательного преобразования, то на каждом шагу матрица преобразования имеет вид правой унитарной матрицы. Так как произведение правых унитарных матриц есть, очевидно, правая унитарная матрица, результирующая матрица преобразования будет тоже правой унитарной.

**Теорема 4.** Для того чтобы квадратичная форма с невырожденной матрицей могла быть преобразована к каноническому виду преобразованием переменных с верхней унитарной матрицей, необходимо и достаточно, чтобы определители всех левых угловых субматриц ее матрицы были отличны от нуля.

Доказательству этой теоремы предпослшем другую теорему, представляющую самостоятельный интерес.

**Теорема 5.** Для того чтобы квадратная невырожденная матрица представлялась в виде произведения левой унитарной, диагональной и правой унитарной, необходимо и достаточно, чтобы определители всех левых угловых субматриц были отличны от нуля. Такое представление однозначно.

**Доказательство.** Необходимость. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2k} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kk} & \dots & a_{kn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nk} & \dots & a_{nn} \end{pmatrix}, \quad A_k = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix}.$$

так что  $A = A_n$ . Пусть, далее,

$$L = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ b_{21} & 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nk} & \dots & 1 \end{pmatrix}, \quad L_k = \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_{21} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ b_{k1} & b_{k2} & \dots & 1 \end{pmatrix},$$

$$R = \begin{pmatrix} 1 & c_{12} & \dots & c_{1k} & \dots & c_{1n} \\ 0 & 1 & \dots & c_{2k} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & c_{kn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix}, \quad R_k = \begin{pmatrix} 1 & c_{12} & \dots & c_{1k} \\ 0 & 1 & \dots & c_{2k} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

$D = \text{diag}(d_1, d_2, \dots, d_k, \dots, d_n)$ ,  $D_k = \text{diag}(d_1, d_2, \dots, d_k)$  и  $A = LDR$ . Тогда  $\det A = \det L \det D \det R = d_1 d_2 \dots d_n$  и, так как  $\det A \neq 0$ , должно быть  $d_i \neq 0$ ,  $i = 1, 2, \dots, n$ .

Легко видеть, что

$$A_k = L_k D_k R_k,$$

откуда следует, что  $\det A_k = \det D_k = d_1 d_2 \dots d_k \neq 0$ .

Достаточность. Применим метод математической индукции по субматрицам  $A_1, A_2, \dots, A_k, \dots, A_n = A$ . При  $k=1$  утверждение теоремы тривиально. Пусть оно верно для  $A_{k-1}$ , и в этом предположении докажем его для  $A_k$ .

Разобьем матрицу  $A_k$  и искомые  $L_k, R_k, D_k$  на клетки, выделив блок  $A_{k-1}$ , так что

$$A_k = \begin{pmatrix} A_{k-1} & u \\ v & a_{kk} \end{pmatrix}, \quad L_k = \begin{pmatrix} L_{k-1} & 0 \\ x & 1 \end{pmatrix}, \quad R_k = \begin{pmatrix} R_{k-1} & y \\ 0 & 1 \end{pmatrix},$$

$$D_k = \begin{pmatrix} D_{k-1} & 0 \\ 0 & d_k \end{pmatrix}.$$

Здесь  $u = (a_{1k}, \dots, a_{k-1,k})^T$ ,  $v = (a_{k1}, \dots, a_{kk-1})$ ,  $x$  — неизвестная строка в матрице  $L_k$ ,  $y$  — неизвестный столбец в матрице  $R_k$ , символом 0 обозначены нулевые строки и столбцы.

Пусть  $A_k = L_k D_k R_k$ . Выполняя умножение по правилу умножения блочных матриц, получим

$$L_{k-1} D_{k-1} R_{k-1} = A_{k-1},$$

$$L_{k-1} D_{k-1} y = u,$$

$$x D_{k-1} R_{k-1} = v,$$

$$x D_{k-1} y + d_k = a_{kk}.$$

В силу индуктивного предположения  $L_{k-1}$ ,  $D_{k-1}$  и  $R_{k-1}$  можно считать известными, обратимыми и определенными однозначно. Тогда

однозначно определяются  $y$ ,  $x$  и  $d_k$ , именно,  $y = D_{k-1}^{-1} L_{k-1}^{-1} u$ ,  $x = = v R_{k-1}^{-1} D_{k-1}^{-1}$  и  $d_k = a_{kk} - x D_{k-1} y$ . Остается убедиться в том, что  $d_k \neq 0$ , что нужно для обратимости  $D_k$ . Но

$$\det A_k = \det D_k = \det D_{k-1} \cdot d_k,$$

откуда  $d_k = \frac{\det A_k}{\det D_{k-1}} \neq 0$ .

Теорема 5 доказана полностью.

Теперь легко доказать теорему 4. Пусть  $A$  — невырожденная матрица квадратичной формы, допускающей унитарное преобразование к канонической форме. Тогда  $A = R^T D R$ , где  $R$  — правая унитарная матрица,  $R^T$  — левая унитарная. В силу теоремы 5, в части необходимости все определители верхних угловых субматриц отличны от нуля.

Обратно, если все такие определители отличны от нуля, то  $A = L D R$  (в прежних обозначениях). Но  $A$  симметрична, так что  $A = A^T = R^T D L^T$ . В силу однозначности разложения должно быть  $L^T = R$ , т. е.  $A = R^T D R$ , что обозначает, что квадратичная форма приводится к каноническому виду посредством линейного преобразования переменных с правой унитарной матрицей  $R$ .

## § 2. Закон инерции квадратичных форм

В этом и следующем параграфах речь будет идти только о квадратичных формах с вещественными коэффициентами и о линейных подстановках переменных с вещественными коэффициентами.

**1. Положительно определенные квадратичные формы.** Квадратичная форма называется *положительно определенной*, если все ее значения при вещественных значениях переменных, не равных одновременно нулю, положительны. Примером положительно определенной формы от переменных  $x_1, x_2, \dots, x_n$  может служить форма  $x_1^2 + x_2^2 + \dots + x_n^2$ .

Квадратичная форма называется *отрицательно определенной*, если все ее значения отрицательны, за исключением нулевого значения при нулевых значениях переменных.

Квадратичная форма называется *положительно (отрицательно) полуопределенной*, если она не принимает отрицательных (положительных) значений.

Так форма  $x_1^2 - 2x_1x_2 + x_2^2 = (x_1 - x_2)^2$  положительно полуопределена. Форма  $x_1^2 + x_2^2$  как форма от двух переменных  $x_1$  и  $x_2$  положительно определена, но как форма от трех переменных  $x_1, x_2, x_3$  лишь полуопределена.

Квадратичные формы, принимающие, как положительные, так и отрицательные значения, называются *неопределенными*.





Если квадратичная форма задана численно, то для приведения ее к каноническому виду требуется приблизительно столько же арифметических операций, как при вычислении одного определителя. Так что в этом случае первый критерий проще. Для теоретических же исследований лучше критерий Сильвестра, так как он дается простыми формулами.

### 3. Закон инерции квадратичных форм.

**Теорема 3.** Если квадратичная форма преобразована двумя способами к каноническому виду, то число квадратов новых переменных с положительными коэффициентами будет одинаково, так же как число квадратов новых переменных с отрицательными коэффициентами. Иными словами, число положительных и отрицательных коэффициентов не зависит от способа приведения формы к каноническому виду.

**Доказательство.** Пусть дана форма, приведенная к каноническому виду двумя способами:

$$\begin{aligned} f(x_1, x_2, \dots, x_n) &= \alpha_1 y_1^2 + \dots + \alpha_p y_p^2 - \alpha_{p+1} y_{p+1}^2 - \dots - \alpha_{p+q} y_{p+q}^2 = \\ &= \beta_1 z_1^2 + \dots + \beta_s z_s^2 - \beta_{s+1} z_{s+1}^2 - \dots - \beta_{s+t} z_{s+t}^2. \end{aligned}$$

Считаем, что все  $\alpha_i$  и  $\beta_j$  положительны. Пусть исходные переменные связаны с новыми посредством следующих невырожденных преобразований:

$$\begin{aligned} x_1 &= b_{11}y_1 + \dots + b_{1n}y_n, & y_1 &= f_{11}x_1 + \dots + f_{1n}x_n, \\ &\dots \dots \dots & &\dots \dots \dots \\ x_n &= b_{n1}y_1 + \dots + b_{nn}y_n; & y_n &= f_{n1}x_1 + \dots + f_{nn}x_n; \\ \\ x_1 &= c_{11}z_1 + \dots + c_{1n}z_n, & z_1 &= g_{11}x_1 + \dots + g_{1n}x_n, \\ &\dots \dots \dots & &\dots \dots \dots \\ x_n &= c_{n1}z_1 + \dots + c_{nn}z_n; & z_n &= g_{n1}x_1 + \dots + g_{nn}x_n. \end{aligned}$$

Допустим, что число положительных коэффициентов не одинаково. Будем считать, для определенности, что  $p < s$ . Положим  $y_1 = 0, \dots, y_p = 0, z_{s+1} = 0, \dots, z_n = 0$ . Все  $y_i$  и  $z_j$  являются линейными формами от  $x_1, \dots, x_n$ . Таким образом, написанная совокупность равенств есть система линейных однородных уравнений относительно  $x_1, x_2, \dots, x_n$ . Число неизвестных равно  $n$ , число уравнений равно  $p + n - s < n$ . Поэтому система имеет нетривиальные решения. Пусть  $x_1^*, \dots, x_n^*$  — одно из них. Соответствующие значения для  $y_1, \dots, y_n$  обозначим через  $y_1^*, \dots, y_n^*$ . Заметим, что  $y_1^* = \dots = y_p^* = 0$ . Соответствующие значения для  $z_1, \dots, z_n$  обозначим через  $z_1^*, \dots, z_n^*$ . Эти значения не равны одновременно нулю (иначе равнялись бы нулю  $x_1^*, \dots, x_n^*$ ), но  $z_{s+1}^* = 0, \dots, z_n^* = 0$ . Поэтому среди чисел  $z_1^*, \dots, z_s^*$  имеются отличные от нуля.

Из представления  $f(x_1, x_2, \dots, x_n) = \alpha_1 y_1^2 + \dots + \alpha_p y_p^2 - \alpha_{p+1} y_{p+1}^2 - \dots - \alpha_{p+q} y_{p+q}^2$  имеем:

$$f(x_1^*, \dots, x_n^*) = -\alpha_{p+1} y_{p+1}^{*2} - \dots - \alpha_{p+q} y_{p+q}^{*2} \leq 0.$$

Из другого представления:

$$f(x_1^*, \dots, x_n^*) = \beta_1 z_1^{*2} + \dots + \beta_s z_s^{*2} > 0.$$

Последнее неравенство строгое, ибо среди  $z_1^*, \dots, z_s^*$  имеются отличные от нуля. Мы пришли к противоречию, так что предположение о различии числа положительных коэффициентов неверно.

Для установления равенства числа отрицательных коэффициентов достаточно перейти к форме  $-f(x_1, \dots, x_n)$  и ее каноническим представлениям

$$\begin{aligned} -f(x_1, \dots, x_n) &= -\alpha_1 y_1^2 - \dots - \alpha_p y_p^2 + \alpha_{p+1} y_{p+1}^2 + \dots + \alpha_{p+q} y_{p+q}^2 \\ &= -\beta_1 z_1^2 - \dots - \beta_s z_s^2 + \beta_{s+1} z_{s+1}^2 + \dots + \beta_{s+t} z_{s+t}^2. \end{aligned}$$

и применить уже доказанное утверждение о равенстве положительных коэффициентов. Теорема доказана полностью.

Заметим еще, что если

$$\Delta_1 = a_{11} \neq 0, \Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0, \dots, \Delta_n = \det A \neq 0,$$

то можно дать формулу для числа отрицательных коэффициентов в канонической форме. Именно, оно равно числу перемен знаков в ряду чисел

$$1 = \Delta_0, \Delta_1, \Delta_2, \dots, \Delta_n.$$

Действительно, коэффициенты в канонической форме, получающейся при преобразовании с правой унитарной матрицей, равны

$$\frac{\Delta_1}{\Delta_0}, \frac{\Delta_2}{\Delta_1}, \frac{\Delta_3}{\Delta_2}, \dots, \frac{\Delta_n}{\Delta_{n-1}},$$

так что число отрицательных среди них равно указанному выше числу перемен знаков.

### § 3. Ортогональное преобразование квадратичной формы к каноническому виду

**1. Собственные значения и собственные векторы матрицы.** Пусть  $A$  — квадратная матрица с элементами, являющимися комплексными (в частности, вещественными) числами. Ненулевой столбец  $X$  называется *собственным вектором* матрицы  $A$ , если имеет место равенство  $AX = \lambda X$  при некотором комплексном (возможно, вещественном)  $\lambda$ , называемом *собственным значением* матрицы  $A$ .



## 2. Собственные значения вещественной симметричной матрицы.

**Теорема 2.** *Все собственные значения вещественной симметричной матрицы вещественны.*

**Доказательство.** Пусть  $A$  — вещественная симметричная матрица и  $X$  — некоторый ее собственный вектор с комплексными компонентами, так что  $AX = \lambda X$  при некотором  $\lambda$ . Подсчитаем двумя способами число  $a = \bar{X}^T A X$  (черточка наверху обозначает, как обычно, комплексное сопряжение). Это действительно число, ибо оно есть произведение строки  $\bar{X}^T$  на столбец  $AX$ . Имеем:  $\bar{a} = \overline{X^T A X}$ . Но  $(\bar{a})^T = \bar{a}$ , так как число  $\bar{a}$ , рассматриваемое как матрица первого порядка, при транспонировании не изменяется. Поэтому  $\bar{a} = (X^T A \bar{X})^T = \bar{X}^T A^T X^T = \bar{X}^T A X = a$ . Итак,  $\bar{a} = a$ , т. е.  $a$  — число вещественное. С другой стороны,  $a = \bar{X}^T A X = \bar{X}^T \lambda X = \lambda (\bar{x}_1 x_1 + \dots + \bar{x}_n x_n) = \lambda (|x_1|^2 + \dots + |x_n|^2)$ . Ввиду того, что  $X \neq 0$ ,  $|x_1|^2 + \dots + |x_n|^2 > 0$  и  $\lambda = \frac{a}{|x_1|^2 + \dots + |x_n|^2}$  есть число вещественное.

Теорема доказана.

Хочется отметить нетривиальность содержания доказанной теоремы. Мы еще не располагаем критериями вещественности корней полинома с вещественными коэффициентами при  $n > 2$ . В дальнейшем мы увидим, что такие критерии не просты. Тем не менее мы получили сейчас широкий класс полиномов, все корни которых вещественны — это характеристические полиномы вещественных симметричных матриц. Даже при  $n = 2$  применение общеизвестного критерия неотрицательности дискриминанта требует некоторых преобразований. Действительно, пусть  $n = 2$ ,  $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ ;

тогда  $\det(tE - A) = t^2 - (a + c)t + ac - b^2$ , и дискриминант  $D$  равен  $(a + c)^2 - 4(ac - b^2) = (a - c)^2 + 4b^2 \geq 0$ .

Из вещественности собственных значений вещественной симметричной матрицы следует, что компоненты собственных векторов можно брать вещественными. Действительно, они определяются из линейной однородной системы уравнений с вещественными коэффициентами. Ясно, что если  $X$  есть собственный вектор матрицы  $A$ , то  $cX$  при любом  $c \neq 0$  будет собственным вектором, принадлежащим тому же собственному значению. Действительно, если  $AX = \lambda X$ , то  $A(cX) = \lambda cX$ . Поэтому собственные векторы для вещественной симметричной матрицы всегда можно выбирать нормированными. Действительно, если  $X$  — какой-либо собственный вектор и  $x_1^2 + x_2^2 + \dots + x_n^2 = r^2$ , то столбец  $\frac{1}{r} X$  останется собственным вектором и будет нормирован.

**3. Построение ортогональных матриц.** Напомним, что матрица называется ортогональной, если ее столбцы нормированы и попарно ортогональны.

**Лемма.** Пусть  $X_1, X_2, \dots, X_k$  — вещественные нормированные попарно ортогональные столбцы длины  $n$ , и пусть  $k < n$ . Тогда существует нормированный столбец  $X_{k+1}$ , ортогональный столбцам  $X_1, X_2, \dots, X_k$ .

**Доказательство.** Пусть

$$X_1 = (x_{11}, x_{21}, \dots, x_{n1})^T,$$

$$X_2 = (x_{12}, x_{22}, \dots, x_{n2})^T,$$

$$\dots \dots \dots$$

$$X_k = (x_{1k}, x_{2k}, \dots, x_{nk})^T$$

и

$$X_{k+1} = (z_1, z_2, \dots, z_n)^T.$$

Запишем требования ортогональности и нормированности в виде уравнений. Придем к системе:

$$x_{11}z_1 + x_{21}z_2 + \dots + x_{n1}z_n = 0,$$

$$x_{12}z_1 + x_{22}z_2 + \dots + x_{n2}z_n = 0,$$

$$\dots \dots \dots$$

$$x_{1k}z_1 + x_{2k}z_2 + \dots + x_{nk}z_n = 0.$$

$$z_1^2 + z_2^2 + \dots + z_n^2 = 1.$$

Первые  $k$  уравнений образуют линейную однородную систему, причем число уравнений  $k$  меньше числа неизвестных  $n$ . Поэтому система имеет нетривиальные решения. Пусть  $z_1^*, z_2^*, \dots, z_n^*$  — одно из них и  $r^2 = z_1^{*2} + z_2^{*2} + \dots + z_n^{*2}$ . Тогда числа  $\frac{1}{r} z_1^*, \frac{1}{r} z_2^*, \dots, \frac{1}{r} z_n^*$  будут удовлетворять всем уравнениям системы, т. е. дадут решение задачи.

Заметим, что условие  $k < n$  здесь существенно. При  $k = n$  столбцы составляют ортогональную матрицу, она невырожденна, и система для определения  $X_{k+1}$  окажется несовместной, так что более чем  $n$  попарно ортогональных нормированных столбцов не может существовать.

Отметим следующие следствия:

Любую матрицу, состоящую из попарно ортогональных нормированных столбцов, можно дополнить до ортогональной матрицы. Действительно, столбцов в такой матрице не может быть больше  $n$ . Если их  $n$ , то матрица ортогональна. Если же их меньше  $n$ , то можно присоединять новые столбцы до тех пор, пока не придем к ортогональной матрице.

В частности, любой нормированный столбец может быть принят за первый столбец ортогональной матрицы.

**Пример.** Вложить столбец  $(1/3, 2/3, -2/3)^T$  в ортогональную матрицу.

Этот столбец нормирован и к нему нужно пристроить еще два нормированных столбца, ортогональных между собой и

ортогональных данному. Присоединяем их по одному:

$$\begin{aligned}\frac{1}{3}z_1 + \frac{2}{3}z_2 - \frac{2}{3}z_3 &= 0, \\ z_1^2 + z_2^2 + z_3^2 &= 1.\end{aligned}$$

Можно взять  $z_1 = 0$ ,  $z_2 = z_3 = 1/\sqrt{2}$ . Далее,

$$\begin{aligned}\frac{1}{3}z_1 + \frac{2}{3}z_2 - \frac{2}{3}z_3 &= 0, \\ \frac{1}{\sqrt{2}}z_2 + \frac{1}{\sqrt{2}}z_3 &= 0, \\ z_1^2 + z_2^2 + z_3^2 &= 1.\end{aligned}$$

Из первых двух уравнений находим  $z_2 = -z_3$ ,  $z_1 = 4z_3$ . Из условия нормированности  $16z_3^2 + z_3^2 + z_3^2 = 1$ , откуда  $z_3 = \pm \frac{1}{3\sqrt{2}}$ .

Итак, одна из искоемых матриц есть

$$\begin{pmatrix} \frac{1}{3} & 0 & \frac{4}{3\sqrt{2}} \\ \frac{2}{3} & \frac{1}{\sqrt{2}} & -\frac{1}{3\sqrt{2}} \\ -\frac{2}{3} & \frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} \end{pmatrix}.$$

При выборе второго столбца имелся довольно широкий произвол, третий определен с точностью до множителя  $\pm 1$ .

**4. Ортогональное преобразование квадратичной формы к каноническому виду.**

**Теорема 3.** *Вещественная квадратичная форма может быть приведена к каноническому виду посредством преобразования переменных с ортогональной матрицей.*

**Доказательство.** Применим метод математической индукции по числу  $n$  переменных. При  $n=1$  нечего доказывать, так что база индукции тривиальна. Допустим, что теорема уже доказана для форм от  $n-1$  переменных.

Пусть  $f(x_1, x_2, \dots, x_n) = X^T A X$ , где  $X = (x_1, x_2, \dots, x_n)^T$ ,  $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$  — вещественная симметричная матрица. Пусть  $X_1 = (p_{11}, p_{21}, \dots, p_{n1})$  — нормированный собственный вектор матрицы  $A$ , соответствующий собственному значению  $\lambda_1$ . Примем  $X_1$  за первый столбец ортогональной матрицы:

$$P = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \dots & \dots & \dots & \dots \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix}.$$

Покажем, что преобразование с этой матрицей «улучшает» матрицу квадратичной формы. Матрица преобразованной формы есть  $P^TAP$ . Имеем

$$AP = \begin{pmatrix} a_{11}p_{11} + a_{12}p_{21} + \dots + a_{1n}p_{n1} & \dots \\ a_{21}p_{11} + a_{22}p_{21} + \dots + a_{2n}p_{n1} & \dots \\ \dots & \dots \\ a_{n1}p_{11} + a_{n2}p_{21} + \dots + a_{nn}p_{n1} & \dots \end{pmatrix} = \begin{pmatrix} \lambda_1 p_{11} & \dots \\ \lambda_1 p_{21} & \dots \\ \dots & \dots \\ \lambda_1 p_{n1} & \dots \end{pmatrix},$$

ибо в первом столбце находится столбец  $AX_1 = \lambda_1 X_1$ . Далее,

$$\begin{aligned} P^TAP &= \begin{pmatrix} p_{11} & p_{21} & \dots & p_{n1} \\ p_{12} & p_{22} & \dots & p_{n2} \\ \dots & \dots & \dots & \dots \\ p_{1n} & p_{2n} & \dots & p_{nn} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 p_{11} & \dots \\ \lambda_1 p_{21} & \dots \\ \dots & \dots \\ \lambda_1 p_{n1} & \dots \end{pmatrix} = \\ &= \begin{pmatrix} \lambda_1 (p_{11}^2 + p_{21}^2 + \dots + p_{n1}^2) & \dots \\ \lambda_1 (p_{12}p_{11} + p_{22}p_{21} + \dots + p_{n2}p_{n1}) & \dots \\ \dots & \dots \\ \lambda_1 (p_{1n}p_{11} + p_{2n}p_{21} + \dots + p_{nn}p_{n1}) & \dots \end{pmatrix} = \begin{pmatrix} \lambda_1 & \dots \\ 0 & \dots \\ \dots & \dots \\ 0 & \dots \end{pmatrix}, \end{aligned}$$

ибо столбцы матрицы  $P$  ортогональны и нормированны. Матрица

$P^TAP$  симметрична, поэтому имеет вид  $\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & b_{n2} & \dots & b_{nn} \end{pmatrix}$ , где  $B =$

$= \begin{pmatrix} b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots \\ b_{n2} & \dots & b_{nn} \end{pmatrix}$  — симметричная матрица. Рассмотрим квадра-

тичную форму с матрицей  $B$ . В силу индуктивного предположения найдется ортогональная матрица  $Q$  такая, что  $Q^TBQ = \text{diag}(\lambda_2, \dots, \lambda_n)$ . Положим  $Q_1 = \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}$ . Ясно, что матрица  $Q_1$  ортогональна, ибо ее первый столбец нормирован и ортогонален остальным столбцам, а остальные столбцы попарно ортогональны и нормированны в силу ортогональности матрицы  $Q$ . Ясно, что  $Q_1^T \begin{pmatrix} \lambda_1 & 0 \\ 0 & B \end{pmatrix} Q_1 = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$  и  $Q_1^T P^TAPQ_1 = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ .

Теорема доказана, ибо  $PQ_1$  есть ортогональная матрица как произведение двух ортогональных.

5. Коэффициенты канонического вида квадратичной формы и столбцы преобразующей ортогональной матрицы. Пусть  $A$  — данная квадратная матрица и  $C$  — невырожденная матрица. Матрица  $C^{-1}AC$  называется *подобной* матрице  $A$  и переход от  $A$  к  $C^{-1}AC$  называется *преобразованием подобия* посредством  $C$ . Отношение подобия симметрично, ибо  $A = C(C^{-1}AC)C^{-1}$ , и транзитивно, т. е.

если две матрицы подобны третьей, то они подобны. Действительно, пусть  $B_1 = C_1^{-1}AC_1$  и  $B_2 = C_2^{-1}AC_2$ . Тогда

$$B_2 = C_2^{-1}C_1B_1C_1^{-1}C_2 = (C_1^{-1}C_2)^{-1}B_1(C_1^{-1}C_2).$$

Покажем, что подобные матрицы имеют одинаковые характеристические многочлены. Действительно,

$$\begin{aligned} \det(tE - C^{-1}AC) &= \det(C^{-1}tEC - C^{-1}AC) = \\ &= \det C^{-1}(tE - A)C = \det C^{-1} \det(tE - A) \det C = \\ &= \det(tE - A) \det(C^{-1}C) = \det(tE - A). \end{aligned}$$

Вернемся к ортогональному преобразованию квадратичных форм. Равенство  $P^TAP = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$  можно переписать в виде  $P^{-1}AP = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ , ибо матрица  $P$  ортогональна, так что матрица  $A$  подобна диагональной матрице  $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ . Поэтому их характеристические многочлены равны. Ясно, что характеристический многочлен диагональной матрицы  $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$  равен  $(t - \lambda_1)(t - \lambda_2) \dots (t - \lambda_n)$ . Итак,  $(t - \lambda_1)(t - \lambda_2) \dots (t - \lambda_n) = \det(tE - A)$ . Тем самым мы доказали, что каково бы ни было ортогональное преобразование квадратичной формы к каноническому виду, коэффициенты этого канонического вида равны собственным значениям матрицы квадратичной формы, причем каждое собственное значение повторяется столько раз, какова его кратность как корня характеристического полинома.

Равенство  $P^TAP = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$  можно записать в виде  $AP = P \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ . Обозначив через  $P_1, P_2, \dots, P_n$  столбцы матрицы  $P$ , получим

$$A(P_1, P_2, \dots, P_n) = (P_1, P_2, \dots, P_n) \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n),$$

откуда

$$(AP_1, AP_2, \dots, AP_n) = (\lambda_1 P_1, \lambda_2 P_2, \dots, \lambda_n P_n)$$

и  $AP_i = \lambda_i P_i$ ,  $i = 1, 2, \dots, n$ .

Итак, столбцы преобразующей ортогональной матрицы являются собственными векторами матрицы квадратичной формы. Доказанные обстоятельства существенно помогают фактическому вычислению коэффициентов при квадратах и элементов преобразующей матрицы. Именно, нужно найти собственные значения и соответствующие им собственные векторы. Но может получиться одна неприятность: столбцы преобразующей матрицы должны быть ортогональны, а собственные векторы априори ортогональными не обязаны быть. Оказывается, что эта неприятность возникает, только если имеются кратные собственные значения. Именно, верна следующая теорема.

**Теорема 4.** *Собственные векторы вещественной симметричной матрицы, соответствующие различным собственным значениям, ортогональны.*

**Доказательство.** Условие ортогональности  $x_1y_1 + x_2y_2 + \dots + x_ny_n = 0$  двух столбцов  $X = (x_1, x_2, \dots, x_n)^T$  и  $Y = (y_1, y_2, \dots, y_n)^T$  можно записать в матричном виде двумя равносильными формулами:  $X^T Y = 0$  или  $Y^T X = 0$ .

Пусть  $A$  — вещественная симметричная матрица,  $X_1$  и  $X_2$  — ее собственные векторы, соответствующие собственным значениям  $\lambda_1$  и  $\lambda_2$ , причем  $\lambda_1 \neq \lambda_2$ . Вычислим двумя способами число  $a = X_2^T A X_1$ . С одной стороны,  $A X_1 = \lambda_1 X_1$ , поэтому  $a = \lambda_1 X_2^T X_1$ . С другой стороны, из  $A X_2 = \lambda_2 X_2$  следует  $X_2^T A = \lambda_2 X_2^T$ , откуда  $a = \lambda_2 X_2^T X_1$ . Вычитая, получим  $(\lambda_1 - \lambda_2) X_2^T X_1 = 0$ , откуда  $X_2^T X_1 = 0$ , ибо  $\lambda_2 \neq \lambda_1$ . Итак, столбцы  $X_1$  и  $X_2$  ортогональны, что и требовалось доказать.

**6. Одновременные преобразования двух квадратичных форм к каноническому виду.** Даны две квадратичные формы  $f(x_1, x_2, \dots, x_n) = X^T A X$  и  $h(x_1, x_2, \dots, x_n) = X^T B X$ . Существует ли невырожденное линейное преобразование переменных  $X = C Y$ , приводящее обе формы к каноническому виду?

Оказывается, такое преобразование возможно не всегда. Однако имеется один частный случай, когда такое приведение возможно, важный тем, что он часто встречается на практике. Именно, верна следующая теорема.

**Теорема 5.** *Две квадратичные формы, из которых одна положительно определенная, можно одновременно привести к каноническому виду посредством невырожденного вещественного линейного преобразования переменных.*

**Доказательство.** Пусть  $f = X^T A X$ ,  $h = X^T B X$  и форма  $h$  положительно определенная. Сделаем преобразование  $X = C Y$ , приводящее форму  $h$  к каноническому виду:  $C^T B C = \text{diag}(d_1, d_2, \dots, d_n)$ . Так как форма  $h$  положительно определенная, все коэффициенты  $d_i$  положительны. Сделаем теперь преобразование  $Y = D Z$ , где  $D = \text{diag}(d_1^{-1/2}, d_2^{-1/2}, \dots, d_n^{-1/2})$ . Это преобразование приведет форму  $h$  к чистой сумме квадратов  $z_1^2 + z_2^2 + \dots + z_n^2$ , так что  $D^T C^T B C D = E$ . Форма  $f$  превратится в форму с матрицей  $D^T C^T A C D$ . Преобразуем эту форму к каноническому виду ортогональным преобразованием  $Z = P \cdot U$ . Это преобразование не изменит матрицы формы  $z_1^2 + z_2^2 + \dots + z_n^2$ , ибо  $P^T E P = P^T P = E$  в силу ортогональности матрицы  $P$ . Итак, результирующее преобразование  $X = C D P U$  приводит обе формы к каноническому виду, причем положительно определенная приведет к виду чистой суммы квадратов  $u_1^2 + u_2^2 + \dots + u_n^2$ . Теорема доказана.

Остановимся еще на некоторых подробностях. Пусть  $M = C D P$  — матрица результирующего преобразования. Тогда  $M^T A M = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ , где  $\lambda_1, \lambda_2, \dots, \lambda_n$  — некоторые вещественные числа и  $M^T B M = E = \text{diag}(1, 1, \dots, 1)$ . Тогда

$$M^T (tB - A) M = \text{diag}(t - \lambda_1, t - \lambda_2, \dots, t - \lambda_n)$$

и

$$\det M^T(tB - A)M = (t - \lambda_1)(t - \lambda_2) \dots (t - \lambda_n).$$

Пусть  $\det B = b_0$ . Тогда  $(\det M)^2 = b_0^{-1}$ , так что  $\det(tB - A) = b_0(t - \lambda_1)(t - \lambda_2) \dots (t - \lambda_n)$ . Тем самым коэффициенты  $\lambda_1, \lambda_2, \dots, \lambda_n$  оказываются равными корням полинома  $\det(tB - A)$ , который иногда называют характеристическим полиномом матрицы  $A$  относительно матрицы  $B$ . Ясно, что этот полином лишь множителем  $b_0$  отличается от полинома  $\det(tE - B^{-1}A)$ , т. е. от характеристического полинома матрицы  $B^{-1}A$ . Из равенств

$$M^TAM = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) \quad \text{и} \quad M^TBM = \text{diag}(1, 1, \dots, 1)$$

следует

$$(M^TBM)^{-1}M^TAM = M^{-1}B^{-1}AM = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n),$$

так что матрица  $B^{-1}A$  подобна диагональной матрице  $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$  и все ее собственные значения вещественны. То же относится и к матрице  $AB^{-1} = B(B^{-1}A)B^{-1}$ , которая подобна матрице  $B^{-1}A$ .

Матрица положительно определенной квадратичной формы называется *положительно определенной матрицей*. Покажем, что матрица, обратная к положительно определенной, сама положительно определенная. Действительно, если  $B$  положительно определенная, то существует невырожденная матрица  $C$  такая, что  $B = C^TDC$ , где  $D$  — диагональная матрица из положительных чисел. Тогда  $B^{-1} = C^{-1}D^{-1}(C^T)^{-1} = C_1^TD^{-1}C_1$ , где  $C_1 = (C^T)^{-1}$ . Это значит, что квадратичная форма с матрицей  $B^{-1}$  приводится к канонической форме с матрицей  $D^{-1}$ , составленной из положительных чисел.

Сказанное выше о матрицах  $B^{-1}A$  и  $AB^{-1}$  мы теперь можем сформулировать так:

Матрица, являющаяся произведением двух вещественных симметричных матриц, из которых одна положительно определенная, подобна вещественной диагональной матрице, и все ее собственные значения вещественны. Заметим, что произведение двух симметричных матриц, вообще говоря, не симметрично.

## § 4. Эрмитовы формы

**1. Определение эрмитовой формы.** Близким аналогом теории вещественных квадратичных форм при переходе к полю комплексных чисел является теория так называемых эрмитовых форм. Эрмитовой формой называется многочлен от комплексных переменных  $x_1, x_2, \dots, x_n$  и сопряженных  $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$  вида 
$$\sum_{i,j=1}^n a_{ij} \bar{x}_i x_j,$$
 причем предполагается, что  $a_{ji} = \bar{a}_{ij}$ . В частности, все диагональные коэффициенты вещественны. Напомним, что матрицей  $C^*$ ,

сопряженной с комплексной матрицей  $C$ , называется транспонированная матрица, в которой все элементы заменены комплексно сопряженными, так что  $C^* = \bar{C}^T$ . Эрмитову форму можно записать в матричных обозначениях в виде  $X^*AX$ , где  $X = (x_1, x_2, \dots, x_n)^T$ , причем матрица  $A$  ее коэффициентов обладает свойством  $A^* = A$  *самосопряженности* или *эрмитовости*. При линейном преобразовании переменных  $X = BY$  предполагается, естественно, что сопряженные преобразуются с сопряженными коэффициентами, т. е.  $X^* = \bar{Y}^*B^*$ . Эрмитова форма преобразуется по формуле

$$X^*AX \rightarrow Y^*B^*ABY.$$

Ясно, что матрица  $B^*AB$  останется эрмитовой, ибо

$$(B^*AB)^* = B^*A^*B^{**} = B^*AB.$$

Отметим, что значения эрмитовой формы при всех комплексных значениях переменных вещественны. Действительно, пусть  $X$  — некоторый столбец из комплексных чисел и  $f = X^*AX$ . Тогда  $\bar{f} = \bar{f}^* = X^*A^*X^{**} = X^*AX = f$ , так что  $f$  вещественно.

Определители эрмитовых матриц тоже вещественны. Действительно,  $\det \bar{A} = \det A = \det A^* = \det A$ .

Заметим еще, что эрмитова форма с диагональной матрицей имеет вид  $d_1\bar{x}_1x_1 + d_2\bar{x}_2x_2 + \dots + d_n\bar{x}_nx_n = d_1|x_1|^2 + d_2|x_2|^2 + \dots + d_n|x_n|^2$  с вещественными  $d_1, d_2, \dots, d_n$ . В частности, эрмитова форма с единичной матрицей есть  $|x_1|^2 + |x_2|^2 + \dots + |x_n|^2$ .

**2. Свойства эрмитовых форм.** Эрмитовы формы обладают свойствами, аналогичными свойствам вещественных квадратичных форм. Доказательства соответствующих теорем тоже почти дословно повторяют аналогичные доказательства для вещественных квадратичных форм. Поэтому мы позволим себе сформулировать эти теоремы, опустив их доказательства.

**Теорема 1.** Эрмитова форма может быть приведена к каноническому виду (с диагональной матрицей) посредством преобразования переменных с невырожденной комплексной матрицей.

**Теорема 2.** Ранг матрицы эрмитовой формы равен числу ненулевых коэффициентов в канонической форме.

Эрмитова форма (и ее матрица) называется *положительно определенной*, если все ее значения положительны, кроме значения при нулевых значениях переменных.

**Теорема 3.** Для того чтобы эрмитова форма была положительно определенной, необходимо и достаточно, чтобы коэффициенты ее канонической формы были положительны.

**Теорема 4.** Для того чтобы эрмитова форма с невырожденной матрицей приводилась к каноническому виду преобразованием с правой унитарной матрицей, необходимо и достаточно, чтобы левые верхние диагональные миноры  $\Delta_1, \Delta_2, \dots, \Delta_n$  были от-

личны от нуля. При этом коэффициенты в канонической форме равны  $\Delta_1, \Delta_2/\Delta_1, \dots, \Delta_n/\Delta_{n-1}$ .

Теорема 5. Для того чтобы эрмитова форма была положительно определенной, необходимо и достаточно, чтобы верхние диагональные миноры  $\Delta_1, \Delta_2, \dots, \Delta_n$  ее матрицы были все положительны.

Теорема 6. Число положительных и число отрицательных коэффициентов в канонической форме не зависит от способа приведения к каноническому виду (закон инерции).

Теорема 7. Все собственные значения эрмитовой матрицы вещественны.

Теорема 8. Эрмитова форма может быть приведена к каноническому виду посредством преобразования переменных с унитарной матрицей. При этом коэффициенты канонической формы равны собственным значениям матрицы формы, а столбцы преобразующей матрицы равны соответствующим собственным векторам.

Теорема 9. Две эрмитовы формы, из которых одна положительно определенная, можно одновременно привести к каноническому виду.

Теорема 10. Собственные значения матрицы, являющейся произведением двух эрмитовых матриц, одна из которых положительно определенная, все вещественны, и матрица подобна диагональной матрице, составленной из собственных значений.

## ГЛАВА VI

---

# ПОЛИНОМЫ И ДРОБИ

### § 1. Теория делимости для полиномов от одной буквы

**1. Делимость в кольце.** Пусть  $A$  — коммутативная ассоциативная область целостности (т. е. кольцо без делителей нуля) с единицей. Говорят, что элемент  $a \in A$  *делится* на элемент  $b \in A$ , если существует такой элемент  $c \in A$ , что  $a = bc$ . Говорят также, что  $a$  — *кратное* для  $b$ ,  $b$  — *делитель*  $a$ ,  $b$  *делит*  $a$ . Из этого определения ясно, что если  $a_1$  и  $a_2$  делятся на  $b$ , то  $a_1 \pm a_2$  делится на  $b$ . Далее, если  $a$  делится на  $b$  и  $b$  делится на  $c$ , то  $a$  делится на  $c$ . Элемент  $e$  кольца называется *обратимым* или *единицей*, если для него существует обратный  $e^{-1} \in A$ , т. е. такой, что  $ee^{-1} = 1$ . Элементы, отличающиеся обратимым множителем, называются *ассоциированными*. Ясно, что любой элемент делится на ассоциированные элементы и на единицы. Единицы и ассоциированные элементы считаются неинтересными, тривиальными делителями. Необратимые элементы, не имеющие делителей кроме тривиальных, называются *неразложимыми*. Теория делимости для данного кольца (или класса колец) заключается в выяснении характера разложения любого элемента кольца в произведение неразложимых. Если такое разложение существует и однозначно, с точностью до порядка следования множителей и факторы множителей на ассоциированные, то кольцо называется *факториальным*.

Мы уже имели пример теории делимости для кольца целых чисел. В этом кольце имеются только две единицы  $\pm 1$ , неразложимыми элементами являются простые числа и имеет место теорема об однозначности разложения на простые множители, т. е. кольцо целых чисел факториально. Другим уже известным примером факториального кольца может служить кольцо полиномов  $K[x]$  над алгебраически замкнутым полем  $K$ . В этом кольце неразложимыми элементами являются только полиномы первой степени, которые ассоциированы с линейными двучленами вида  $x - c$ . Имеет место однозначное разложение на линейные множители

$$f(x) = a_0(x - c_1)(x - c_2) \dots (x - c_n).$$

В кольце полиномов  $K[x]$  с коэффициентами из произвольного поля  $K$  единицами являются все элементы поля  $K$ , кроме нуля. Других единиц нет, ибо если  $f_1 f_2 = 1$ ,  $f_1, f_2 \in K[x]$ , то степени  $f_1$  и  $f_2$  не могут быть больше нуля, т. е.  $f_1$  и  $f_2$  — константы из  $K$ . Ассоциированными являются полиномы, отличающиеся множите-

лями из  $K$ . Полиномы со старшим коэффициентом 1 называются *нормализованными*. Ясно, что любой полином из  $K[x]$  ассоциирован с нормализованным, и два нормализованных полинома ассоциированы, только если они совпадают.

## 2. Деление с остатком.

Теорема 1 (о делении с остатком). Для данных полиномов  $f, g \in K[x]$ ,  $g \neq 0$ , существуют и единственны полиномы  $q$  и  $r \in K[x]$  такие, что  $f = gq + r$  и степень  $r$  меньше степени  $g$ .

Теорема эта очень похожа на соответствующую теорему теории делимости целых чисел. Полином  $q$  называется *неполным частным*,  $r$  — *остатком* от деления  $f$  на  $g$ .

**Доказательство.** Пусть  $f = a_0x^n + a_1x^{n-1} + \dots + a_n$ ,  $g = b_0x^m + b_1x^{m-1} + \dots + b_m$ , причем  $b_0 \neq 0$ . Применим метод математической индукции по степени полинома  $f$ , считая  $g$  фиксированным. Пусть  $n < m$ . Тогда  $f = g \cdot 0 + f$ , так что в качестве  $q$  можно взять 0, в качестве  $r$  — сам  $f$ ; оба требования будут выполнены. Этот случай дает базу для индукции. Допустим теперь, что для полиномов степени, меньшей  $n$ , теорема доказана и докажем ее для полинома  $f$ , считая  $n \geq m$ . Воспроизведем первый шаг известного процесса деления многочленов, т. е. построим одночлен  $\frac{a_0}{b_0}x^{n-m}$  и составим разность  $f_1 = f - \frac{a_0}{b_0}x^{n-m}g$ . Полином  $f_1$  имеет меньшую чем  $n$  степень, ибо при вычитании высшие члены исчезнут. В силу индуктивного предположения найдутся полиномы  $q_1$  и  $r$  такие, что  $f_1 = gq_1 + r$  и  $\deg r < \deg g$ . Тогда

$$f = \frac{a_0}{b_0}x^{n-m}g + f_1 = \frac{a_0}{b_0}x^{n-m}g + gq_1 + r = \left(\frac{a_0}{b_0}x^{n-m} + q_1\right)g + r.$$

Оба требования выполнены, если взять  $q = \frac{a_0}{b_0}x^{n-m} + q_1$ . Остается доказать единственность. Пусть  $f = gq + r$  и  $f = gq_1 + r_1$ , причем степени полиномов  $r$  и  $r_1$  меньше степени полинома  $g$ . Тогда  $g(q - q_1) = r_1 - r$ , но степень полинома  $r_1 - r$  меньше степени  $g$ . Это возможно, только если  $r_1 - r = 0$  и  $q - q_1 = 0$ , т. е.  $q = q_1$ ,  $r = r_1$ .

## 3. Наибольший общий делитель двух полиномов.

*Наибольшим общим делителем* двух полиномов  $f_1, f_2$  из кольца  $K[x]$  называется полином наибольшей степени среди полиномов с коэффициентами из поля  $K$  или любого его расширения  $\mathbb{K}$ , делящих оба полинома  $f_1$  и  $f_2$ .

Заметим, что мы не предполагаем заранее, что наибольший общий делитель имеет коэффициенты из поля  $K$ , и «допускаем к конкурсу» полиномы с коэффициентами из любого, большего чем  $K$ , поля  $\mathbb{K}$ . Так, для полиномов  $x^2 - 1$  и  $x^3 - 1$  (с коэффициентами из поля  $\mathbb{Q}$  рациональных чисел) наибольшим общим делителем будет как полином  $x - 1$ , так и полином  $e^{\sqrt{2}}(x - 1)$  или полином  $(1 + i)(x - 1)$ .

**Теорема 2.** *Наибольший общий делитель двух полиномов  $f_1, f_2 \in K[x]$  единствен с точностью до ассоциированности и делится на любой общий делитель этих полиномов. Коэффициенты нормализованного наибольшего общего делителя полиномов из  $K[x]$  принадлежат полю  $K$ . Нормализованный наибольший общий делитель  $d(x)$  допускает линейное представление в виде  $d(x) = f_1(x)M_1(x) + f_2(x)M_2(x)$ , где  $M_1$  и  $M_2$  — некоторые полиномы из  $K[x]$ .*

**Доказательство.** Рассмотрим множество полиномов

$$W = \{f_1N_1 + f_2N_2 \mid N_1, N_2 \in K[x]\}.$$

Здесь предполагается, что  $N_1$  и  $N_2$  независимо пробегает все полиномы из  $K[x]$ . В этом бесконечном множестве полиномов выберем отличный от нуля полином  $d(x)$  наименьшей степени. Покажем, что он является наибольшим общим делителем полиномов  $f_1$  и  $f_2$ .

Для этого прежде всего установим, что остаток от деления двух полиномов из множества  $W$  принадлежит этому множеству. Действительно, пусть  $h_1$  и  $h_2$  принадлежат  $W$ , так что  $h_1 = f_1N_1 + f_2N_2$  и  $h_2 = f_1N_3 + f_2N_4$ . Тогда остаток  $r$  от деления  $h_1$  на  $h_2$ , равный  $h_1 - qh_2$ , где  $q$  — неполное частное, равен  $f_1N_1 + f_2N_2 - q(f_1N_3 + f_2N_4) = f_1(N_1 - qN_3) + f_2(N_2 - qN_4) \in W$ , ибо  $N_1 - qN_3 \in K[x]$  и  $N_2 - qN_4 \in K[x]$ .

Теперь легко доказать, что  $d$  есть наибольший общий делитель  $f_1$  и  $f_2$ . Так как  $f_1 \in W$  и  $d \in W$ , остаток от деления  $f_1$  на  $d$  тоже принадлежит  $W$ , но степень этого остатка меньше степени  $d$ . Поэтому остаток равен нулю, ибо  $d$  — полином наименьшей степени среди отличных от нуля полиномов из  $W$ . Таким образом,  $f_1$  делится на  $d$ . Аналогично,  $f_2$  делится на  $d$ , так что  $d$  есть общий делитель  $f_1$  и  $f_2$ . Далее,  $d \in W$  и, следовательно,

$$d = f_1M_1 + f_2M_2$$

при некоторых  $M_1$  и  $M_2$ . Пусть  $\delta$  — какой-то общий делитель  $f_1$  и  $f_2$  с коэффициентами из  $K$  или какого-то большого поля. Тогда, по свойствам делимости,  $f_1M_1 + f_2M_2 = d$  делится на  $\delta$ . Поэтому степень  $d$  не меньше степени  $\delta$ , так что  $d$  есть действительно наибольший общий делитель. Наконец, если  $d_1$  — какой-либо другой наибольший общий делитель, то его степень равна степени  $d$  и, так как  $d$  делится на  $d_1$ , их частное есть константа, т. е.  $d$  и  $d_1$  ассоциированы. Нормализованный наибольший общий делитель  $d_0$  получится из  $d_1$  посредством деления его на старший коэффициент  $a_0$ . Коэффициенты  $d_0 = \frac{1}{a_0}d$  принадлежат  $K$ , и  $d_0 = f_1\left(\frac{1}{a_0}M_1\right) + f_2\left(\frac{1}{a_0}M_2\right)$  имеет линейное представление. Тем самым мы доказали все свойства наибольшего общего делителя, сформулированные в теореме.

Кроме двух свойств, аналогичных тем, которые мы видели в теории делимости для кольца  $\mathbb{Z}$  целых чисел, следует отметить также, что коэффициенты нормализованного наибольшего общего делителя принадлежат тому же полю, что и коэффициенты данных полиномов. Это существенно и не совсем очевидно. Например, полиномы  $f_1 = x^4 - 1$  и  $f_2 = x^3 + 2x^2 + x + 2$  с рациональными коэффициентами оба имеют корнем число  $i$ , так что нормализованный полином  $x - i$  есть общий делитель  $f_1$  и  $f_2$ , но это не наибольший общий делитель, ибо его коэффициенты не принадлежат полю рациональных чисел. Как легко видеть, здесь наибольший общий делитель есть  $x^2 + 1 = (x + i)(x - i)$ .

Находить наибольший общий делитель двух полиномов можно тем же способом, что и для двух целых чисел, — алгоритмом Евклида. Именно, выполним цепочку делений с остатком:

$$\begin{aligned} f_1 &= f_2 q_1 + r_1, & \deg r_1 < \deg f_2, \\ f_2 &= r_1 q_2 + r_2, & \deg r_2 < \deg r_1, \\ r_1 &= r_2 q_3 + r_3, & \deg r_3 < \deg r_2 \\ &\dots\dots\dots & \dots\dots\dots \\ r_{k-2} &= r_{k-1} q_k + r_k, & \deg r_k < \deg r_{k-1}, \\ r_{k-1} &= r_k q_{k+1}. \end{aligned}$$

Процесс оборвется, на каком-то шагу деление выполнится без остатка, ибо степень каждого последующего остатка меньше степени предыдущего.

Все остатки, которые мы строим, принадлежат множеству  $W = \{f_1 N_1 + f_2 N_2 \mid N_1, N_2 \in K[x]\}$ , и мы «спускаемся» в смысле степени в этом множестве. Последний отличный от нуля остаток  $r_k$  и будет искомым наибольшим общим делителем для  $f_1$  и  $f_2$ . Действительно, пересмотр равенств снизу вверх показывает, что  $r_k$  является делителем  $r_{k-1}, r_{k-2}, \dots, r_1, f_2, f_1$ , а пересмотр сверху вниз — что все остатки  $r_1, r_2, \dots, r_k$  делятся на любой общий делитель  $f_1$  и  $f_2$ . Очевидно, что из алгоритма Евклида следуют все свойства наибольшего общего делителя, сформулированные в теореме.

**4. Свойства взаимно простых полиномов.** Два полинома называются *взаимно простыми*, если их нормализованный наибольший общий делитель равен 1, т. е. эти полиномы не имеют общих делителей, кроме констант.

Предложение 3. Для того чтобы полиномы  $f_1$  и  $f_2$  были взаимно простыми, необходимо и достаточно, чтобы существовали полиномы  $M_1$  и  $M_2$  такие, что  $f_1 M_1 + f_2 M_2 = 1$ .

Действительно, если  $f_1 M_1 + f_2 M_2 = 1$ , то всякий общий делитель для  $M_1$  и  $M_2$  делит единицу и является константой. Если  $f_1$  и  $f_2$  взаимно простые, то их нормализованный наибольший общий делитель 1 имеет линейное представление  $1 = f_1 M_1 + f_2 M_2$ .

**Предложение 4.** Если произведение  $f_1 f_2$  делится на  $f_3$  и  $f_1$  взаимно просто с  $f_3$ , то  $f_2$  делится на  $f_3$ .

Действительно, поскольку  $f_1, f_3$  взаимно простые, найдутся  $M_1$  и  $M_2$  такие, что  $f_1 M_1 + f_3 M_2 = 1$ . Умножив на  $f_2$ , получим:  $f_2 = f_1 f_2 M_1 + f_3 f_2 M_2$ . Первое слагаемое правой части делится на  $f_3$ , ибо  $f_1 f_2$  делится на  $f_3$ , второе делится на  $f_3$  тривиальным образом, следовательно, их сумма  $f_2$  делится на  $f_3$ .

**Предложение 5.** Если  $f_1$  и  $f_2$  оба взаимно просты с  $g$ , то и их произведение  $f_1 f_2$  взаимно просто с  $g$ .

Действительно, существуют  $M_1, M_2, M_3, M_4$  такие, что  $f_1 M_1 + g M_2 = 1$  и  $f_2 M_3 + g M_4 = 1$ . Перемножив эти равенства, получим  $f_1 f_2 M_1 M_3 + g(M_2 f_2 M_3 + f_1 M_1 M_4 + g M_2 M_4) = 1$ , так что  $f_1 f_2$  и  $g$  удовлетворяют признаку взаимной простоты.

**Предложение 6.** Если каждый из полиномов  $f_1, f_2, \dots, f_k$  взаимно прост с  $g$ , то и их произведение  $f_1 f_2 \dots f_k$  взаимно просто с  $g$ .

Это предложение доказывается очевидным проведением индукции на основании предложения 5.

**Предложение 7.** Если каждый из полиномов  $f_1, \dots, f_m$  взаимно прост с каждым из полиномов  $g_1, g_2, \dots, g_n$ , то произведение  $f_1 \dots f_m$  взаимно просто с произведением  $g_1 \dots g_n$ .

Это доказывается многократным применением предложения 6.

**Предложение 8.** Если  $f$  и  $g$  взаимно просты, то  $f^m$  и  $g^n$  взаимно просты.

Это непосредственно следует из предложения 7, достаточно положить  $f_1 = \dots = f_m = f$  и  $g_1 = \dots = g_n = g$ .

Отметим еще одно свойство взаимно простых полиномов, не имеющее аналога в теории делимости целых чисел.

**Предложение 9.** Если полиномы  $f$  и  $g$  взаимно просты, то они не имеют общих корней ни в каком расширении основного поля.

Действительно, пусть  $f, g$  принадлежат кольцу  $K[x]$  и взаимно просты. Пусть  $\mathfrak{K}$  — любое поле, содержащее поле  $K$ , и пусть  $x_0 \in \mathfrak{K}$ . Из взаимной простоты следует, что существуют полиномы  $M_1$  и  $M_2 \in K[x]$  такие, что  $f M_1 + g M_2 = 1$ . Перейдя к значениям при  $x_0$ , получим  $f(x_0) M_1(x_0) + g(x_0) M_2(x_0) = 1$ , откуда следует, что  $f(x_0)$  и  $g(x_0)$  не могут одновременно равняться нулю.

**5. Неприводимые полиномы.** Отличный от константы полином  $\varphi \in K[x]$  называется *неприводимым в поле  $K$* , если он не имеет нетривиальных делителей в  $K[x]$ . В противном случае полином называется *приводимым в поле  $K$* .

Очевидно, что неприводимые полиномы в теории делимости полиномов должны играть такую же роль, как простые числа в теории делимости целых чисел, т. е. роль неразложимых в кольце  $K[x]$  элементов.

Отметим, что понятие неприводимого полинома существенно привязано к полю. Так, полином  $x^2 - 2$  неприводим в поле  $\mathbb{Q}$  ра-

циональных чисел, ибо он не имеет рациональных корней, но он приводим в поле  $\mathbb{R}$  вещественных чисел:  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ .

**Предложение 10.** Пусть  $f \in K[x]$  и  $\varphi$  неприводим в  $K$ . Тогда либо  $f$  делится на  $\varphi$ , либо  $f$  взаимно прост с  $\varphi$ .

**Доказательство.** Рассмотрим нормализованный наибольший общий делитель  $d$  полиномов  $f$  и  $\varphi$ . Полином  $\varphi$  делится на  $d$  и  $d \in K[x]$ . Поэтому  $d$  или ассоциирован с  $\varphi$ , или равен 1. В первом случае  $f$  делится на  $\varphi$ , ибо делится на  $d$ . Во втором  $f$  и  $\varphi$  взаимно просты.

**Предложение 11.** Если  $\varphi_1$  и  $\varphi_2$  неприводимы в  $K[x]$ , то они либо взаимно просты, либо ассоциированы.

Действительно, если  $\varphi_1$  и  $\varphi_2$  не взаимно просты, то  $\varphi_1$  делится на  $\varphi_2$  и  $\varphi_2$  делится на  $\varphi_1$ , так что  $\varphi_1$  и  $\varphi_2$  ассоциированы.

**Предложение 12.** Пусть  $f_1, f_2 \in K[x]$  и произведение  $f_1 f_2$  делится на неприводимый в  $K[x]$  полином  $\varphi$ . Тогда один из сомножителей делится на  $\varphi$ .

Действительно, либо  $f_1$  делится на  $\varphi$ , либо  $f_1$  и  $\varphi$  взаимно просты. Во втором случае  $f_2$  делится на  $\varphi$  в силу предложения 4.

**Предложение 13.** Пусть  $f_1, f_2, \dots, f_k \in K[x]$  и произведение  $f_1 f_2 \dots f_k$  делится на неприводимый в  $K[x]$  полином  $\varphi$ . Тогда один из сомножителей делится на  $\varphi$ .

Доказывается очевидным применением индукции на основании предложения 12.

**Предложение 14.** Если неприводимый над  $K$  полином имеет корень  $x_0$  в некотором расширении  $\mathbb{R}$  поля  $K$  и этот корень является корнем полинома  $f \in K[x]$ , то  $f$  делится на  $\varphi$ .

Действительно,  $f$  и  $\varphi$  не взаимно просты, ибо имеют общий делитель  $x - x_0 \in \mathbb{R}[x]$ , и, согласно предложению 10,  $f$  делится на  $\varphi$ .

Отсюда следует, что любой корень полинома  $\varphi$  является корнем  $f$ , так что, по словам венгерского математика Пойа, «корни неприводимых полиномов ходят в гости всей семье».

### 6. Каноническое разложение.

**Предложение 15.** Каждый полином  $f \in K[x]$  степени  $\geq 1$  делится по крайней мере на один неприводимый в  $K[x]$  полином.

**Доказательство** индукцией по степени. Полиномы первой степени неприводимы. Далее, если  $f$  неприводим, то он делится на себя. Если приводим, то делится на полином  $f_1 \in K[x]$  меньшей степени, который по индуктивному предположению делится на неприводимый в  $K[x]$  полином  $\varphi$ . Тогда и  $f$  делится на  $\varphi$ .

**Теорема 16.** Любой полином из  $K[x]$  степени  $\geq 1$  может быть представлен в виде произведения неприводимых над  $K$  полиномов, и такое представление единственно с точностью до порядка сомножителей и ассоциированности.

**Доказательство.** Пусть  $f \in K[x]$ . В силу предложения 14  $f$  делится на неприводимый полином  $\varphi_1$ , так что  $f = \varphi_1 f_1$ . В свою

очередь,  $f_1$  делится на некоторый неприводимый полином  $\varphi_2$ , так что  $f_1 = \varphi_2 f_2$  и  $f = \varphi_1 \varphi_2 f_2$ , и т. д. Процесс выделения неприводимых сомножителей закончится в конечное число шагов, ибо степени полиномов  $f, f_1, f_2 \dots$  строго убывают. Итак,  $f = \varphi_1 \varphi_2 \dots \varphi_k$ , где все  $\varphi_i$  неприводимы. Остается доказать единственность разложений. Применим индукцию по степени. Базу индукции дают полиномы первой степени. Пусть  $f = \varphi_1 \varphi_2 \dots \varphi_k$  и  $f = \psi_1 \psi_2 \dots \psi_l$  — два разложения полинома  $f$  на неприводимые. Произведение  $\psi_1 \psi_2 \dots \psi_l$  делится на  $\varphi_1$ . В силу предложения 13 один из сомножителей  $\psi_1, \psi_2, \dots, \psi_l$  делится на  $\varphi_1$ . За счет изменения нумерации можно считать, что  $\psi_1$  делится на  $\varphi_1$ . Так как  $\psi_1$  и  $\varphi_1$  оба неприводимы, они ассоциированы, т. е.  $\psi_1 = c_1 \varphi_1$  при  $c_1 \in K$ . Положим  $f = \varphi_1 f_1$ . Полином  $f_1 \in K[x]$  имеет меньшую степень чем  $f$  и имеет два разложения на неприводимые сомножители:  $f_1 = \varphi_2 \dots \varphi_k$  и  $f_1 = (c_1 \varphi_2) \dots \psi_l$ . В силу индуктивного предположения эти разложения совпадают с точностью до порядка сомножителей и ассоциированности, а значит, такими же будут разложения  $f = \varphi_1 \varphi_2 \dots \varphi_k$  и  $f = \psi_1 \psi_2 \dots \psi_l$ . Теорема доказана.

Если считать неприводимые полиномы нормализованными, то в разложение следует ввести константный множитель  $a_0$ , равный коэффициенту в старшем члене полинома  $f$ , так что разложение принимает вид  $f = a_0 \varphi_1 \varphi_2 \dots \varphi_k$ . В этой форме разложение единственно с точностью до порядка следования сомножителей. Среди сомножителей могут быть равные, и их можно объединить в степени. Разложение принимает вид

$$f = a_0 \varphi_1^{n_1} \varphi_2^{n_2} \dots \varphi_m^{n_m},$$

где  $\varphi_1, \varphi_2, \dots, \varphi_m$  — попарно различные нормализованные неприводимые в  $K[x]$  полиномы. Это разложение называется *каноническим* разложением на множители полинома из  $K[x]$ . Оно аналогично разложению целых чисел в произведение простых.

**Предложение 17.** *Над любым полем существует бесконечно много неприводимых полиномов.*

Доказательство проведем по той же схеме, что и доказательство бесконечности множества простых чисел. Именно, если дана любая конечная совокупность неприводимых полиномов  $\varphi_1, \varphi_2, \dots, \varphi_k$ , составим полином  $F = \varphi_1 \varphi_2 \dots \varphi_k + 1$ . Он делится по крайней мере на один неприводимый полином  $\psi$ , который не может равняться ни  $\varphi_1$ , ни  $\varphi_2, \dots$ , ни  $\varphi_k$ , ибо иначе 1 делилась бы на  $\psi$ . Таким образом, для любого конечного множества неприводимых полиномов мы можем построить новый неприводимый полином, не содержащийся в этом множестве.

Предложение 17 тривиально, если поле содержит бесконечно много элементов, ибо над таким полем существует бесконечно много полиномов первой степени  $x - c$ , которые все неприводимы, и содержательно лишь для конечных полей, к числу которых принадлежат кольца вычетов по простым модулям. Для любого ко-

нечного поля существует лишь конечное число  $q^n$  нормализованных полиномов  $x^n + a_1x^{n-1} + \dots + a_n$  степени  $n$  (здесь  $q$  обозначает число элементов поля). Поскольку число неприводимых полиномов бесконечно, среди них существуют полиномы сколь угодно высокой степени. При помощи значительно более тонких рассуждений можно доказать, что над конечным полем существуют неприводимые полиномы любой степени.

Вычислим неприводимые полиномы второй и третьей степени над полем из двух элементов (полем вычетов по модулю 2). Полиномов первой степени два:  $x$  и  $x+1$ . Полиномов второй степени четыре:  $x^2$ ,  $x^2+1$ ,  $x^2+x$  и  $x^2+x+1$ . Из них приводимы  $x^2$ ,  $(x+1)^2 = x^2+1$  и  $x(x+1) = x^2+x$ . Неприводимым оказывается один полином  $x^2+x+1$ . Полиномов третьей степени восемь. Из них шесть приводимы:  $x^3$ ,  $x^2(x+1) = x^3+x^2$ ,  $x(x+1)^2 = x^3+x$ ,  $(x+1)^3 = x^3+x^2+x+1$ ,  $x(x^2+x+1) = x^3+x^2+x$  и  $(x+1)(x^2+x+1) = x^3+1$ . Остальные два полинома  $x^3+x+1$  и  $x^3+x^2+1$  неприводимы.

Аналогично, отбрасывая приводимые полиномы, которые легко конструируются из неприводимых полиномов меньших степеней, можно строить неприводимые полиномы четвертой, пятой степеней и т. д. Имеются и другие, более тонкие средства.

**7. Каноническое разложение над полем  $\mathbb{R}$  комплексных чисел и над полем  $\mathbb{C}$  вещественных чисел.** Каноническое разложение над полем  $\mathbb{C}$  нам уже известно. Это разложение  $f(x) = a_0(x-x_1)^{n_1} \dots (x-x_k)^{n_k}$  на линейные множители, соответствующие корням  $f(x)$ .

**Предложение 18.** *Над полем вещественных чисел неприводимыми полиномами являются только полиномы первой степени и полиномы второй степени, не имеющие вещественных корней.*

**Доказательство.** Пусть  $f = a_0x^n + \dots + a_n \in \mathbb{R}[x]$  и  $n \geq 2$ . Если полином  $f$  имеет вещественный корень, то он имеет делитель первой степени и, следовательно, приводим. Неприводимыми могут быть только полиномы, не имеющие вещественных корней. Пусть  $f$  — такой полином. Он имеет по крайней мере один комплексный корень  $x_0 = a + bi$ , при  $b \neq 0$ . Рассмотрим вспомогательный полином

$$\varphi(x) = (x-x_0)(x-\bar{x}_0) = (x-a-bi)(x-a+bi) = x^2 - 2ax + a^2 + b^2.$$

Ясно, что  $\varphi(x) \in \mathbb{R}[x]$  и  $\varphi$  неприводим над  $\mathbb{R}$ , ибо иначе он имел бы делитель первой степени и вещественный корень. Полиномы  $f$  и  $\varphi$  не взаимно простые, ибо имеют общий корень в  $\mathbb{C}$  и, следовательно,  $f$  делится на  $\varphi$ . Если степень  $f$  равна 2, то  $f$  ассоциирован с  $\varphi$  и неприводим. Если степень  $f$  больше 2, то  $f$  приводим.

В силу доказанного предложения каноническое разложение полинома  $f \in \mathbb{R}[x]$  имеет вид:

$$f(x) = a_0(x-x_1)^{m_1} \dots (x-x_k)^{m_k} (x^2+p_1x+q_1)^{l_1} \dots (x^2+p_rx+q_r)^{l_r},$$

где полиномы  $x^2 + p_i x + q_i \in \mathbb{R}[x]$  не имеют вещественных корней, т. е.  $p_i^2 - 4q_i < 0$ .

Отметим простое, но важное следствие: *если полином с вещественными коэффициентами имеет комплексный корень  $a + bi$ ,  $b \neq 0$ , то он имеет и сопряженный корень  $a - bi$  той же кратности.*

Действительно, комплексные корни  $a + bi$  при  $b \neq 0$  являются корнями полиномов второй степени, входящих в каноническое разложение, а каждый такой полином вместе с корнем  $a + bi$  имеет корень  $a - bi$ .

**Пример.** Найти каноническое разложение в  $\mathbb{R}[x]$  полинома  $x^{2n} + 1$ .

Здесь множителей первой степени нет, так как полином не имеет вещественных корней. Все комплексные корни простые, так что множители второй степени входят с показателями 1. Сперва напишем разложение в кольце  $\mathbb{C}[x]$ , для чего найдем корни

$$\begin{aligned} x_k &= \sqrt[2n]{-1} = \sqrt[2n]{\cos(-\pi) + i \sin(-\pi)} = \\ &= \cos \frac{(2k-1)\pi}{2n} + i \sin \frac{(2k-1)\pi}{2n} \end{aligned}$$

при  $k = 1, 2, \dots, 2n$ . Корни  $x_k$  при  $k = 1, 2, \dots, n$  имеют аргументы меньше  $\pi$ , так что они находятся в верхней полуплоскости. Корни  $x_k$  при  $k = n+1, \dots, 2n$  расположены в нижней полуплоскости и, в силу следствия из канонического разложения, сопряжены с корнями  $x_k$  при  $k = 1, \dots, n$  (легко проверить непосредственно, что  $\bar{x}_k = x_{2n-k}$ ). Поэтому

$$\begin{aligned} x^{2n} + 1 &= \prod_{k=1}^n (x - x_k) \prod_{k=n+1}^{2n} (x - x_k) = \prod_{k=1}^n (x - x_k) (x - \bar{x}_k) = \\ &= \prod_{k=1}^n (x^2 - (x_k + \bar{x}_k)x + x_k \bar{x}_k) = \prod_{k=1}^n \left( x^2 - 2x \cos \frac{(2k-1)\pi}{2n} + 1 \right). \end{aligned}$$

## § 2. Производная

### 1. Определение производной и формулы для ее вычисления.

Введем понятие производной от полинома  $f(x) \in K[x]$ . Для полиномов над любым полем обычное понятие производной как предела отношения приращений, не работает, ибо понятие предела, например, для конечных полей не имеет смысла. Определим производную формально. Именно, *производной* от полинома

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

называется полином

$$f'(x) = n a_0 x^{n-1} + (n-1) a_1 x^{n-2} + \dots + a_{n-1}.$$

Производная обладает следующими свойствами.

1.  $(c)' = 0$ ,  $c$  — константа.

2.  $(x - c)' = 1$ .

3.  $(f_1 + f_2)' = f_1' + f_2'$ .

4.  $(cf)' = cf'$ .

Эти свойства непосредственно следуют из определения.

5.  $(f_1 f_2)' = f_1' f_2 + f_1 f_2'$ .

Это свойство докажем в три приема.

а)  $f_1 = ax^m$ ,  $f_2 = bx^k$ , так что  $f_1 f_2 = abx^{m+k}$ . Тогда

$$(f_1 f_2)' = (m+k)abx^{m+k-1} = mabx^{m+k-1} + kabx^{m+k-1} =$$

$$= (max^{m-1})bx^k + ax^m(kbx^{k-1}) = f_1' f_2 + f_1 f_2'.$$

б)  $f_1 = a_0 x^m + a_1 x^{m-1} + \dots + a_m$ ,  $f_2 = bx^k$ . Здесь  $f_1 f_2 = a_0 x^m \cdot bx^k + a_1 x^{m-1} \cdot bx^k + \dots + a_m \cdot bx^k$ . В силу свойств 3, 4 и случая а)

$$(f_1 f_2)' = (a_0 x^m)' bx^k + a_0 x^m (bx^k)' + (a_1 x^{m-1})' bx^k +$$

$$+ a_1 x^{m-1} (bx^k)' + \dots + (a_m)' bx^k + a_m (bx^k)'.$$

Объединяя нечетные и четные слагаемые, получим  $(f_1 f_2)' = f_1' f_2 + f_1 f_2'$ .

с)  $f_1 = a_0 x^m + a_1 x^{m-1} + \dots + a_m$ ,  $f_2 = b_0 x^k + b_1 x^{k-1} + \dots + b_k$ . Тогда  $f_1 f_2 = f_1 b_0 x^k + f_1 b_1 x^{k-1} + \dots + f_1 b_k$  и, в силу свойств 3, 4 и случая б),

$$(f_1 f_2)' = f_1' b_0 x^k + f_1 (b_0 x^k)' + f_1' b_1 x^{k-1} + f_1 (b_1 x^{k-1})' + \dots + f_1' b_k + f_1 b_k' =$$

$$= f_1' (b_0 x^k + b_1 x^{k-1} + \dots + b_k) + f_1 (b_0 x^k + b_1 x^{k-1} + \dots + b_k)' =$$

$$= f_1' f_2 + f_1 f_2'.$$

6.  $(f_1 f_2 \dots f_k)' = f_1' f_2 \dots f_k + f_1 f_2' \dots f_k + \dots + f_1 f_2 \dots f_k'.$

Доказывается индукцией по  $k$ , на основании свойства 5.

7.  $(f^k)' = k f^{k-1} f'.$

Следует из свойства 6, достаточно положить  $f_1 = f_2 = \dots = f_k = f$ .

8.  $((x - c)^k)' = k(x - c)^{k-1}.$

Производная от производной называется *второй производной*, производная от второй производной называется *третьей производной* и т. д. Легко убедиться в том, что  $k$ -я производная от  $m$ -й производной равна  $(k + m)$ -й производной исходного полинома.

**2. Разложение полинома по степеням линейного двучлена.** Пусть  $f = a_0 x^n + a_1 x^{n-1} + \dots + a_n \in k[x]$  и  $x - c$  — данный линейный двучлен.

**Предложение 19.** Полином  $f$  может быть разложен по степеням  $x - c$ .

**Доказательство.** Проведем индукцию по степени с тривиальной базой полиномов нулевой степени. Разделим  $f$  на  $x - c$  с остатком. Получим

$$f(a) = (x - c)f_1(x) + b_n,$$

где  $b_n$  — остаток,  $f_1(x)$  — полином степени  $n - 1$ . В силу индуктивного предположения

$$f_1(x) = b_0(x - c)^{n-1} + b_1(x - c)^{n-2} + \dots + b_{n-1},$$

откуда

$$f(x) = b_0(x - c)^n + b_1(x - c)^{n-1} + \dots + b_{n-1}(x - c) + b_n.$$

Приведенное доказательство дает и процесс для вычисления коэффициентов. Свободный член  $b_n$  разложения дается как остаток от деления  $f$  на  $x - c$ . Рассуждение по индукции заменяет единообразный процесс, так что  $b_{n-1}$  есть остаток при делении неполного частного  $f_1$  на  $x - c$ , и вычисление последующих коэффициентов требует вычисления неполного частного  $f_2$  при делении  $f_1$  на  $x - c$ . Далее,  $b_{n-2}$  находится как остаток при делении  $f_2$  на  $x - c$  и т. д. Итак, нужно делить на  $x - c$  полином  $f$  и последующие неполные частные. Остатки дадут коэффициенты разложения, начиная со свободного члена. Деление целесообразно выполнять, пользуясь схемой Хорнера, рассмотренной на стр. 58.

**Пример.** Разложим полином  $x^5$  по степеням  $x - 2$ . Согласно схеме Хорнера запишем:

$$\begin{array}{r} 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \mid 2 \\ 1 \quad 2 \quad 4 \quad 8 \quad 16 \quad \underline{32} \\ 1 \quad 4 \quad 12 \quad 32 \quad \underline{80} \\ 1 \quad 6 \quad 24 \quad \underline{80} \\ 1 \quad 8 \quad \underline{40} \\ 1 \quad \underline{10} \\ 1 \end{array}$$

Остатки подчеркнуты. Таким образом,

$$x^5 = (x - 2)^5 + 10(x - 2)^4 + 40(x - 2)^3 + 80(x - 2)^2 + + 80(x - 2) + 32.$$

В случае поля нулевой характеристики можно дать удобную для теоретических рассуждений формулу для коэффициентов разложения.

Выведем эту формулу.

Пусть  $f = d_0 + d_1(x - c) + d_2(x - c)^2 + \dots + d_n(x - c)^n$  (нам удобно записать по возрастающим степеням  $x - c$ ).

Возьмем производные до  $n$ -го порядка включительно (дальнейшие все равны нулю):

$$\begin{aligned} f' &= d_1 + 2 d_2 (x - c) + \dots + n d_n (x - c)^{n-1}, \\ f'' &= 2 d_2 + 3 \cdot 2 d_3 (x - c) + \dots + n(n-1) d_n (x - c)^{n-2}, \\ &\dots \dots \dots \\ f^{(n-1)} &= (n-1)(n-2) \dots 2 d_{n-1} + n(n-1) \dots 2 d_n (x - c), \\ f^{(n)} &= n(n-1) \dots 2 d_n. \end{aligned}$$

Положим во всех этих равенствах  $x = c$ . Получим

$$\begin{aligned} f(c) &= d_0, \\ f'(c) &= d_1, \\ f''(c) &= 2 d_2, \\ &\dots \dots \dots \\ f^{(n-1)}(c) &= (n-1)(n-2) \dots 2 d_{n-1}, \\ f^{(n)}(c) &= n(n-1) \dots 2 d_n, \end{aligned}$$

откуда

$$d_0 = f(c), d_1 = \frac{f'(c)}{1}, d_2 = \frac{f''(c)}{2!}, \dots, d_{n-1} = \frac{f^{(n-1)}(c)}{(n-1)!}, d_n = \frac{f^{(n)}(c)}{n!},$$

и разложение принимает вид

$$f = f(c) + \frac{f'(c)}{1!} (x - c) + \frac{f''(c)}{2!} (x - c)^2 + \dots + \frac{f^{(n)}(c)}{n!} (x - c)^n.$$

Эта формула называется *формулой Тейлора*.

Для приближенного вычисления корней полинома бывает нужно вычислять  $f(c)$  и  $f'(c)$  при значении  $c$ , близком к корню. Ясно, что выполнить это проще всего при помощи схемы Хорнера, вычислив по этой схеме два коэффициента разложения  $f$  по степеням  $x - c$ .

**Пример.** Для полинома  $x^3 - x - 1$  вычислить  $f(1,2)$  и  $f'(1,2)$ .

Применяем схему Хорнера:

$$\begin{array}{r|rrrr} 1 & 0 & -1 & -1 & | 1,2 \\ 1 & 1,2 & 0,44 & -0,472 & \\ 1 & 2,4 & 3,32 & & \end{array}$$

Итак,  $f(1,2) = -0,472$  и  $f'(1,2) = 3,32$ .

### 3. Разделение множителей различной кратности.

**Предложение 20.** *Простой корень полинома не является корнем его производной.*

Пусть  $c$  — простой корень полинома  $f$ , так что  $f = (x - c)f_1$  и  $f_1$  не делится на  $x - c$ , т. е.  $f_1(c) \neq 0$ . Тогда  $f' = f_1 + (x - c)f_1'$  и  $f'(c) = f_1(c) \neq 0$ .

**Предложение 21.** *Корень  $c$  полинома из  $K[x]$  кратности  $k$  является корнем производной кратности  $k - 1$ , если только  $k$  не*

делится на характеристику основного поля  $K$  (в частности, если эта характеристика равна 0).

Действительно, пусть  $f = (x - c)^k f_1$ , причем  $f_1(c) \neq 0$ . Тогда  $f' = k(x - c)^{k-1} f_1 + (x - c)^k f_1' = (x - c)^{k-1} [k f_1 + (x - c) f_1'] = (x - c)^{k-1} F(x)$ . Полином  $F(x)$  не делится на  $x - c$ , ибо  $F(c) = k f_1(c) \neq 0$  ( $k$  не делится на характеристику!).

Эти предложения можно несколько обобщить.

Напомним, что полиномы  $f \in K[x]$  разлагаются в произведении неприводимых над  $K$  множителей

$$f = a_0 \varphi_1^{k_1} \varphi_2^{k_2} \dots \varphi_m^{k_m}, \quad \varphi_i \neq \varphi_j.$$

Предположим, что характеристика поля  $k$  равна нулю.

**Предложение 22.** *Однократный неприводимый множитель полинома не входит в разложение его производной.*

Действительно, пусть  $f = a_0 \varphi F$ ,  $\varphi$  неприводим и  $F$  не делится на  $\varphi$ . Тогда  $f' = a_0 \varphi' F + a_0 \varphi F'$ . Полином  $\varphi'$  ненулевой, его степень меньше степени  $\varphi$ , поэтому  $\varphi'$  взаимно прост с  $\varphi$  (в поле ненулевой характеристики могло случиться, что  $\varphi' = 0$ ). Полином  $F$  тоже взаимно прост с  $\varphi$ , ибо  $F$  не делится на  $\varphi$  и  $\varphi$  неприводим. Первое слагаемое  $a_0 \varphi' F$  взаимно просто с  $\varphi$ , второе  $a_0 \varphi F'$  делится на  $\varphi$ . Следовательно,  $f'$  взаимно прост с  $\varphi$ .

**Предложение 23.** *Неприводимый над  $K$  полином  $\varphi$ , входящий в разложение полинома  $f \in K[x]$  с показателем  $k$ , входит в разложение  $f'$  с показателем  $k - 1$ .*

Действительно, пусть  $f = \varphi^k F_1$  при  $F_1$ , взаимно простом с  $\varphi$ . Тогда  $f' = k \varphi^{k-1} \varphi' F_1 + \varphi^k F_1' = \varphi^{k-1} (k \varphi' F_1 + \varphi F_1')$ . Первое слагаемое в скобках  $k \varphi' F_1$  взаимно просто с  $\varphi$ , второе делится на  $\varphi$ . Следовательно, полином  $k \varphi' F_1 + \varphi F_1'$  взаимно прост с  $\varphi$  и  $f'$  не делится на  $\varphi^k$ .

Эти предложения позволяют, оставаясь в кольце  $K[x]$ , отделить друг от друга произведения неприводимых сомножителей, входящих в  $f \in K[x]$  с различными показателями.

Действительно, пусть  $f = a_0 \varphi_1^{k_1} \varphi_2^{k_2} \dots \varphi_m^{k_m}$  и пусть  $d_1$  — наибольший общий делитель  $f$  и  $f'$ . Неприводимыми множителями для  $d_1$  могут быть только  $\varphi_1, \varphi_2, \dots, \varphi_m$ , ибо  $f$  делится на  $d_1$ , и они входят в  $d_1$  с показателями  $k_1 - 1, k_2 - 1, \dots, k_m - 1$ , так что  $f = d_1 f_1$ , где  $d_1 = \varphi_1^{k_1-1} \varphi_2^{k_2-1} \dots \varphi_m^{k_m-1}$  и  $f_1 = a_0 \varphi_1 \varphi_2 \dots \varphi_m$ . В  $d_1$  не будут входить однократные неприводимые множители  $f$ . Найдем далее наибольший общий делитель  $d_2$  полиномов  $d_1$  и  $d_1'$ . Он будет состоять из неприводимых множителей, входящих в  $f$  с большим чем 2 показателем. Их показатели в  $d_2$  на 2 меньше, чем в  $f$ . Полином  $f_2 = \frac{d_1}{d_2}$  будет состоять из неприводимых множителей, входящих в  $f$  с показателями 2 и выше. Далее, пусть  $d_3$  есть наибольший об-

щий делитель  $d_2$  и  $d'_2$ ,  $f_3 = \frac{d_2}{d_3}$ . Полином  $f_3$  составлен из неприводимых множителей, входящих в  $f$  с показателем 3 и выше, и т. д. Частное от деления  $f_1$  на  $f_2$  будет составлено из неприводимых множителей, входящих в  $f$  ровно в первой степени, частное от деления  $f_2$  на  $f_3$  состоит из неприводимых множителей, входящих в  $f$  равно во второй степени и т. д.

Пример.  $f = x^5 + 2x^4 - 2x^3 - 4x^2 + x + 2$ .  $f' = 5x^4 + 8x^3 - 6x^2 - 8x + 1$ .

Применив алгоритм Евклида, получим, что н. о. д.  $(f, f')$  равен  $d_1 = x^2 - 1$ . Далее,  $d'_1 = 2x$ ,  $d_2 = 1$ ,  $d'_2 = 0$ ,  $d_3 = 1$ . Поэтому  $f_1 = f/d = x^3 + 2x^2 - x - 2$ ,  $f_2 = d_1/d_2 = x^2 - 1$ ,  $f_3 = d_2/d_3 = 1$ . Поделив  $f_1$  на  $f_2$ , получим  $x + 2$ , частное от деления  $f_2$  на  $f_3$  есть  $x^2 - 1$ . Итак,  $f = (x + 2)(x^2 - 1)^2 = (x + 2)(x - 1)^2(x + 1)^2$ .

### § 3. Рациональные дроби

**1. Определение рациональных дробей и действий над ними.** *Дробной рациональной функцией* или, короче, *рациональной дробью* называется частное от деления двух полиномов. Если полиномы рассматривать как функции, в определении дробной рациональной функции нет никаких затруднений. Однако возникают некоторые неприятности при привычном всем действии сокращения дробей. Так, строго говоря, мы должны считать функции  $\frac{1}{x+1}$  и  $\frac{x-1}{x^2-1}$  как различные, ибо различны их естественные области определения. Однако вторая превращается в первую при сокращении на  $x - 1$ .

Мы рассматривали полиномы не как функции с заранее данной областью определения, а как формальные выражения, над которыми можно совершать действия и преобразования по определенным правилам. Эту же точку зрения нам надлежит принять при рассмотрении рациональных дробей.

**Определение.** Рациональной функцией над полем  $K$  назовем «картинку» вида  $\frac{f}{g}$ , где  $f$  и  $g \in K[x]$ , причем  $g(x) \neq 0$ .

Введем теперь понятие равенства дробей.

Две дроби  $\frac{f_1}{g_1}$  и  $\frac{f_2}{g_2}$  считаются *равными*, если полином  $f_1g_2 - f_2g_1$  равен 0.

Здесь, в отличие от прежних определений равенства для вновь вводимых объектов (комплексных чисел, полиномов и матриц), равенство определяется при помощи некоторого соглашения, а не по тождественности записи. В математике принято называть *эквивалентностью* или *равенством* такое отношение между сравниваемыми объектами, которое удовлетворяет следующим требованиям.

1. Рефлексивность:  $a = a$ , т. е. объект  $a$  равен самому себе.

2. Симметричность: из  $a = b$  следует  $b = a$ .

3. Транзитивность: из  $a = c$  и  $b = c$  следует, что  $a = b$ , т. е. два объекта, равные третьему, равны между собой.

Проверим эти требования для равенства рациональных дробей.

Рефлексивность:  $\frac{f}{g} = \frac{f}{g}$ , ибо  $fg - gf = 0$ .

Симметричность: если  $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ , то  $\frac{f_2}{g_2} = \frac{f_1}{g_1}$ , ибо  $f_2g_1 - f_1g_2 = -(f_1g_2 - f_2g_1) = 0$ .

Транзитивность. Если  $\frac{f_1}{g_1} = \frac{f_3}{g_3}$  и  $\frac{f_2}{g_2} = \frac{f_3}{g_3}$ , то  $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ .

Действительно, пусть  $\frac{f_1}{g_1} = \frac{f_3}{g_3}$  и  $\frac{f_2}{g_2} = \frac{f_3}{g_3}$ . Рассмотрим полином  $g_3(f_1g_2 - f_2g_1)$ . Он равен  $g_3f_1g_2 - g_2f_3g_1 + g_2f_3g_1 - g_3f_2g_1 = g_2(f_1g_3 - f_3g_1) + g_1(f_3g_2 - f_2g_3) = 0$ , ибо  $\frac{f_1}{g_1} = \frac{f_3}{g_3}$  и  $\frac{f_3}{g_3} = \frac{f_2}{g_2}$ .

Из равенства  $g_3(f_1g_2 - f_2g_1) = 0$  заключаем, что  $f_1g_2 - f_2g_1 = 0$ , т. е. что  $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ , ибо кольцо  $K[x]$  есть область целостности.

Из данного определения равенства следует, что при любом полиноме  $h \neq 0$  имеет место равенство  $\frac{f}{g} = \frac{fh}{gh}$ , т. е. в числитель и знаменатель можно вставлять один и тот же множитель или сокращать на общий множитель. Далее, само определение равенства можно сформулировать так: две дроби равны, если от одной из них можно перейти к другой посредством вставки и сокращения.

Действительно, если  $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ , т. е.  $f_1g_2 = f_2g_1$ , то

$$\frac{f_1}{g_1} = \frac{f_1g_2}{g_1g_2} = \frac{f_2g_1}{g_1g_2} = \frac{f_2}{g_2}.$$

Заметим еще, что  $\frac{0}{g} = \frac{0g}{1 \cdot g} = \frac{0}{1}$ , т. е. все дроби с нулевым числителем равны между собой и равны  $\frac{0}{1}$ .

Обратимся теперь к определениям действий над дробями. Определим сложение дробей:

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} \stackrel{\text{def}}{=} \frac{f_1g_2 + f_2g_1}{g_1g_2}.$$

Это определение совершенно естественно: посредством надлежащих вставок выравниваются знаменатели и затем числители складываются. Однако несмотря на естественность данного определения, нужно проверить его корректность — не изменится ли результат при замене слагаемых на равные.

Пусть  $\frac{f_1}{g_1} = \frac{f_3}{g_3}$  и  $\frac{f_2}{g_2} = \frac{f_4}{g_4}$ . Тогда

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2 + f_2g_1}{g_1g_2} \quad \text{и} \quad \frac{f_3}{g_3} + \frac{f_4}{g_4} = \frac{f_3g_4 + f_4g_3}{g_3g_4}.$$

Сравним результаты, исходя из определения равенства дробей. Имеем

$$g_3g_4(f_1g_2 + f_2g_1) - g_1g_2(f_3g_4 + f_4g_3) = \\ = g_2g_4(f_1g_3 - f_3g_1) + g_1g_3(f_2g_4 - f_4g_2) = 0.$$

Результаты сложения оказались равны, так что определение корректно.

Из определения ясно, что сложение коммутативно и ассоциативно. Элемент  $\frac{0}{1}$  играет роль нуля. Действительно,  $\frac{f}{g} + \frac{0}{1} = \frac{f \cdot 1 + 0 \cdot g}{g \cdot 1} = \frac{f}{g}$ . Для  $\frac{f}{g}$  противоположным является  $-\frac{f}{g}$ , ибо  $\frac{f}{g} + \frac{-f}{g} = \frac{fg - fg}{g^2} = \frac{0}{g^2} = \frac{0}{1}$ .

Итак, рациональные дроби образуют абелеву группу по отношению к сложению.

Теперь определим умножение столь же естественным образом:

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} \stackrel{\text{def}}{=} \frac{f_1f_2}{g_1g_2}.$$

Проверим корректность определения. Пусть  $\frac{f_1}{g_1} = \frac{f_3}{g_3}$  и  $\frac{f_2}{g_2} = \frac{f_4}{g_4}$ , т. е.  $f_1g_3 - f_3g_1 = 0$  и  $f_2g_4 - f_4g_2 = 0$ .

Сравним, согласно определению равенства, дроби  $\frac{f_1f_2}{g_1g_2}$  и  $\frac{f_3f_4}{g_3g_4}$ . Имеем

$$f_1f_2g_3g_4 - f_3f_4g_1g_2 = f_1f_2g_3g_4 - f_3f_2g_1g_4 + f_3f_2g_1g_4 - f_3f_4g_1g_2 = \\ = f_2g_4(f_1g_3 - f_3g_1) + f_3g_1(f_2g_4 - f_4g_2) = 0.$$

Умножение, очевидно, коммутативно и ассоциативно и связано со сложением дистрибутивностью. Проверим последнее:

$$\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) \frac{f_3}{g_3} = \frac{f_1g_2 + f_2g_1}{g_1g_2} \cdot \frac{f_3}{g_3} = \frac{f_1f_3g_2 + f_2f_3g_1}{g_1g_2g_3}; \\ \frac{f_1}{g_1} \cdot \frac{f_3}{g_3} + \frac{f_2}{g_2} \cdot \frac{f_3}{g_3} = \frac{f_1f_3}{g_1g_3} + \frac{f_2f_3}{g_2g_3} = \frac{f_1f_3g_2}{g_1g_2g_3} + \frac{f_2f_3g_1}{g_1g_2g_3} = \frac{f_1f_3g_2 + f_2f_3g_1}{g_1g_2g_3}.$$

Элемент  $\frac{1}{1}$  является единицей. Действительно,  $\frac{f}{g} \cdot \frac{1}{1} = \frac{f}{g}$ . Далее, всякий отличный от нуля элемент имеет обратный. Действительно,  $\frac{f}{g} \neq \frac{0}{1}$  означает, что  $f \neq 0$ , т. е.  $\frac{g}{f}$  имеет смысл и  $\frac{f}{g} \cdot \frac{g}{f} = \frac{1}{1}$ .

Итак, множество построенных формальных дробей образует поле. Оно называется *полем рациональных функций* от буквы  $x$  и обозначается  $K(x)$  (простые скобки!).

Кольцо  $K[x]$  естественно вкладывается в поле  $K(x)$ .

Именно, положим  $\frac{f}{1} = f$ , где  $f \in K[x]$ . Нужно убедиться в корректности этого отождествления, для чего нужно доказать, что оно не вступает в противоречие с определением равенства и определениями действий сложения и умножения. Это легко проверяется:  $\frac{f_1}{1} = \frac{f_2}{1}$  равносильно равенству  $f_1 \cdot 1 - f_2 \cdot 1 = 0$ , т. е.  $f_1 = f_2$ ;  $\frac{f_1}{1} + \frac{f_2}{1} = \frac{f_1 + f_2}{1}$  и  $\frac{f_1}{1} \cdot \frac{f_2}{1} = \frac{f_1 f_2}{1}$ , т. е. при сложении и умножении дробей вида  $\frac{f}{1}$  получаются результаты, соответствующие результатам тех же действий над полиномами.

2. **Поле частных.** Присмотримся внимательнее к рассуждениям п. 1. Мы видим, что в этих рассуждениях мы почти не пользовались тем, что употреблявшиеся буквы обозначали полиномы. Нам было нужно, чтобы эти буквы были элементами коммутативного ассоциативного кольца с единицей, являющегося областью целостности. Этим мы пользовались при проверке транзитивности равенства дробей и при определениях их сложения и умножения, так как в определении дроби запрещено появление элемента 0 в знаменателе и нужно, чтобы знаменатель суммы и произведения был отличен от нуля.

Мы можем теперь повторить построения п. 1 на более высоком уровне абстракции.

Пусть  $A$  — произвольная коммутативная ассоциативная область целостности. Рассмотрим множество пар  $\frac{f}{g}$ ,  $g \neq 0$ , элементов  $A$ . Введем для них определения равенства и действий сложения и умножения:

1.  $\frac{f_1}{g_1} \stackrel{\text{def}}{=} \frac{f_2}{g_2} \Leftrightarrow f_1 g_2 - f_2 g_1 = 0$ ;
2.  $\frac{f_1}{g_1} + \frac{f_2}{g_2} \stackrel{\text{def}}{=} \frac{f_1 g_2 + f_2 g_1}{g_1 g_2}$ ;
3.  $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} \stackrel{\text{def}}{=} \frac{f_1 f_2}{g_1 g_2}$ .

Слово в слово так же, как в п. 1, проверяется корректность этих определений. По отношению к сложению символы  $\frac{f}{g}$  образуют абелеву группу с нулем  $\frac{0}{g}$  (который не зависит от  $g$ , согласно определению равенства). По отношению к умножению все ненулевые пары (т. е. отличные от  $\frac{0}{g}$ ) образуют абелеву группу с единицей  $\frac{g}{g}$  (не зависящей от  $g$ ) и с обратным для  $\frac{f}{g}$  элементом  $\frac{g}{f}$ . Умножение со сложением связано дистрибутивностью. Таким образом, мы построили поле, которое называется *полем частных* для области целостности  $A$ .

Кольцо  $A$  могло не содержать единицу, в поле частных она появляется.

Наконец, кольцо  $A$  вкладывается в свое поле частных посредством отождествления

$$\frac{fg}{g} = f \quad (\text{при любом } g \neq 0).$$

Ясно, что поле частных для кольца целых чисел есть поле  $\mathbb{Q}$  рациональных чисел. Подобно полиномам от одной буквы, множество полиномов  $K[x_1, \dots, x_k]$  от нескольких букв  $x_1, x_2, \dots, x_k$  является областью целостности и вкладывается в поле частных  $K(x_1, x_2, \dots, x_n)$ , состоящее из дробей  $\frac{F(x_1, x_2, \dots, x_k)}{G(x_1, x_2, \dots, x_k)}$ .

**3. Правильные рациональные дроби.** Вернемся к изучению рациональных дробей от одной буквы. Рациональная дробь может быть записана в форме  $\frac{f}{g}$  многими способами. Однако всегда можно перейти к несократимой записи — со взаимно простыми числителем и знаменателем. Для этого достаточно найти наибольший общий делитель числителя и знаменателя и сократить на него. Далее, старший коэффициент знаменателя можно вынести и присоединить к числителю, после чего знаменатель можно считать нормализованным. Несократимая запись дроби с нормализованным знаменателем называется нормализованной записью дроби или *нормализованной* дробью. Две нормализованные дроби равны, только если равны их числители и знаменатели, т. е. совпадают по записи. Действительно, если  $\frac{f_1}{g_1} = \frac{f_2}{g_2}$  — равенство двух нормализованных дробей, то  $f_1 g_2 = f_2 g_1$ . Полином  $g_1$  взаимно прост с  $f_1$  в силу несократимости  $\frac{f_1}{g_1}$ , и, следовательно,  $g_2$  делится на  $g_1$ . Аналогично,  $g_1$  делится на  $g_2$ , т. е. они ассоциированы. Так как их старшие коэффициенты равны 1, они совпадают; следовательно, совпадают  $f_1$  и  $f_2$ .

Рациональная дробь называется *правильной*, если степень ее числителя меньше степени знаменателя. Если дробь правильная в некоторой записи, то она остается правильной в несократимой записи, так как при сокращении степени числителя и знаменателя уменьшаются на одно и то же число, а значит, и во всякой другой записи, ибо любая запись получается из несократимой посредством умножения числителя и знаменателя на один и тот же полином.

**Предложение 1.** *Любая рациональная дробь есть сумма полинома и правильной дроби.*

Действительно, пусть  $\frac{f}{g}$  — данная дробь. Поделим  $f$  на  $g$  с остатком:  $f = gq + r$ ,  $\deg r < \deg g$ . Тогда  $\frac{f}{g} = \frac{gq + r}{g} = \frac{gq}{g} + \frac{r}{g} =$

$= q + \frac{r}{g}$ . Здесь  $q$  — полином (он может равняться 0, если  $\deg f < \deg g$ ), а  $\frac{r}{g}$  — правильная дробь.

**Предложение 2.** Сумма, разность и произведение правильных дробей есть правильная дробь.

(Здесь имеется существенное отличие от арифметики рациональных чисел, где, например,  $\frac{1}{2} + \frac{2}{3} = \frac{7}{6}$ .)

**Доказательство.** Пусть дроби  $\frac{f_1}{g_1}$  и  $\frac{f_2}{g_2}$  правильные. Они останутся правильными и при записи  $\frac{f_1 g_2}{g_1 g_2}$  и  $\frac{f_2 g_1}{g_1 g_2}$ , а  $\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2}$ . Степени обоих слагаемых в числителе меньше степени знаменателя, следовательно, степень числителя меньше степени знаменателя. Для произведения  $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$  имеем  $\deg f_1 f_2 = \deg f_1 + \deg f_2 < \deg g_1 + \deg g_2 = \deg g_1 g_2$ .

Таким образом, правильные дроби образуют кольцо. Оно не содержит 1.

#### 4. Разложение рациональной дроби на простейшие.

**Предложение 3.** Если знаменатель правильной рациональной дроби  $\frac{f}{g} \in K(x)$  есть произведение двух взаимно простых полиномов,  $g = g_1 g_2$ , то дробь представляется в виде суммы двух правильных дробей со знаменателями, равными сомножителям  $g_1$  и  $g_2$  знаменателя исходной дроби, т. е.  $\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$ , причем обе дроби в правой части правильные. Такое представление единственно.

**Доказательство.** Так как  $g_1$  и  $g_2$  взаимно просты, найдутся полиномы  $M_1$  и  $M_2$  такие, что  $g_1 M_1 + g_2 M_2 = 1$ . Тогда

$$\frac{f}{g_1 g_2} = \frac{f}{g_1 g_2} (g_1 M_1 + g_2 M_2) = \frac{f M_1}{g_2} + \frac{f M_2}{g_1}.$$

В этом разложении слагаемые правой части, вообще говоря, не являются правильными дробями. Поделим полином  $f M_2$  на  $g_1$  с остатком:  $f M_2 = g_1 q + f_1$ ,  $\deg f_1 < \deg g_1$ , так что  $\frac{f M_2}{g_1} = q + \frac{f_1}{g_1}$ .

Присоединим  $q$  к первому слагаемому. Получим  $\frac{f}{g_1 g_2} = \frac{f M_1}{g_2} + q + \frac{f_1}{g_1} = \frac{f M_1 + q g_2}{g_2} + \frac{f_1}{g_1}$ . Здесь первое слагаемое  $\frac{f M_1 + q g_2}{g_2} = \frac{f_2}{g_2}$  автоматически оказывается правильной дробью как разность правильных дробей  $\frac{f}{g_1 g_2}$  и  $\frac{f_1}{g_1}$ . Итак,  $\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$  и оба слагаемых в правой части равенства — правильные дроби.

Остается доказать единственность. Пусть

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_3}{g_1} + \frac{f_4}{g_2},$$

причем все дроби правильные. Тогда  $\frac{f_1 - f_3}{g_1} = \frac{f_4 - f_2}{g_2}$  и  $g_2(f_1 - f_3) = g_1(f_4 - f_2)$ . Левая часть делится на  $g_1$  и полином  $g_2$  взаимно прост с  $g_1$ . Поэтому  $f_1 - f_3$  делится на  $g_1$ , что возможно только при  $f_1 - f_3 = 0$ , ибо степень  $f_1 - f_3$  меньше степени  $g_1$ . Итак,  $f_1 = f_3$  и, следовательно,  $f_2 = f_4$ . Предложение доказано полностью.

Теперь обобщим это предложение.

**Предложение 4.** Если знаменатель  $g$  правильной рациональной дроби  $\frac{f}{g} \in K(x)$  есть произведение  $g_1 g_2 \dots g_k$  нескольких попарно взаимно простых полиномов, то дробь представляется в виде суммы  $\frac{f_1}{g_1} + \frac{f_2}{g_2} + \dots + \frac{f_k}{g_k}$  правильных дробей и такое представление единственно.

Доказательство проведем индукцией по числу сомножителей. База индукции есть при  $k = 2$ . Далее,  $g = g_1(g_2 \dots g_k)$  и полиномы  $g_1$  и  $g_2 \dots g_k$  взаимно просты. Поэтому  $\frac{f}{g} = \frac{f_1}{g_1} + \frac{F}{g_2 \dots g_k}$ .

Ко второму слагаемому применяется индуктивное предположение.

Разложение  $\frac{f}{g} = \frac{f_1}{g_1} + \frac{F}{g_2 \dots g_k}$  единственно по предложению 3, и разложение  $\frac{F}{g_2 \dots g_k} = \frac{f_2}{g_2} + \dots + \frac{f_k}{g_k}$  единственно по индуктивному предположению. Следовательно, разложение  $\frac{f}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \dots + \frac{f_k}{g_k}$  единственно.

Полином из  $K[x]$  имеет каноническое разложение на неприводимые множители  $g = a_0 \varphi_1^{m_1} \varphi_2^{m_2} \dots \varphi_k^{m_k}$ . В соответствии с этим правильная рациональная дробь раскладывается на сумму правильных дробей со знаменателями  $\varphi_1^{m_1}, \varphi_2^{m_2}, \dots, \varphi_k^{m_k}$ . Эти дроби носят название *примарных*.

Действительно, пусть дробь (в нормализованной записи) есть  $\frac{f}{\varphi_1^{m_1} \varphi_2^{m_2} \dots \varphi_k^{m_k}}$ , где  $\varphi_1, \varphi_2, \dots, \varphi_k$  — попарно различные нормализованные неприводимые полиномы. Тогда они попарно взаимно просты и их степени  $\varphi_1^{m_1}, \dots, \varphi_k^{m_k}$  тоже попарно взаимно просты. Применение предложения 4 дает требуемое разложение:

$$\frac{f}{\varphi_1^{m_1} \varphi_2^{m_2} \dots \varphi_k^{m_k}} = \frac{f_1}{\varphi_1^{m_1}} + \frac{f_2}{\varphi_2^{m_2}} + \dots + \frac{f_k}{\varphi_k^{m_k}}.$$

Оно единственно в силу предыдущих предложений.

Примарная дробь называется *простейшей*, если ее числитель есть полином, степень которого меньше степени неприводимого полинома, входящего в знаменатель.

**Предложение 5.** *Любая правильная примарная дробь представляется в виде суммы простейших дробей.*

**Доказательство.** Пусть  $\frac{f}{\varphi^m}$  — данная примарная правильная дробь. Поделим  $f$  на  $\varphi$  с остатком:  $f = \varphi q_1 + f_1$ ,  $\deg f_1 < \deg \varphi$ . Тогда  $\frac{f}{\varphi^m} = \frac{f_1}{\varphi^m} + \frac{q_1}{\varphi^{m-1}}$ . Такое представление единственно, ибо если  $\frac{f}{\varphi^m} = \frac{f_1}{\varphi^m} + \frac{q_1}{\varphi^{m-1}}$  при  $\deg f_1 < \deg \varphi$ , то  $f = f_1 + q_1 \varphi$ , т. е.  $f_1$  есть остаток деления  $f$  на  $\varphi$  и  $q_1$  — неполное частное. Выделив остаток от деления  $q_1$  на  $\varphi$ ,  $q_1 = f_2 + \varphi q_2$ ,  $\deg f_2 < \deg \varphi$ , получим  $\frac{q_1}{\varphi^{m-1}} = \frac{f_2}{\varphi^{m-1}} + \frac{q_2}{\varphi^{m-2}}$ . Продолжая процесс, придем к правильной дроби  $\frac{q_{m-1}}{\varphi}$ , которая является простейшей. Итак,

$$\frac{f}{\varphi^m} = \frac{f_1}{\varphi^m} + \frac{f_2}{\varphi^{m-1}} + \dots + \frac{f_m}{\varphi} \quad (\text{где } f_m = q_{m-1}).$$

Единственность разложения очевидна, в силу единственности на каждом шагу процесса.

**Теорема 6.** *Правильная рациональная дробь из поля  $K(x)$  может быть представлена в виде суммы простейших дробей, и такое представление единственно.*

Действительно, всякая правильная дробь из  $K(x)$  единственным образом представляется в виде суммы правильных примарных дробей и каждая правильная примарная дробь представляется в виде суммы простейших. Если знаменатель исходной дроби имеет каноническое разложение  $\varphi_1^{n_1} \varphi_2^{m_2} \dots \varphi_k^{m_k}$ , то знаменателями простейших дробей будут  $\varphi_1^{n_1}$ ,  $\varphi_1^{n_1-1}, \dots, \varphi_1$ ,  $\varphi_2^{m_2}$ ,  $\varphi_2^{m_2-1}, \dots, \varphi_2$ ,  $\dots$ ,  $\varphi_k^{m_k}$ ,  $\varphi_k^{m_k-1}, \dots, \varphi_k$ .

**5. Разложение рациональной дроби на простейшие над полем  $\mathbb{C}$  комплексных чисел.** Поле  $\mathbb{C}$  всех комплексных чисел алгебраически замкнуто, и любой нормализованный полином разлагается на  $\mathbb{C}$  в произведение линейных множителей

$$g = (x - x_1)^{m_1} \dots (x - x_k)^{m_k}.$$

В этом случае простейшими дробями будут  $\frac{A}{(x - x_i)^{s_i}}$ , где  $A \in \mathbb{C}$ , так что разложение правильной дроби на простейшие

имеет вид

$$\frac{f}{g} = \frac{A_{11}}{(x-x_1)^{m_1}} + \dots + \frac{A_{1m_1}}{x-x_1} + \frac{A_{21}}{(x-x_2)^{m_2}} + \dots + \frac{A_{2m_2}}{x-x_2} + \dots$$

$$\dots + \frac{A_{k1}}{(x-x_k)^{m_k}} + \dots + \frac{A_{km_k}}{x-x_k}.$$

Это разложение играет значительную роль в математическом анализе. Простейшие дроби легко дифференцировать и интегрировать.

**6. Разложение рациональной дроби на простейшие над полем  $\mathbb{R}$  вещественных чисел.** Над полем  $\mathbb{R}$  имеется два типа неприводимых полиномов — полиномы первой степени  $x - x_i$  и полиномы второй степени  $x^2 + p_j x + q_j$  при  $p_j^2 - 4q_j < 0$ . Соответственно, имеется два типа простейших дробей:

$$\frac{A}{(x-x_i)^{m_i}} \quad \text{и} \quad \frac{Bx+C}{(x^2+p_j x+q_j)^{l_j}} \quad \text{при} \quad p_j^2 - 4q_j < 0.$$

Разложение над  $\mathbb{R}$  тоже полезно для целей математического анализа.

Пример.  $\frac{1}{(x-1)^2(x^2+1)}.$

Эта дробь разлагается на слагаемые  $\frac{A_1}{(x-1)^2}$ ,  $\frac{A_2}{x-1}$  и  $\frac{Bx+C}{x^2+1}$ . Записав это разложение и умножив на знаменатель  $(x-1)^2(x^2+1)$ , получим равенство

$$1 = A_1(x^2+1) + A_2(x-1)(x^2+1) + (Bx+C)(x-1)^2.$$

Нужно определить коэффициенты  $A_1$ ,  $A_2$ ,  $B$  и  $C$ . Самый естественный путь для их определения — так называемый *метод неопределенных коэффициентов*, т. е. сравнение коэффициентов при 1,  $x$ ,  $x^2$  и  $x^3$ . Это даст систему четырех уравнений с четырьмя неизвестными, имеющую, как мы уже знаем, единственное решение. Вот эта система:

$$\begin{aligned} A_1 - A_2 + C &= 1, \\ A_2 + B - 2C &= 0, \\ A_1 - A_2 - 2B + C &= 0, \\ A_2 + B &= 0, \end{aligned}$$

из которой находим  $A_1 = 1/2$ ,  $A_2 = -1/2$ ,  $B = 1/2$ ,  $C = 0$ , так что

$$\frac{1}{(x-1)^2(x^2+1)} = \frac{1}{2(x-1)^2} - \frac{1}{2(x-1)} + \frac{x}{2(x^2+1)}.$$

Коэффициенты можно было бы определить несколько проще, полагая в равенстве полиномов

$$1 = A_1(x^2+1) + A_2(x-1)(x^2+1) + (Bx+C)(x-1)^2$$



Рассмотрим несколько примеров ее применения.

Пример 1.  $\frac{x^3 + 5x + 7}{(x+2)(x+1)x(x-1)(x-2)}$ .

Здесь

$$\begin{aligned} F(x) &= (x+2)(x+1)x(x-1)(x-2), \\ F'(-2) &= (-2+1)(-2)(-2-1)(-2-2) = 24, \\ F'(-1) &= (-1+2)(-1)(-1-1)(-1-2) = -6, \\ F'(0) &= (0+2)(0+1)(0-1)(0-2) = 4, \\ F'(1) &= -6, \quad F'(2) = 24 \end{aligned}$$

и

$$\begin{aligned} \frac{x^3 + 5x + 7}{(x+2)(x+1)x(x-1)(x-2)} &= \\ &= -\frac{11}{24(x+2)} - \frac{1}{6(x+1)} + \frac{7}{4x} - \frac{13}{6(x-1)} + \frac{25}{24(x-2)}. \end{aligned}$$

Пример 2. Разложить над полем  $\mathbb{R}$  дробь  $\frac{1}{x^{2n}+1}$ .

Сперва напишем разложение над  $\mathbb{C}$ . Напомним, что корни полинома  $F(x) = x^{2n} + 1$  лежат на единичной окружности и попарно сопряжены. Именно, с корнями  $x_k = \cos \frac{(2k-1)\pi}{2n} + i \sin \frac{(2k-1)\pi}{2n}$ ,  $k=1, 2, \dots, n$ , сопряжены корни  $\bar{x}_k = x_{2n+1-k}$ . Корни попарно различны, так что формула Лагранжа применима. Имеем  $F'(x) = 2nx^{2n-1}$ , откуда  $F'(x_k) = 2nx_k^{2n-1} = 2nx_k^{-1}x_k^{2n} = -2nx_k^{-1}$ . По формуле Лагранжа

$$\frac{1}{x^{2n}+1} = -\frac{1}{2n} \sum_{k=1}^n \frac{x_k}{x-x_k} - \frac{1}{2n} \sum_{k=1}^n \frac{\bar{x}_k}{x-\bar{x}_k}.$$

Объединив теперь комплексно сопряженные слагаемые, получим

$$\begin{aligned} \frac{1}{x^{2n}+1} &= -\frac{1}{2n} \sum_{k=1}^n \frac{x_k}{x-x_k} + \frac{\bar{x}_k}{x-\bar{x}_k} = \\ &= -\frac{1}{2n} \sum_{k=1}^n \frac{(x_k + \bar{x}_k)x - 2}{x^2 - (x_k + \bar{x}_k)x + 1} = \frac{1}{n} \sum_{k=1}^n \frac{1 - x \cos \frac{(2k-1)\pi}{2n}}{x^2 - 2x \cos \frac{(2k-1)\pi}{2n} + 1}. \end{aligned}$$

Пример 3. Разложить дробь  $\frac{1}{x^p - x}$  на простейшие над полем  $\text{GF}(p)$  вычетов по модулю  $p$ .

В силу теоремы Ферма все элементы поля  $\bar{0}, \bar{1}, \dots, \overline{p-1}$  суть корни полинома  $F(x) = x^p - x$ , так что  $x^p - x = x(x - \bar{1}) \dots (x - \overline{p-1})$ . Имеем  $F'(x) = px^{p-1} - 1 = -1$ . Следовательно,

$$\frac{1}{x^p - x} = - \sum_{k=0}^{p-1} \frac{1}{x - \bar{k}}.$$



Он отличен от нуля, ибо все  $x_i$  попарно различны. Следовательно, задача имеет единственное решение. Оно дает интерполяционный полином, степень которого не превосходит  $n-1$  (она может оказаться меньше  $n-1$ , если один или несколько старших коэффициентов окажутся равными нулю). Интерполяционный полином степени  $n-1$  или меньше является интерполяционным полиномом наименьшей степени, ибо среди полиномов степени меньше  $n$  он существует только один и все другие интерполяционные полиномы имеют степень  $n$  и выше.

**2. Интерполяционная формула Лагранжа.** Для интерполяционного полинома степени не большей  $n-1$  существует несложная формула. Ее можно получить из решения системы линейных уравнений предыдущего пункта, но мы ее выведем чрезвычайно кратким, но искусственным путем, используя формулу Лагранжа для разложения дроби на простейшие.

Пусть  $\frac{x | x_1 \ x_2 \dots x_n}{y | y_1 \ y_2 \dots y_n}$  — данная таблица значений,  $x_i \neq x_j$  и  $f(x)$  — интерполяционный полином наименьшей степени. Обозначим  $F(x) = (x-x_1)(x-x_2)\dots(x-x_n)$  и рассмотрим рациональную дробь  $\frac{f(x)}{F(x)}$ . Она правильная, ибо степень числителя меньше  $n$ , и мы можем применить формулу Лагранжа для разложения дроби на простейшие. Получим

$$\frac{f(x)}{F(x)} = \sum_{k=1}^n \frac{f(x_k)}{F'(x_k)(x-x_k)}.$$

В правой части равенства все известно, ибо  $f(x_k) = y_k$ . Умножив на  $F(x)$ , получим искомую формулу:

$$f(x) = \sum_{k=1}^n \frac{f(x_k)}{F'(x_k)} \cdot \frac{F(x)}{x-x_k}.$$

Эта формула очень удобна для теоретических исследований, но не удобна для практического вычисления интерполяционного полинома.

Например, для функции, заданной таблицей

$$\frac{x | 1 \ 2 \ 3 \ 4}{y | 2 \ 3 \ 4 \ 5}$$

интерполяционным полиномом является, очевидно,  $x+1$ . По формуле же Лагранжа, исходя из  $F(x) = (x-1)(x-2)(x-3)(x-4)$ , мы придем к тому же результату лишь после некоторых

преобразований:

$$\begin{aligned} f(x) &= \frac{2}{-6}(x-2)(x-3)(x-4) + \frac{3}{2}(x-1)(x-3)(x-4) + \\ &+ \frac{4}{-2}(x-1)(x-2)(x-4) + \frac{5}{6}(x-1)(x-2)(x-3) = \\ &= -\frac{1}{3}(x^3 - 9x^2 + 26x - 24) + \frac{3}{2}(x^3 - 8x^2 + 19x - 12) - \\ &- 2(x^3 - 7x^2 + 14x - 8) + \frac{5}{6}(x^3 - 6x^2 + 11x - 6) = x + 1. \end{aligned}$$

Обратим внимание еще на одно обстоятельство. Если окажется, что нужно расширить таблицу данных, то построение интерполяционного полинома по формуле Лагранжа заставляет выполнить пересчет с самого начала — изменится полином  $F$  и значения его производных.

Выведем теперь из формулы Лагранжа некоторые интересные и нетривиальные тождества. Пусть, как прежде,  $F(x) = (x-x_1)(x-x_2) \dots (x-x_n)$  при  $x_i \neq x_j$ . Положим  $f(x) = x^s$ , где  $s \leq n-1$ . Получим:

$$x^s = \sum_{k=1}^n \frac{x_k^s}{F'(x_k)} \cdot \frac{F(x)}{x-x_k}.$$

Сравним коэффициенты при  $x^{n-1}$  в обеих частях равенства. Ясно, что  $\frac{F(x)}{x-x_k}$  есть полином степени  $n-1$  со старшим коэффициентом 1. Следовательно,

$$\begin{aligned} \sum_{k=1}^n \frac{x_k^s}{F'(x_k)} &= 0 \quad \text{при } s=0, 1, \dots, n-2, \\ \sum_{k=1}^n \frac{x_k^{n-1}}{F'(x_k)} &= 1. \end{aligned}$$

**3. Способ интерполяции Ньютона.** Способ основан на последовательном решении интерполяционных задач:

$$\frac{x|x_1}{y|y_1}, \quad \frac{x|x_1 \ x_2}{y|y_1 \ y_2}, \quad \dots, \quad \frac{x|x_1 \ x_2 \dots x_n}{y|y_1 \ y_2 \dots y_n}.$$

Интерполяционные полиномы для этих задач обозначим через  $f_1, f_2, \dots, f_n$ . Решением первой задачи является, очевидно, константа  $f_1 = y_1$ . Сравним решения двух соседних задач  $f_{k-1}$  и  $f_k$ . Разность  $f_k - f_{k-1}$  полиномов  $f_k$  и  $f_{k-1}$  обращается в 0 при  $x = x_1, x = x_2, \dots, x = x_{k-1}$  и, следовательно, делится на  $(x-x_1)(x-x_2) \dots (x-x_{k-1})$ . Степень  $f_k - f_{k-1}$  не превосходит  $k-1$ . Поэтому частное есть константа, т. е.

$$f_k - f_{k-1} = A_k(x-x_1)(x-x_2) \dots (x-x_{k-1}).$$

Положим в этом равенстве  $x = x_k$ . Получим

$$y_k - f_{k-1}(x_k) = A_k(x_k - x_1)(x_k - x_2) \dots (x_k - x_{k-1}),$$

откуда

$$A_k = \frac{y_k - f_{k-1}(x_k)}{(x_k - x_1)(x_k - x_2) \dots (x_k - x_{k-1})}.$$

Следовательно, решение последней интерполяционной задачи есть

$$f = f_n = A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + \dots \\ \dots + A_n(x - x_1)(x - x_2) \dots (x - x_{n-1}),$$

где коэффициенты  $A_k$  вычисляются последовательно по выведенным выше формулам.

Для коэффициентов можно дать довольно громоздкие выражения непосредственно через данные задачи, в форме так называемых разделенных разностей. Мы не будем на этом останавливаться.

При фактическом вычислении интерполяционного полинома целесообразно записать его в форме

$$A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + \dots \\ \dots + A_n(x - x_1)(x - x_2) \dots (x - x_{n-1})$$

с неопределенными коэффициентами и затем находить их, последовательно полагая  $x = x_1, x = x_2, \dots, x = x_n$ .

Например, для рассмотренной выше таблицы

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ \hline y & 2 & 3 & 4 & 5 \end{array}$$

запишем

$$f = A_1 + A_2(x - 1) + A_3(x - 1)(x - 2) + A_4(x - 1)(x - 2)(x - 3).$$

Получим

$$\begin{array}{ll} \text{при } x = 1: & 2 = A_1; \\ \text{при } x = 2: & 3 = 2 + A_2, \quad A_2 = 1; \\ \text{при } x = 3: & 4 = 2 + 1 \cdot 2 + 2A_3, \quad A_3 = 0; \\ \text{при } x = 4: & 5 = 2 + 1 \cdot 3 + 6A_4, \quad A_4 = 0. \end{array}$$

Итак,  $f(x) = 2 + (x - 1) = x + 1$ .

**4. Приближенная интерполяция.** Задача о приближенном интерполировании особенно существенна при обработке экспериментальных данных. Их, как правило, нельзя считать абсолютно точными, и строить точный интерполяционный полином не имеет смысла. Часто оказывается целесообразным выбирать полином возможно более низкой степени так, чтобы он удовлетворял поставленным требованиям приближенно, но наилучшим образом в том или ином смысле. Степень полинома обычно подсказывается условиями задачи, требующей интерполяции.

Итак, пусть дана таблица данных

$$\begin{array}{c|cccc} x & x_1 & x_2 & \dots & x_n \\ y & y_1 & y_2 & \dots & y_n \end{array}$$

и требуется найти полином  $f(x)$  степени  $m < n - 1$ , приближенно принимающий данные значения. Числа  $y_k - f(x_k)$  носят название *невязок*, они в совокупности должны быть малы. Основные критерии этой «совокупной малости» следующие.

I. Требуется подобрать  $f(x)$  так, чтобы наибольшая по модулю невязка была возможно меньше.

II. Требуется подобрать  $f(x)$  так, чтобы сумма модулей невязок была возможно меньше.

III. Требуется подобрать  $f(x)$  так, чтобы сумма квадратов невязок была возможно меньше.

Решение задачи по первым двум критериям непросто и приводится к довольно сложным экстремальным задачам. Гораздо проще решение задачи по третьему критерию. Оказывается также, что этот критерий наиболее приемлем с точки зрения теории вероятностей.

Рассмотрим задачу подробнее.

Речь идет об отыскании коэффициентов  $a_0, a_1, \dots, a_m$  полинома  $f(x) = a_0 + a_1x + \dots + a_mx^m$ , обеспечивающих минимум выражения

$$\sum_{k=1}^n (y_k - a_0 - a_1x_k - \dots - a_mx_k^m)^2.$$

Это выражение есть полином второй степени относительно неизвестных  $a_0, a_1, \dots, a_m$ . Абсолютный минимум (как функции  $m+1$  переменных) будет также минимумом этого выражения, рассматриваемого как функция одного из коэффициентов при фиксированных остальных. Поэтому все частные производные по  $a_0, a_1, \dots, a_m$  в точке минимума равны нулю. Приравнявая их нулю, получим систему линейных уравнений. Оказывается, что эта система имеет единственное решение, и оно действительно дает минимум.

Рассмотрим, например, таблицу

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ y & 1,5 & 1,2 & 0,8 & 0,5 \end{array}$$

Мы видим, что  $y$  — почти линейная функция от  $x$  в пределах табличных значений, так что ищем решения в виде полинома первой степени  $f(x) = ax + b$ .

Сумма квадратов невязок равна:

$$\Phi = (a + b - 1,5)^2 + (2a + b - 1,2)^2 + (3a + b - 0,8)^2 + (4a + b - 0,5)^2.$$

Вычисляем производные по  $a$  и по  $b$ :

$$\frac{1}{2} \frac{\partial \Phi}{\partial a} = (a + b - 1,5) + 2(2a + b - 1,2) + 3(3a + b - 0,8) + \\ + 4(4a + b - 0,5) = 30a + 10b - 8,3;$$

$$\frac{1}{2} \frac{\partial \Phi}{\partial b} = (a + b - 1,5) + (2a + b - 1,2) + (3a + b - 0,8) + \\ + (4a + b - 0,5) = 10a + 4b - 4,0.$$

Решаем систему уравнений:

$$30a + 10b - 8,3 = 0,$$

$$10a + 4b - 4,0 = 0.$$

Получаем:  $a = -0,34$ ,  $b = 1,85$ , так что решением задачи является  $f(x) = -0,34x + 1,85$ .

Сравним значения этого полинома с данными задачи:

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ \hline y & 1,51 & 1,17 & 0,83 & 0,49 \end{array}$$

Максимальный модуль невязки равен 0,03. Если значения для  $y$  измерялись с точностью до 0,05, то построенный полином дает вполне удовлетворительную точность.

## СРАВНЕНИЯ В КОЛЬЦЕ ПОЛИНОМОВ И РАСШИРЕНИЯ ПОЛЕЙ

### § 1. Сравнения в кольце полиномов над полем

**1. Кольцо вычетов по полиному.** Рассматривается кольцо полиномов  $K[x]$  над полем  $K$ . Пусть  $f$  — данный полином. Два полинома  $g_1$  и  $g_2 \in K[x]$  называются *сравнимыми* по модулю  $f$ , если их разность  $g_1 - g_2$  делится на  $f$ . Сравнение обозначается так:  $g_1 \equiv g_2 \pmod{f}$ . Справедливы следующие предложения:

Предложение 1. Если  $g_1 \equiv g_3 \pmod{f}$  и  $g_2 \equiv g_4 \pmod{f}$ , то  $g_1 \pm g_2 \equiv g_3 \pm g_4 \pmod{f}$ .

Предложение 2. Если  $g_1 \equiv g_3 \pmod{f}$  и  $g_2 \equiv g_4 \pmod{f}$ , то  $g_1 g_2 \equiv g_3 g_4 \pmod{f}$ .

Доказательство ничем не отличается от доказательств аналогичных предложений теории сравнений в кольце целых чисел (предложения 3 и 4 § 2 гл. I).

Попарно сравнимые полиномы объединяются в классы. Для классов естественным образом определяются действия сложения и умножения: именно, суммой и произведением классов называется класс, содержащий сумму и произведения каких-либо полиномов из этих классов. Корректность этих определений обеспечивается предложениями 1 и 2. По отношению к этим действиям классы образуют кольцо, коммутативное и ассоциативное. Нулем в этом кольце является класс полиномов, сравнимых с нулем, т. е. делящихся на  $f$ . Единицей является класс, содержащий «полином» 1, т. е. множество полиномов, которые становятся делящимися на  $f$  после вычитания 1.

Все полиномы одного класса по модулю  $f$  имеют один и тот же н. о. д. с  $f$ . Действительно, если  $g_1 = g_2 + qf$ , то всякий общий делитель  $g_2$  и  $f$  делит  $g_1$  и всякий общий делитель  $g_1$  и  $f$  делит  $g_2$ . Класс называется *примитивным*, если входящие в него полиномы взаимно просты с модулем. Класс называется *обратимым*, если для него существует обратный, т. е. такой, произведение которого с данным равно единичному.

Предложение 3. Обратимыми являются примитивные классы и только они.

Доказательство. Пусть  $g$  принадлежит примитивному классу, так что  $(g, f) = 1$ . Тогда найдутся полиномы  $M, N$  из кольца  $K[x]$  такие, что  $gM + fN = 1$ . Ясно, что  $gM \equiv 1 \pmod{f}$ , так что  $M$  принадлежит классу, обратному к классу, содержащему  $g$ .

Пусть теперь класс, содержащий  $g$ , обратим. Это значит, что для полинома  $g$  найдется такой полином  $M$ , что  $gM \equiv 1 \pmod{f}$ . Обозначив через  $N$  частное от деления  $1 - gM$  на  $f$ , получим  $gM + fN = 1$ , а это и означает, что  $g$  и  $f$  взаимно просты.

Из доказанного предложения немедленно следует

**Предложение 4.** *Кольцо вычетов по модулю неприводимого полинома есть поле.*

Действительно, в этом случае все классы, кроме нулевого, обратимы.

Если же полином  $f$  приводим, то кольцо вычетов по модулю  $f$  не только не поле, но даже не область целостности. Действительно, пусть  $f = f_1 f_2$ , где  $f_1, f_2 \in K[x]$  отличны от констант. Тогда содержащие  $f_1$  и  $f_2$  классы отличны от нулевого, но их произведение есть нулевой класс.

**2. Значения рациональных дробей.** Пусть  $K(x)$  — поле рациональных дробей от буквы  $x$  над полем  $K$ ,  $\mathfrak{K}$  — какое-либо расширение поля  $K$ . Пусть  $\alpha \in \mathfrak{K}$ . Если для дроби  $\frac{f}{g}$  элемент  $\alpha$  является корнем для знаменателя и не является корнем числителя, говорят, что  $\frac{f}{g}$  имеет *полюс* в точке  $\alpha$ . Если  $g(\alpha) \neq 0$ , то имеет смысл значение  $\frac{f(\alpha)}{g(\alpha)}$  дроби. Если числитель и знаменатель умножить на один и тот же полином, не обращающийся в нуль при  $\alpha$ , то значение дроби, очевидно, не меняется. Следовательно, оно не меняется и при сокращении. Если дробь несократима, т. е. если ее числитель и знаменатель взаимно просты, то они не могут обращаться в нуль одновременно, так что если  $\alpha$  не является полюсом дроби, то имеется ее значение в  $\alpha$ , которое принимается за значение дроби независимо от ее записи. Так, дробь  $\frac{x-2}{x^2-4}$  имеет значение при  $x=2$ , хотя знаменатель и обращается в 0 в этой точке, именно, это значение равно  $\frac{1}{4}$ , ибо  $\frac{x-2}{x^2-4} = \frac{1}{x+2}$ .

## § 2. Расширение полей

**1. Простое расширение поля.** Пусть дано поле  $K$ , содержащее его поле  $\mathfrak{K}$ , и  $\alpha \in \mathfrak{K}$ . Рациональные дроби поля  $K(x)$ , не имеющие  $\alpha$  полюсом, имеют значения в  $\alpha$ , принадлежащие полю  $\mathfrak{K}$ . Множество значений  $\frac{f(\alpha)}{g(\alpha)}$  всех дробей  $\frac{f}{g} \in K(x)$  образует, очевидно, поле. Действительно, если  $\alpha$  не является полюсом для  $\frac{f_1}{g_1}$  и для  $\frac{f_2}{g_2}$ , то  $\alpha$  не будет полюсом для их суммы, разности и произведения, так что если значения  $\frac{f_1}{g_1}$  и  $\frac{f_2}{g_2}$  в  $\alpha$  имеют смысл, то имеет

смысл значение в  $\alpha$  для их суммы, разности и произведения. Далее, если  $\frac{f(\alpha)}{g(\alpha)} \neq 0$ , то  $f(\alpha) \neq 0$ , так что дробь  $\frac{g}{f}$  не имеет  $\alpha$  полюсом и имеет значение в  $\alpha$ . Ясно, что  $\frac{g(\alpha)}{f(\alpha)} = \left(\frac{f(\alpha)}{g(\alpha)}\right)^{-1}$ . Так построенное поле обозначается через  $K(\alpha)$  и называется *простым расширением* поля  $K$  посредством присоединения  $\alpha$ .

Элемент  $\alpha \in \mathfrak{R}$  называется *трансцендентным* относительно поля  $K$ , если он не является корнем какого-либо ненулевого полинома с коэффициентами из  $K$ . Если же  $\alpha$  является корнем некоторого полинома из  $K[x]$ , то  $\alpha$  называется *алгебраическим* относительно  $K$ . Алгебраический элемент  $\alpha$  является корнем однозначно определенного неприводимого полинома  $\varphi \in K[x]$ . Действительно, если  $f(\alpha) = 0$  при некотором  $f \in K[x]$  и  $f = \varphi_1 \varphi_2 \dots \varphi_m$  — разложение  $f$  на неприводимые над  $K$  множители (допускаются равные множители), то  $\varphi_1(\alpha) \varphi_2(\alpha) \dots \varphi_m(\alpha) = 0$ , и, так как все  $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$  принадлежат полю  $\mathfrak{R}$ , должен равняться нулю один из сомножителей  $\varphi_i$ . Если два нормализованных неприводимых полинома имеют корнем  $\alpha$ , то они не взаимно просты и, следовательно, совпадают.

Числа, трансцендентные и алгебраические над полем  $\mathbb{Q}$  рациональных чисел, носят названия, соответственно, *трансцендентных* и *алгебраических* чисел. Так, числа  $i$ ,  $\sqrt{2}$ ,  $\sqrt[5]{3}$  алгебраические, в то время, как числа  $e$ ,  $\pi$ ,  $2^{\sqrt{2}}$  трансцендентные, что доказано в работах выдающихся ученых 19-го и 20-го веков.

Простые расширения, получающиеся посредством присоединения трансцендентного элемента, называются *простыми трансцендентными расширениями*, расширения же посредством алгебраического элемента называются *простыми алгебраическими расширениями*. Рассмотрим подробнее строение простых трансцендентных и алгебраических расширений.

Если  $\alpha \in \mathfrak{R}$  трансцендентен относительно  $K$ , то  $\alpha$  не может быть полюсом ни одной из дробей поля  $K(x)$ , ибо не может быть корнем полинома, находящегося в знаменателе. Поэтому каждая дробь  $\frac{f}{g}$  имеет значение  $\frac{f(\alpha)}{g(\alpha)}$ . Разные дроби имеют разные значения. Действительно, если  $\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)}$ , то  $f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) = 0$ , откуда следует, что полином  $f_1g_2 - f_2g_1$  равен нулю в силу трансцендентности  $\alpha$ , так что дроби  $\frac{f_1}{g_1}$  и  $\frac{f_2}{g_2}$  равны.

Итак, между дробями поля  $K(x)$  и их значениями в  $\alpha$  имеется взаимно однозначное соответствие, которое, очевидно, сохраняется при действиях сложения и умножения. Таким образом, поле  $K(x)$  и поле  $K(\alpha)$  изоморфны. Тем самым мы установили, что все простые трансцендентные расширения изоморфны между собой, ибо

они все изоморфны полю дробей  $K(x)$ . Разумеется, само поле  $K(x)$  тоже является простым трансцендентным расширением поля  $K$ , ибо  $x$  не является корнем полинома с коэффициентами из  $K$  (в качестве объемлющего поля  $\mathbb{R}$ , содержащего поле  $K$  и  $x$ , можно взять само  $K(x)$ ).

Пусть теперь  $\alpha \in \mathbb{R}$  алгебраично над  $K$  и  $\varphi \in K[x]$  — неприводимый над  $K$  полином, корнем которого является  $\alpha$ . Пусть, далее,  $\frac{f}{g} \in K(x)$  — несократимая дробь, для которой  $\alpha$  не является полюсом, т. е.  $g(\alpha) \neq 0$ . Это значит, что полином  $g$  взаимно прост с неприводимым над  $K$  полиномом  $\varphi$ . Поэтому существуют полиномы  $M, N \in K[x]$  такие, что  $gM + \varphi N = 1$ . Переходя к значениям при  $\alpha$ , получим  $g(\alpha)M(\alpha) = 1$ , так что  $\frac{1}{g(\alpha)} = M(\alpha)$  и  $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)M(\alpha)$ .

Таким образом, значение дроби  $\frac{f}{g}$  оказывается равным значению полинома  $fM$ . Далее, полиномы из  $K[x]$  имеют одинаковые значения в  $\alpha$  в том и только в том случае, когда они сравнимы по модулю  $\varphi$ . Действительно, если  $f_1 \equiv f_2 \pmod{\varphi}$ , то  $f_1 - f_2 = \varphi q$  и  $f_1(\alpha) - f_2(\alpha) = \varphi(\alpha)q(\alpha) = 0$ . Обратно, если  $f_1(\alpha) = f_2(\alpha)$ , то полином  $f_1 - f_2 \in K[x]$  имеет общий корень с неприводимым над  $K$  полиномом  $\varphi$  и, следовательно, делится на него, т. е.  $f_1 \equiv f_2 \pmod{\varphi}$ . Итак, мы получили взаимно однозначное соответствие между классами по модулю  $\varphi$  и значениями полиномов  $F \in K[x]$  в точке  $\alpha$ . Ясно, что это соответствие сохраняется при сложении и при умножении. Таким образом, алгебраическое расширение  $K(\alpha)$  оказывается изоморфным полю вычетов кольца  $K[x]$  по модулю неприводимого полинома  $\varphi$ , корнем которого является  $\alpha$ .

Таким образом, это поле вычетов оказывается абстрактной изоморфной моделью, не зависящей ни от того поля  $\mathbb{R}$ , из которого взят  $\alpha$ , ни от выбора корня полинома  $\varphi$ . Так, например, полином  $x^3 - 3$ , неприводимый над полем рациональных чисел (если бы был приводим, то имел бы рациональный линейный множитель и рациональный корень), имеет в поле  $\mathbb{C}$  комплексных чисел три корня  $\alpha_1 = \sqrt[3]{3}$ ,  $\alpha_2 = \sqrt[3]{3}\rho$  и  $\alpha_3 = \sqrt[3]{3}\rho^2$ , где  $\rho = e^{2\pi i/3}$ , но все три поля  $\mathbb{Q}(\sqrt[3]{3})$ ,  $\mathbb{Q}(\sqrt[3]{3}\rho)$  и  $\mathbb{Q}(\sqrt[3]{3}\rho^2)$  изоморфны полю вычетов кольца  $\mathbb{Q}[x]$  по модулю полинома  $x^3 - 3$  и, следовательно, изоморфны между собой, хотя множества чисел, их составляющих, различны. Так, поле  $\mathbb{Q}(\sqrt[3]{3})$  состоит только из вещественных чисел, а элементами поля  $\mathbb{Q}(\sqrt[3]{3}\rho)$ , кроме элементов  $\mathbb{Q}$ , являются комплексные числа с отличной от нуля мнимой частью.

Заметим еще, что поле  $\mathbb{C}$  комплексных чисел получается из поля  $\mathbb{R}$  вещественных чисел присоединением корня неприводимого над  $\mathbb{R}$  полинома  $x^2 + 1$ . Поэтому оно изоморфно полю вычетов кольца  $\mathbb{R}[x]$  по модулю полинома  $x^2 + 1$ . Это дает один из способов обоснования понятия комплексного числа. (Комплексными числами называются классы вычетов кольца  $\mathbb{R}[x]$  по полиному

$x^2 + 1$ . Обозначив класс, содержащий  $x$ , через  $i$ , получим, что все комплексные числа имеют вид  $a + bi$  при  $a, b \in \mathbb{R}$ . Так как  $x^2 \equiv -1 \pmod{x^2 + 1}$ , то  $i^2 = -1$  и т. д.).

Вычисление, посредством которого значение дроби  $\frac{f}{g}$  на алгебраическом элементе преобразуется в значение полинома, называется исключением иррациональности в знаменателе.

**Пример.** Исключить иррациональность в знаменателе выражения  $\frac{\alpha + 1}{\alpha^2 + \alpha + 1}$ , где  $\alpha$  — корень полинома  $x^3 - x - 1$ .

Мы знаем, что результат может быть единственным образом представлен в виде  $A\alpha^2 + B\alpha + C$ . Записав равенство  $\frac{\alpha + 1}{\alpha^2 + \alpha + 1} = A\alpha^2 + B\alpha + C$ , получим, что  $\alpha + 1 = (A\alpha^2 + B\alpha + C)(\alpha^2 + \alpha + 1) = A\alpha^4 + (A + B)\alpha^3 + (A + B + C)\alpha^2 + (B + C)\alpha + C$ .

Далее,  $\alpha^3 = \alpha + 1$  и  $\alpha^4 = \alpha^2 + \alpha$ . Поэтому

$$\alpha + 1 = A(\alpha^2 + \alpha) + (A + B)(\alpha + 1) + (A + B + C)\alpha^2 + (B + C)\alpha + C.$$

В силу однозначности записи в виде полинома от  $\alpha$  не выше второй степени, получаем

$$2A + B + C = 0,$$

$$2A + 2B + C = 1,$$

$$A + B + C = 1.$$

Получилась система трех линейных уравнений с тремя неизвестными, и мы знаем заранее, что она имеет единственное решение. Мы легко его найдем:  $A = -1$ ,  $B = 1$ ,  $C = 1$ . Итак,

$$\frac{\alpha + 1}{\alpha^2 + \alpha + 1} = -\alpha^2 + \alpha + 1.$$

**2. Конструирование простых расширений.** Результаты п. 1 показывают, что с точностью до изоморфизма можно конструировать простые расширения поля  $K$ , не обращаясь к рассмотрению поля  $\mathbb{R}$ , из которого берутся присоединяемые элементы. Так, простое трансцендентное расширение есть поле рациональных дробей  $K(x)$  от некоторой буквы. Простое трансцендентное расширение поля  $K(x)$  есть поле рациональных дробей от буквы  $y$  с коэффициентами из  $K(x)$ . Каждую такую дробь посредством умножения на произведения всех знаменателей коэффициентов при  $y$  можно привести к виду  $\frac{F(x, y)}{G(x, y)}$  частного двух полиномов от  $x$  и  $y$ , так что двукратное трансцендентное расширение приводит к полю частных кольца полиномов от двух букв, и т. д.

Алгебраические же расширения можно конструировать как поля вычетов кольца полиномов по неприводимым полиномам.

Рассмотрим еще один пример. Мы выяснили раньше, что над полем из двух элементов имеется один неприводимый полином  $x^2 + x + 1$  второй степени.

Поле вычетов по нему состоит из четырех элементов  $0, 1, \rho, \rho + 1$ , где через  $\rho$  обозначен класс, содержащий  $x$ . Сложение в этом поле совершается естественным образом, только характеристика поля равна 2, так что сложение каждого элемента с собой дает 0. Умножение же характеризуется тем, что  $\rho^2 + \rho + 1 = 0$ , т. е.  $\rho^2 = \rho + 1$ .

Как уже говорилось выше, над полем вычетов  $GF(p)$  по простому модулю  $p$  существуют неприводимые полиномы любой степени. Поле вычетов по модулю неприводимого полинома степени  $n$  имеет  $p^n$  элементов, ибо каждый элемент такого поля можно однозначно записать в виде полинома степени  $n - 1$  или ниже, и для коэффициентов таких полиномов имеется ровно  $p^n$  возможностей. Оказывается, что все такие поля изоморфны, так что различные неприводимые полиномы степени  $n$  приводят к изоморфным полям вычетов. Так построенные поля из  $p^n$  элементов носят название *полей Галуа* и обозначаются  $GF(p^n)$ . Доказывается, что никаких других полей из конечного числа элементов не существует,

# ПОЛИНОМЫ С ЦЕЛЫМИ КОЭФФИЦИЕНТАМИ. ПОЛИНОМЫ НАД ФАКТОРИАЛЬНЫМИ КОЛЬЦАМИ

## § 1. Полиномы с целыми коэффициентами

Полиномы с рациональными коэффициентами и полиномы с целыми коэффициентами тесно связаны между собой, ибо каждый полином с рациональными коэффициентами может быть превращен в полином с целыми коэффициентами посредством умножения на общий знаменатель коэффициентов. Изучение кольца  $\mathbb{Z}[x]$  полиномов с целыми коэффициентами интересно также потому, что  $\mathbb{Z}[x]$  есть простейший пример кольца полиномов над факториальным кольцом.

### 1. Рациональные корни полиномов с целыми коэффициентами.

**Теорема 1.** Если несократимая дробь  $\frac{p}{q}$  является корнем полинома  $a_0x^n + a_1x^{n-1} + \dots + a_n$ ,  $a_n \neq 0$ , с целыми коэффициентами, то ее числитель является делителем свободного члена, а знаменатель  $q$  — делителем старшего коэффициента.

**Доказательство.** Пусть  $a_0\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + \dots + a_{n-1}\frac{p}{q} + a_n = 0$ . Тогда  $a_0p^n + a_1p^{n-1}q + \dots + a_{n-1}pq^{n-1} + a_nq^n = 0$  и  $a_nq^n = p(-a_0p^{n-1} - a_1p^{n-2}q - \dots - a_{n-1}q^{n-1})$ . Таким образом, число  $a_nq^n$  делится на  $p$  в кольце целых чисел. По условию  $q$  и  $p$  взаимно просты, следовательно,  $a_n$  делится на  $p$ . Аналогично, из равенства

$$a_0p^n = q(-a_1p^{n-1} - \dots - a_{n-1}pq^{n-2} - a_nq^{n-1})$$

заключаем, что  $a_0$  делится на  $q$ .

Доказанная теорема дает возможность найти рациональные корни полинома с целыми (следовательно, и с рациональными) коэффициентами в конечном числе действий. Именно, нужно найти все делители свободного члена и все делители старшего коэффициента, составить из них несократимые дроби и испытать посредством подстановки в полином. Если во всех случаях испытание даст отрицательный результат, то это значит, что полином не имеет рациональных корней. Сделанное в теореме предположение о неравенстве нулю свободного члена не ограничивает общности: если свободный член и, быть может, еще несколько младших коэффициентов обращаются в 0, то можно вынести из полинома надлежащую степень  $x$  так, чтобы после вынесения остался поли-

ном с отличным от нуля свободным членом. Этот полином будет иметь те же ненулевые корни, что и исходный.

Отметим следующее следствие. Если  $a_0 = 1$ , то все рациональные корни полинома являются целыми числами, именно, делителями свободного члена.

**Пример.**  $3x^2 - 10x + 3$ . Кандидатами в корни, согласно теореме, являются числа 1, -1, 3, -3,  $1/3$ ,  $-1/3$ . Подстановка в полином дает, что корнями являются 3 и  $1/3$ .

**2. Редукция полиномов с целыми коэффициентами по числовому модулю.** Пусть  $m$  — целое положительное число. Два полинома  $f_1(x)$  и  $f_2(x)$  называются *сравнимыми* по модулю  $m$ , если все коэффициенты их разности делятся на  $m$ . Полиномы разбиваются на классы сравнимых по модулю  $m$ . Все коэффициенты полиномов из одного класса определены с точностью до целых кратных  $m$ , т. е. класс естественно отождествляется с полиномом, коэффициенты которого принадлежат кольцу вычетов  $\mathbb{Z}/m\mathbb{Z}$ . Совершенно ясно, что если  $f_1 \equiv f_2 \pmod{m}$  и  $f_3 \equiv f_4 \pmod{m}$ , то  $f_1 \pm f_3 \equiv f_2 \pm f_4 \pmod{m}$  и  $f_1 f_3 \equiv f_2 f_4 \pmod{m}$ . Поэтому для классов по модулю  $m$  естественным образом определяются сложение и умножение, и эти действия совпадают с действиями сложения и умножения полиномов с коэффициентами из кольца вычетов  $\mathbb{Z}/m\mathbb{Z}$ .

Особый интерес представляет редукция по простому модулю, так как в результате редукции получаются полиномы над полем  $\text{GF}(p)$ , и их множество образует область целостности.

Полином из  $\mathbb{Z}[x]$  называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1. Так, полином  $3x^3 - 10x + 6$  примитивен, а  $2x^3 - 10x + 6$  не примитивен.

**Предложение 2 (лемма Гаусса).** *Произведение двух примитивных полиномов есть примитивный полином.*

**Доказательство.** Пусть  $f_1$  и  $f_2 \in \mathbb{Z}[x]$  — примитивные полиномы. Допустим, что их произведение  $f_1 f_2$  не примитивно. Обозначим через  $p$  какой-либо простой делитель наибольшего общего делителя коэффициентов  $f_1 f_2$ . Тогда  $\bar{f}_1 \bar{f}_2 = \bar{f}_1 \bar{f}_2 = \bar{0}$  (черточка обозначает результат редукции). Так как кольцо полиномов над полем  $\text{GF}(p)$  есть область целостности, один из сомножителей должен равняться нулю, а это значит, что все коэффициенты  $f_1$  или  $f_2$  делятся на  $p$ , что противоречит предположению о примитивности.

### 3. Теорема Гаусса и факториальность кольца $\mathbb{Z}[x]$ .

**Предложение 3.** *Пусть  $f = a_0 x^n + a_1 x^{n-1} + \dots + a_n$  — примитивный полином,  $b$  — рациональное число такое, что  $bf$  имеет целые коэффициенты. Тогда  $b$  — целое число.*

**Доказательство.** Пусть  $b = \frac{c}{d}$  — несократимая дробь. По условию, все числа  $ba_i = \frac{ca_i}{d}$  целые,  $i = 0, \dots, n$ .

Числа  $s$  и  $d$  взаимно просты, следовательно, все  $a_i$  делятся на  $d$ , что возможно только при  $d = 1$ , в силу примитивности  $f$ .

**Теорема 4 (теорема Гаусса).** *Если полином с целыми коэффициентами раскладывается на два множителя над полем рациональных чисел, то он может быть разложен на множители с целыми коэффициентами, именно, представлен в виде произведения целого числа на произведение примитивных полиномов.*

Отсюда следует, что если полином с целыми коэффициентами приводим над полем рациональных чисел, то он приводим и над полем целых чисел.

**Доказательство.** Пусть  $f \in \mathbb{Z}[x]$  и  $f = f_1 f_2$ , где  $f_1$  и  $f_2$  — полиномы с рациональными, быть может дробными, коэффициентами. Обозначим через  $N_1$  и  $N_2$  общие знаменатели коэффициентов полиномов  $f_1$  и  $f_2$ . Тогда  $f_1 = \frac{1}{N_1} \tilde{f}_1$ ,  $f_2 = \frac{1}{N_2} \tilde{f}_2$ , где  $\tilde{f}_1$  и  $\tilde{f}_2$  имеют уже целые коэффициенты. Пусть  $M_1$  и  $M_2$  — наибольшие общие делители коэффициентов полиномов  $\tilde{f}_1$  и  $\tilde{f}_2$  соответственно. Тогда  $\tilde{f}_1 = M_1 \tilde{\tilde{f}}_1$  и  $\tilde{f}_2 = M_2 \tilde{\tilde{f}}_2$ , где  $\tilde{\tilde{f}}_1$  и  $\tilde{\tilde{f}}_2$  — уже примитивные полиномы. Тогда

$$f = f_1 f_2 = \frac{M_1 M_2}{N_1 N_2} \tilde{\tilde{f}}_1 \tilde{\tilde{f}}_2.$$

По лемме Гаусса  $\tilde{\tilde{f}}_1 \tilde{\tilde{f}}_2$  есть примитивный полином и, согласно предложению 3, рациональное число  $b = \frac{M_1 M_2}{N_1 N_2}$  в действительности целое. Итак,  $f = b \tilde{\tilde{f}}_1 \tilde{\tilde{f}}_2$ , где  $b$  — целое число,  $\tilde{\tilde{f}}_1$  и  $\tilde{\tilde{f}}_2$  — примитивные полиномы. Теорема доказана.

Очевидно, что результат остается верным, если  $f$  есть произведение нескольких полиномов с рациональными коэффициентами, именно, после вынесения общих знаменателей коэффициентов и наибольших общих делителей коэффициентов получившихся полиномов мы получим, что  $f$  есть произведение целого числа на произведение примитивных полиномов, отличающихся от полиномов исходного разложения лишь числовыми множителями. Очевидно, что примитивные полиномы могут быть ассоциированы, только если они совпадают или отличаются множителем  $-1$ .

**Теорема 5.** *Любой полином с целыми коэффициентами может быть представлен в виде произведения простых чисел и неприводимых над  $\mathbb{Q}$  примитивных полиномов. Такое разложение единственно с точностью до порядка следования сомножителей и присоединения к сомножителям множителя  $-1$ .*

Действительно, от разложения  $f = \varphi_1 \varphi_2 \dots \varphi_k$  полинома  $f \in \mathbb{Z}[x]$  на неприводимые множители над  $\mathbb{Q}$  мы можем, в силу теоремы Гаусса, перейти к разложению  $f = b \psi_1 \psi_2 \dots \psi_k$ , где  $b$  — целое число, а примитивные полиномы  $\psi_1, \psi_2, \dots, \psi_k$  отличаются от полиномов  $\varphi_1, \varphi_2, \dots, \varphi_k$  лишь числовыми множителями. Тем самым сомножители  $\psi_1, \psi_2, \dots, \psi_k$  определены однозначно, с точ-

ностью до порядка следования сомножителей (который совпадает с порядком следования  $\varphi_1, \varphi_2, \dots, \varphi_k$ ) и множителей  $\pm 1$ . В свою очередь, целое число  $b$ , которое равно, в силу леммы Гаусса, наибольшему общему делителю коэффициентов полинома  $f$ , однозначно разлагается на простые множители.

Ясно, что простые числа и примитивные неприводимые полиномы являются неразложимыми элементами кольца  $Z[x]$ . Тем самым доказана

**Теорема 6.** *Кольцо  $Z[x]$  полиномов с целыми коэффициентами факториально.*

**4. Задача о приводимости полинома над полем рациональных чисел.** Поставленную задачу достаточно исследовать для полиномов с целыми коэффициентами, ибо любой полином из  $Q[x]$  ассоциирован с полиномом из  $Z[x]$ . Теорема Гаусса позволяет дать способ разложения полинома с целыми коэффициентами на два множителя или убедиться в его неприводимости над  $Q$ . Способ этот теоретически прост, но практически довольно громоздок. Опишем его.

Пусть дан полином  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ ,  $a_i \in Z$ . Допустим, что он приводим над  $Q$ . Тогда существует, согласно теореме Гаусса, его разложение на два множителя с целыми коэффициентами:  $f = f_1 f_2$ ,  $f_1, f_2 \in Z[x]$ . Сумма степеней  $f_1$  и  $f_2$  равна  $n$ , значит, степень одного из них, положим,  $f_1$ , не превосходит  $k = \lfloor n/2 \rfloor$ . Мы знаем, что полином, степень которого не превосходит  $k$ , вполне определяется, если для него известно  $k+1$  значение, согласно решению задачи об интерполяции. Возьмем  $k+1$  целых значений для  $x$ :

$$x_0, x_1, \dots, x_k, \quad x_i \neq x_j, \quad x_i \in Z.$$

Если произойдет такое счастливое обстоятельство, что одно из выбранных чисел окажется корнем полинома  $f$ , то задача решена,  $f$  приводим, и мы можем написать его разложение на два сомножителя. Положим теперь, что  $f(x_i) \neq 0$  при  $i = 0, 1, \dots, k$ . Из равенств

$$f_1(x_i) f_2(x_i) = f(x_i)$$

заключаем, что числа  $f_1(x_i)$  нам «почти» известны. Действительно,  $f_1(x_i)$  и  $f_2(x_i)$  — целые числа, так что  $f_1(x_i)$  является одним из делителей известного нам числа  $f(x_i)$ . Для  $f_1(x_i)$  имеется конечное число возможностей. Обозначим через  $t_i$  число делителей числа  $f(x_i)$ . Составим таблицы

$$\begin{array}{c|cccc} x & x_0 & x_1 & \dots & x_k \\ y & d_0 & d_1 & \dots & d_k \end{array}$$

расставляя в нижние строки наборы из всевозможных делителей чисел  $f(x_0), f(x_1), \dots, f(x_k)$ . Число таких таблиц конечно и равно  $t_0 t_1 \dots t_k$ , ибо  $i$ -е место в нижней строке можно заполнить  $t_i$  способами. Построим для каждой таблицы интерполяционный поли-

ном. Если  $f$  приводим, то его множитель  $f_1$  найдется среди построенных полиномов. Поэтому, построив интерполяционные полиномы, нужно выбросить те, у которых имеется хотя бы один дробный коэффициент (ибо искомым  $f_1$  имеет целые коэффициенты), а полиномы с целыми коэффициентами испытать посредством деления на них полинома  $f$ . Если испытание в каком-то случае даст положительный результат, то полином  $f$  приводим, и мы нашли его разложение на два множителя. Если же испытание во всех случаях даст отрицательный результат, то полином  $f$  неприводим. Тем самым поставленная задача решена в конечном числе действий.

### 5. Редукционный признак неприводимости полинома.

**Теорема 7.** Пусть  $p$  — простое число,  $f = a_0x^n + \dots + a_n \in \mathbb{Z}[x]$ ,  $a_0 \not\equiv 0 \pmod{p}$  и редукция  $\bar{f}$  полинома  $f$  по модулю  $p$  неприводима. Тогда  $f$  неприводим над  $\mathbb{Q}$ .

**Доказательство.** Если  $f$  приводим над  $\mathbb{Q}$ , то по теореме Гаусса имеет разложение на множители с целыми коэффициентами  $f = f_1 f_2$ , где  $f_1 = b_0x^m + \dots + b_m$  и  $f_2 = c_0x^k + \dots + c_k$ , при  $m \geq 1$  и  $k \geq 1$ . Из  $a_0 = b_0c_0$  и  $\bar{a}_0 \neq \bar{0}$  заключаем, что  $\bar{b}_0 \neq \bar{0}$  и  $\bar{c}_0 \neq \bar{0}$ . Таким образом,  $\bar{f} = \bar{f}_1 \bar{f}_2$ ,  $\bar{f}_1 = \bar{b}_0x^m + \dots + \bar{b}_m$  и  $\bar{f}_2 = \bar{c}_0x^k + \dots + \bar{c}_k$ . Оба полинома  $\bar{f}_1$  и  $\bar{f}_2$  отличны от констант. Мы пришли к противоречию с условием, которое и доказывает теорему.

**Пример.** Легко установить, что полином  $x^4 + x^3 + x^2 + x + 1$  неприводим по модулю 2. Отсюда следует, что любой полином четвертой степени с нечетными коэффициентами неприводим над  $\mathbb{Q}$ .

### 6. Признак неприводимости Эйзенштейна.

**Теорема 8.** Пусть  $p$  — простое число,  $f = a_0x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{Z}[x]$ ,  $a_0 \not\equiv 0 \pmod{p}$ ,  $a_i \equiv 0 \pmod{p}$  при  $i = 1, \dots, n$  и  $a_n \not\equiv 0 \pmod{p^2}$ . Тогда  $f$  неприводим над  $\mathbb{Q}$ .

**Доказательство.** Пусть  $f$  приводим над  $\mathbb{Q}$  и пусть  $f = f_1 f_2$ , где  $f_1 = b_0x^m + \dots + b_m$ ,  $f_2 = c_0x^k + \dots + c_k$ ,  $m \geq 1$ ,  $k \geq 1$ , — разложение  $f$  на множители с целыми коэффициентами, которое существует в силу теоремы Гаусса.

Переходим к редукции по модулю  $p$ . Ясно, что  $\bar{f} = \bar{a}_0x^n$  и  $\bar{f} = \bar{f}_1 \bar{f}_2$ . Одночлен  $x$  неприводим над  $\text{GF}(p)$  и, в силу однозначности канонического разложения над полем, заключаем, что  $\bar{f}_1 = \bar{b}_0x^m$  и  $\bar{f}_2 = \bar{c}_0x^k$ . Поэтому все коэффициенты, кроме старших, полиномов  $f_1$  и  $f_2$  делятся на  $p$ . В частности,  $b_m \equiv 0 \pmod{p}$  и  $c_k \equiv 0 \pmod{p}$ . Следовательно,  $a_n = b_m c_k$  делится на  $p^2$ , что противоречит условию теоремы. Это противоречие доказывает теорему.

**Пример 1.**  $x^n + 2b_1x^{n-1} + \dots + 2b_{n-1}x + 4b_n + 2$  при  $b_1, b_2, \dots, b_n \in \mathbb{Z}$  неприводим над  $\mathbb{Q}$  в силу применимости признака Эйзенштейна для  $p = 2$ .

**Пример 2.**  $f = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + 1$ ,  $p$  — простое число. Здесь признак Эйзенштейна непосредственно не применим.

Рассмотрим полином  $g(y) = f(y+1)$ . Ясно, что полиномы  $f$  и  $g$  приводимы или неприводимы над  $\mathbb{Q}$  одновременно. Имеем:

$$g(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \frac{p(p-1)}{1 \cdot 2} y^{p-3} + \dots \\ \dots + \frac{p(p-1) \dots (p-k+1)}{k!} y^{p-k-1} + \dots + p.$$

Простое  $p$  входит в числитель всех коэффициентов, начиная со второго, и не входит в знаменатель  $k!$ . Поэтому все коэффициенты, начиная со второго, делятся на  $p$ , а свободный член  $p$  не делится на  $p^2$ . По признаку Эйзенштейна полином  $g$ , а вместе с ним и полином  $f$ , неприводим над  $\mathbb{Q}$ .

## § 2. Полиномы от одной буквы над факториальным кольцом

**1. Наибольший общий делитель элементов факториального кольца.** Пусть  $A$  — факториальное кольцо. *Наибольшим общим делителем* двух (или нескольких) элементов  $A$  называется общий делитель, делящийся на любой общий делитель тех же элементов. Докажем, что для любых элементов факториального кольца наибольший общий делитель существует. Доказательство проведем для двух элементов (обобщение на любое конечное множество элементов тривиально). Пусть  $a = e_1 p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$  и  $b = e_2 p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$  — разложение  $a$  и  $b$  на неразложимые множители (здесь  $e_1$  и  $e_2$  — единицы,  $p_1, \dots, p_k$  неразложимы, допускаются нулевые показатели). Тогда любой общий делитель элементов  $a$  и  $b$  содержит каждое  $p_i$  с показателем, не превосходящим как  $m_i$ , так и  $n_i$ . Поэтому  $d = p_1^{\min(m_1, n_1)} p_2^{\min(m_2, n_2)} \dots p_k^{\min(m_k, n_k)}$  будет наибольшим общим делителем.

Заметим, что линейного представления наибольшего общего делителя в факториальном кольце может и не быть. Так, в кольце  $\mathbb{Z}[x]$  элементы 2 и  $x$  неразложимы, их наибольший общий делитель равен 1, но равенство  $1 = 2f + xg$  при  $f, g \in \mathbb{Z}[x]$ , невозможно, ибо полиномы в правой части равенства имеют четный свободный член.

**2. Сравнения в факториальном кольце.** Пусть  $A$  — факториальное кольцо и  $m$  — некоторый его элемент. Элементы  $a, b \in A$  называются *сравнимыми* по модулю  $m$ , что обозначается  $a \equiv b \pmod{m}$ , если их разность  $a - b$  делится на  $m$  в кольце  $A$ . Ясно, что все элементы  $A$  разбиваются на классы попарно сравнимых. Далее, очевидные предложения: если  $a_1 \equiv b_1 \pmod{m}$  и  $a_2 \equiv b_2 \pmod{m}$ , то  $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$  и  $a_1 a_2 \equiv b_1 b_2 \pmod{m}$ , позволяют превратить множество классов в кольцо, при естественном определении действий сложения и умножения. Это кольцо называется *кольцом вычетов* по модулю  $m$  и обозначается  $A/mA$ .

**Предложение 1.** *Кольцо вычетов  $A/pA$  факториального кольца по неразложимому элементу  $p$  есть область целостности.*

**Доказательство.** Пусть  $a, b \in A$  и  $\bar{a}, \bar{b}$  — содержащие их классы по модулю  $p$ . Допустим, что  $\bar{a}\bar{b} = \bar{0}$ . Это означает, что  $ab$  делится на  $p$ . Разложим  $a$  и  $b$  на неразложимые множители. Неразложимый элемент  $p$  должен входить в объединение неразложимых множителей, входящих в  $a$  и  $b$ , в силу однозначности разложения. Следовательно,  $p$  входит в  $a$  или в  $b$ , т. е.  $\bar{a} = 0$  или  $\bar{b} = 0$ .

Заметим, что для колец  $A = \mathbb{Z}$  и  $A = K[x]$  кольцо вычетов было не только областью целостности, но даже полем. Вообще же это не так. Например, для кольца  $A = \mathbb{Z}[x]$  элементы 2 и  $x^2 + 1$  неразложимы.  $A/2A$  есть кольцо полиномов над полем  $\text{GF}(2)$  вычетов по модулю 2,  $A/(x^2 + 1)A$  изоморфно кольцу комплексных чисел с целыми компонентами. В обоих случаях это не поля.

**3. Лемма Гаусса.** Полином из кольца полиномов  $A[x]$  с коэффициентами из факториального кольца  $A$  называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1.

Если  $m \in A$ , то полиномы из  $A[x]$  разбиваются на классы сравнимых по модулю  $m$ , если отнести в один класс те, разность которых имеет коэффициенты, делящиеся на  $m$ . Ясно, что для классов единственным образом определяются сложение и умножение, по отношению к которым классы образуют кольцо, изоморфное кольцу полиномов над кольцом  $A/mA$ .

**Предложение 2 (лемма Гаусса).** *Произведение двух примитивных полиномов из  $A[x]$  есть примитивный полином.*

**Доказательство.** Допустим, что произведение  $f_1 f_2$  двух примитивных полиномов не примитивно. Пусть  $p$  — неразложимый элемент, входящий во все коэффициенты  $f_1 f_2$ . Переходя в кольцо классов вычетов по  $p$  в кольце  $A[x]$ , получим  $\bar{f}_1 \bar{f}_2 = \bar{0}$ . Но это кольцо есть кольцо полиномов над областью целостности  $A/pA$ , и потому само является областью целостности. Поэтому либо  $\bar{f}_1 = 0$ , либо  $\bar{f}_2 = 0$ , что противоречит примитивности  $f_1$  и  $f_2$ .

Ясно, что лемма остается справедливой для произведения любого числа примитивных полиномов.

**4. Факториальность кольца полиномов над факториальным кольцом.** Пусть  $A$  — факториальное кольцо и  $K$  — его поле частных.

**Предложение 3.** *Если  $f \in A[x]$  — примитивный полином и  $c \in K$  такое, что  $cf \in A[x]$ , то  $c \in A$ .*

**Доказательство.** Пусть  $c = \frac{b}{d}$ . Без нарушения общности можно считать, что н.о.д.  $(b, d)$  равен 1, ибо если он отличен от 1, то  $\frac{b}{d}$  можно сократить. Пусть  $f = a_0 x^n + \dots + a_n$ . При любом  $i$   $\frac{a_i b}{d} \in A$ . В силу факториальности  $A$  каждый неразложимый множитель  $d$  входит в  $a_i$ , ибо  $d$  и  $b$  общих неразложимых множителей

не имеют. Следовательно,  $d$  — обратимый элемент кольца  $A$ , иначе  $f$  не был бы примитивен, так что  $c \in A$ .

**Предложение 4** (теорема Гаусса). *Если полином  $f \in A[x]$  приводим над полем  $K$ , то он может быть разложен и над кольцом  $A$ .*

Пусть  $f = f_1 f_2$ , где  $f_1 \in K[x]$  и  $f_2 \in K[x]$ . Запишем  $f_1$  и  $f_2$  в виде  $c_1 g_1$  и  $c_2 g_2$ , где  $c_1, c_2 \in K$ , а  $g_1$  и  $g_2$  — примитивные полиномы в  $A[x]$ . Это всегда можно сделать. Далее,  $f = c_1 c_2 g_1 g_2$ . В силу леммы Гаусса и предложения 3,  $c_1 c_2 \in A$ . Тем самым теорема доказана.

Обратимся теперь к разложению полинома на неразложимые множители. Пусть  $f \in A[x]$  и над полем  $K$  разложение  $f$  на неприводимые множители есть  $f = \varphi_1 \varphi_2 \dots \varphi_k$  (равные или ассоциированные множители допускаются). Каждый  $\varphi_i$  представлен в виде  $c_i \psi_i$ , где  $c_i \in K$ ,  $\psi_i \in A[x]$  примитивен. Тогда  $f = c \psi_1 \psi_2 \dots \psi_k$ , где  $c = c_1 \dots c_k$  и, в силу леммы Гаусса и предложения 3,  $c \in A$ . Сомножители определены однозначно, с точностью до множителей, являющихся единицами кольца  $A$ .

Они неразложимы, ибо неприводимы над  $K$  и примитивны, так что не делятся ни на полиномы из  $A[x]$ , ни на константы из  $A$ . Далее,  $c$  можно разложить на неразложимые в  $A$  множители. Получим

$$f = c_1 c_2 \dots c_l \psi_1 \psi_2 \dots \psi_k.$$

Это разложение на неразложимые множители однозначно.

Тем самым мы доказали факториальность кольца полиномов от одной буквы над факториальным кольцом.

Отсюда немедленно, применением индукции, заключаем, что кольцо полиномов от любого конечного множества букв над факториальным кольцом факториально. В частности, факториальны кольца  $Z[x_1, \dots, x_n]$  и  $K[z_1, \dots, z_n]$  при любом поле  $K$ .

**5. Кольца главных идеалов.** Подмножество  $M$  коммутативного ассоциативного кольца  $A$  называется *идеалом* этого кольца, если оно образует группу относительно сложения и допускает умножение на любой элемент из  $A$ . Иными словами, если  $b_1, b_2 \in M$  и  $a \in A$ , то  $b_1 \pm b_2 \in M$  и  $ab_1 \in M$ .

(Заметим, что понятие идеала естественно распространяется на любые кольца, только в случае некоммутативности, идеалы разбиваются на три сорта — правые, левые и двусторонние, в зависимости от того, какие умножения на элементы из  $A$  допускаются.) Ясно, что если  $m \in A$ , то множество  $mA$  всех кратных  $m$  элемента  $m$  образует идеал. Такой идеал носит название *главного идеала*, порожденного элементом  $m$ .

Кольцо называется *кольцом главных идеалов*, если все его идеалы главные.

**Предложение 5** (теорема об обрыве цепочки делителей). Пусть  $a_1, a_2, \dots, a_n, \dots$  — бесконечная последовательность элементов кольца  $A$  главных идеалов такая, что  $a_i$  делится на  $a_{i+1}$ ,

$i = 1, 2, \dots$  Тогда, начиная с некоторого места, члены последовательности ассоциированы.

**Доказательство.** Рассмотрим главные идеалы  $a_1A, a_2A, \dots, a_nA, \dots$ . Так как  $a_1$  делится на  $a_2$ , то  $a_1 \in a_2A$ , и, следовательно,  $a_1A \subseteq a_2A$ . По тем же соображениям  $a_iA \subseteq a_{i+1}A$  при всех  $i$ . Рассмотрим объединение  $B$  всех идеалов  $a_iA$ . Если  $b_1$  и  $b_2$  — два элемента из  $B$ , то они входят в идеалы  $a_iA$  и  $a_jA$  при некоторых  $i$  и  $j$  и, если  $i \leq j$ , оба входят в идеал  $a_jA$ . Следовательно,  $b_1 \pm b_2$  и  $b_1a$  при любом  $a \in A$  входят в  $a_jA$ , а следовательно, и в  $B$ . Таким образом, множество  $B$  есть идеал. Кольцо  $A$  есть кольцо главных идеалов и, следовательно,  $B = bA$  при некотором  $b \in B$ . Элемент  $b$  принадлежит одному из идеалов  $a_iA$ ,  $i = 1, 2, \dots$ , пусть, для определенности, идеалу  $a_mA$ . Тогда  $b \in a_nA$  при всех  $n \geq m$ . Поэтому  $b$  делится на все  $a_m$ ,  $m \geq n$ . С другой стороны, все  $a_i$  принадлежат  $B = bA$  и, следовательно, все  $a_i$ ,  $i = 1, 2, \dots$ , делятся на  $b$ . Итак,  $b$  делится на  $a_m$  при  $m \geq n$  и  $a_m$  делится на  $b$ . Поэтому  $a_m$  при  $m \geq n$  ассоциированы с  $b$  и потому ассоциированы друг с другом. Теорема доказана.

Из теоремы следует, что если имеется последовательность элементов  $a_1, a_2, \dots$ , в которой каждый член последовательности делится на следующий и не ассоциирован с ним, то такая последовательность конечна.

**6. Существование разложения на неразложимые множители в кольце главных идеалов.**

**Предложение 6.** *Любой элемент, не являющийся единицей в кольце главных идеалов, делится по крайней мере на один неразложимый элемент.*

**Доказательство.** Пусть  $A$  — кольцо главных идеалов и  $a \in A$ . Если  $a$  неразложим, то нечего доказывать. Пусть  $a = a_1b$ , причем  $a_1$  и  $b$  не являются единицами кольца. Тогда  $a$  делится на  $a_1$  и  $a$  не ассоциирован с  $a_1$ . Если  $a_1$  неразложим, то теорема для  $a$  доказана. Если  $a_1$  разложим, то найдется  $a_2$  такой, что  $a_1$  делится на  $a_2$  и  $a_1$  не ассоциирован с  $a_2$ . Если  $a_2$  неразложим, теорема для  $a$  доказана, ибо  $a$  делится на  $a_2$ . Если  $a_2$  разложим, повторяем рассуждение и т. д. Последовательность  $a, a_1, a_2, \dots$  оборвется на каком-то шагу, что и значит, что мы придем к неразложимому элементу  $a_k$ , на который делятся все предшествующие, включая  $a$ . Предложение доказано.

**7. Наибольший общий делитель элементов кольца главных идеалов.**

**Предложение 7.** *Для любых двух элементов  $a_1, a_2$  кольца  $A$  главных идеалов (и для любого конечного множества  $a_1, a_2, \dots, a_k$ ) существует общий делитель  $d$ , допускающий линейное представление  $d = a_1u_1 + a_2u_2$  ( $d = a_1u_1 + a_2u_2 + \dots + a_ku_k$ ) и, следовательно, делящийся на любой общий делитель  $a_1$  и  $a_2$  ( $a_1, a_2, \dots, a_k$ ).*

Такой общий делитель называется *наибольшим общим делителем*.

**Доказательство.** Рассмотрим множество элементов  $M = = a_1A + a_2A = \{a_1v_1 + a_2v_2 \mid v_1, v_2 \in A\}$ . Ясно, что  $M$  есть идеал, содержащий  $a_1$  и  $a_2$  (и ими порожденный, т. е. наименьший идеал, содержащий  $a_1$  и  $a_2$ ). Следовательно,  $M = dA$ , где  $d$  — один из элементов  $M$ . Все элементы идеала  $M$  делятся на  $d$ , в частности,  $a_1$  и  $a_2$  делятся на  $d$ . Но  $d$ , как и все элементы множества  $M$ , имеет линейное представление  $d = a_1u_1 + a_2u_2$  при некоторых  $u_1, u_2 \in A$ . Ясно, что  $d$  делится на любой общий делитель  $a_1$  и  $a_2$ , ибо правая часть на него делится. Предложение доказано. (Для доказательства предложения для  $a_1, a_2, \dots, a_k$  нужно рассмотреть идеал  $M = a_1A + a_2A + \dots + a_kA$ .)

Из линейного представления наибольшего общего делителя следует критерий взаимной простоты элементов — *для того чтобы  $a_1, a_2 \in A$  были взаимно просты, необходимо и достаточно существование таких  $u_1, u_2 \in A$ , что  $a_1u_1 + a_2u_2 = 1$* . Из этого критерия выводятся свойства взаимно простых элементов, в частности, если  $a_1a_2$  делится на  $b$ , а  $a_1$  и  $b$  взаимно просты, то  $a_2$  делится на  $b$ . Из этих свойств следуют свойства неразложимых элементов, аналогичные свойствам простых чисел и неприводимых полиномов, в частности, предложение о том, что если произведение  $a_1a_2 \dots a_m$  делится на неразложимый элемент  $p$ , то на него делится один из сомножителей. Наконец, справедлива

**Теорема 8.** *Разложение элемента кольца главных идеалов на неразложимые множители единственно с точностью до порядка следования сомножителей и ассоциированности.*

Тем самым, любое кольцо главных идеалов является факториальным кольцом.

Заметим, что *кольцо вычетов  $A/pA$  кольца главных идеалов по неразложимому элементу  $p$  является полем*. Действительно, если  $a$  принадлежит ненулевому классу по модулю  $p$ , т. е. не делится на  $p$ , то  $a$  и  $p$  взаимно просты и найдутся такие  $u, v \in A$ , что  $au + pv = 1$ , т. е.  $au \equiv 1 \pmod{p}$ , так что класс, содержащий  $u$ , есть обратный для класса, содержащего  $a$ .

Оглянувшись назад, мы увидим, что теория делимости в кольце  $\mathbb{Z}$  целых чисел и в кольце  $K[x]$  полиномов над полем фактически основывалась на том, что эти кольца являются кольцами главных идеалов. Именно, рассматривались идеалы  $a_1A + a_2A$ , относительно которых устанавливалось, что они главные.

Средством для этого была «теорема о делении с остатком», заключавшаяся в том, что для элементов  $a$  и  $b \neq 0$  существуют элементы  $q$  и  $r$  такие, что  $a = bq + r$ , причем  $r$  в некотором смысле меньше чем  $b$ . Уточняет это обстоятельство следующее определение:

Кольцо  $A$  называется *евклидовым*, если для любых элементов  $a$  и  $b \neq 0$  существуют  $q$  и  $r$  такие, что  $a = bq + r$  и  $\varphi(r) < \varphi(b)$ ,

где  $\varphi$  — функция на  $A$  с неотрицательными целыми значениями (иногда еще дополненными символом  $-\infty$ ). В кольце целых чисел роль  $\varphi$  играла абсолютная величина числа, в кольце полиномов — степень полинома.

*Всякое евклидово кольцо есть кольцо главных идеалов.* Действительно, пусть  $M$  — идеал евклидова кольца. Обозначим через  $d$  отличный от нуля элемент идеала, в котором функция  $\varphi$  имеет наименьшее значение. Тогда все элементы идеала  $M$  делятся на  $d$ , т. е.  $M = dA$ , ибо иначе для остатка  $r = a - dq \in M$  от деления какого-либо элемента  $a$  на  $d$  имели бы  $\varphi(r) < \varphi(d)$ .

## РАСПРЕДЕЛЕНИЕ КОРНЕЙ ПОЛИНОМА

### § 1. Существование корней в $\mathbb{C}$

**1. Элементы теории пределов для комплексных чисел.** В настоящей главе полиномы рассматриваются только над полями  $\mathbb{C}$  и  $\mathbb{R}$  как функции от комплексной или вещественной переменной, так что эта глава является скорее главой математического анализа, а не алгебры, хотя теорема о существовании корня у любого отличного от константы полинома с комплексными коэффициентами (т. е. установление алгебраической замкнутости поля  $\mathbb{C}$ ) носит название основной теоремы алгебры.

Выше, в § 5 гл. II, было дано определение предела последовательности комплексных чисел  $z_n = x_n + y_n i$  как такого числа  $c = a + bi$ , что  $a = \lim_{n \rightarrow \infty} x_n$ ,  $b = \lim_{n \rightarrow \infty} y_n$ . Предельное соотношение

$\lim_{n \rightarrow \infty} z_n = c$  равносильно соотношению  $|z_n - c| \rightarrow 0$ , ибо

$$\max(|x_n - a|, |y_n - b|) \leq |z_n - c| = \sqrt{(x_n - a)^2 + (y_n - b)^2} \leq \\ \leq \sqrt{2} \cdot \max(|x_n - a|, |y_n - b|).$$

Последовательность  $z_n$  такая, что  $|z_n| \leq R$  при некотором  $R$ , называется ограниченной.

Для вещественных переменных известна теорема Больцано — Вейерштрасса: из любой ограниченной последовательности можно извлечь сходящуюся подпоследовательность. То же самое верно и для последовательностей, составленных из комплексных чисел.

Действительно, пусть  $z_n = x_n + y_n i$  — ограниченная последовательность, т. е.  $|z_n| < R$ . Тогда  $|x_n| < R$ , так что  $x_n$  есть ограниченная последовательность вещественных чисел. Из нее можно выбрать сходящуюся подпоследовательность  $x_{n_k} \rightarrow a$ . Рассмотрим соответствующую подпоследовательность мнимых частей  $y_{n_k}$ . Она ограничена, и из нее можно извлечь сходящуюся подпоследовательность  $y_{n_{k_m}} \rightarrow b$ .

Соответствующая подпоследовательность комплексных чисел имеет сходящиеся последовательности вещественных и мнимых частей и, следовательно, сходится, и ее предел равен  $a + bi$ .

**2. Доказательство основной теоремы.** Прежде чем приступить к формальному доказательству, наметим его идею. Пусть  $f(z)$  — полином, рассматриваемый как функция от комплексной перемен-

ной  $z$ . Представим себе «график» функции  $\omega = |f(z)|$ , считая, что значения  $z$  изображаются на горизонтальной плоскости, перпендикулярной к плоскости чертежа, а значения  $|f(z)|$  откладываются вверх в направлении оси  $\omega$ . Мы установим, что  $f(z)$  и  $|f(z)|$  являются непрерывными функциями от  $z$  на всей плоскости комплексной переменной. Функция  $F(z)$  от комплексной переменной  $z$  называется непрерывной в точке  $z_0$ , если достаточно близким к  $z_0$  значениям  $z$  соответствуют сколь угодно близкие к  $F(z_0)$  значения  $F(z)$ . В более точных терминах — для любого  $\varepsilon > 0$  найдется такое  $\delta > 0$ , что  $|F(z) - F(z_0)| < \varepsilon$ , как только  $|z - z_0| < \delta$ .

Непрерывность  $|f(z)|$  дает основания представлять себе график  $\omega = |f(z)|$  в виде непрерывной поверхности, накрывающей плоскость  $\omega = 0$ , и местами доходящей до этой плоскости. Собственно говоря, нам и нужно доказать, что существует такое значение  $z_0$ , в котором  $f(z_0) = 0$ , и, тем самым,  $|f(z_0)| = 0$ , т. е. что поверхность  $\omega = |f(z)|$  доходит до плоскости  $\omega = 0$  в точке  $z_0$ . Мы докажем, что если дана точка на поверхности  $\omega = |f(z)|$ , которая расположена выше плоскости  $\omega = 0$ , то в ее окрестности найдется точка поверхности, расположенная ниже данной точки. Тогда останется только доказать, что на поверхности  $\omega = |f(z)|$  существует самая низкая точка, скажем, при  $z = z_0$ . Она не может находиться выше плоскости  $\omega = 0$ , ибо тогда она не была бы самой низкой. Следовательно,  $|f(z_0)| = 0$  и, следовательно,  $f(z_0) = 0$ , т. е.  $z_0$  есть корень полинома  $f(z)$ .

Теперь приступим к доказательству основной теоремы, разбив это доказательство на цепочку лемм.

**Лемма 1.** Дан полином  $f(z) = a_0 z^n + \dots + a_{n-1} z$  с нулевым свободным членом. Тогда для любого  $\varepsilon > 0$  найдется такое  $\delta > 0$ , что  $|f(z)| < \varepsilon$ , как только  $|z| < \delta$ .

**Доказательство.** Пусть  $|z| < 1$ . Тогда  $|f(z)| = |a_0 z^n + a_1 z^{n-1} + \dots + a_{n-1} z| = |z| \cdot |a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1}| \leq |z| (|a_0| + |a_1| + \dots + |a_{n-1}|)$ . Положим  $|a_0| + |a_1| + \dots + |a_{n-1}| = M$ . Если  $|z| < \min\left(1, \frac{\varepsilon}{M}\right)$ , то  $|f(z)| \leq |z| M < \frac{\varepsilon}{M} M = \varepsilon$ , что и требовалось доказать.

**Лемма 2.** Полином есть непрерывная функция во всех точках плоскости комплексной переменной.

**Доказательство.** Пусть дан полином  $f(z)$  и точка  $z_0$ . Расположим полином по степеням  $z - z_0$ :

$$f(z) = c_0 + c_1(z - z_0) + \dots + c_n(z - z_0)^n.$$

Тогда  $c_0 = f(z_0)$ , так что

$$f(z) - f(z_0) = c_1(z - z_0) + \dots + c_n(z - z_0)^n.$$

Правая часть есть полином от  $z - z_0$  с нулевым свободным членом,

По лемме 1 для любого  $\varepsilon > 0$  найдется такое  $\delta > 0$ , что  $|f(z) - f(z_0)| < \varepsilon$ , как только  $|z - z_0| < \delta$ , что и требовалось доказать.

**Лемма 3.** *Модуль полинома есть непрерывная функция.*

**Доказательство.** Из неравенства  $|f(z) - f(z_0)| \geq ||f(z)| - |f(z_0)||$  следует, что для данного  $\varepsilon > 0$  то  $\delta$ , которое «обслуживает»  $f(z)$ , подходит и для  $|f(z)|$ . Действительно, при  $|z - z_0| < \delta$  имеем  $||f(z)| - |f(z_0)|| \leq |f(z) - f(z_0)| < \varepsilon$ .

**Лемма 4** (о возрастании модуля полинома). *Если  $f(z)$  — полином, отличный от константы, то для любого  $M > 0$  существует такое  $R > 0$ , что  $|f(z)| > M$ , как только  $|z| > R$ .*

Это означает, что любая горизонтальная плоскость  $w = M$  отсекает от поверхности  $w = |f(z)|$  конечный кусок, накрывающий часть круга  $|z| \leq R$ .

**Доказательство.** Пусть  $f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n = a_0 z^n \left(1 + \frac{a_1}{a_0} z^{-1} + \dots + \frac{a_n}{a_0} z^{-n}\right) = a_0 z^n (1 + \varphi(z^{-1}))$ , где  $\varphi(z^{-1})$  — полином от  $z^{-1}$  с нулевым свободным членом. В силу леммы 1 для  $\varepsilon = 1/2$  найдется такое  $\delta > 0$ , что при  $|z^{-1}| < \delta$  будет  $|\varphi(z^{-1})| < 1/2$ . Модуль  $a_0 z^n$  может быть сделан сколь угодно большим, именно, при  $|z| > \sqrt[n]{2M/|a_0|}$  будет  $|a_0 z^n| > 2M$ . Возьмем  $R = \max_n \left(\sqrt[n]{2M/|a_0|}, 1/\delta\right)$ . Тогда при  $|z| > R$  будет  $|z^{-1}| < \delta$  и  $|z| > \sqrt[n]{2M/|a_0|}$ , так что  $|f(z)| \geq |a_0 z^n| (1 - |\varphi(z^{-1})|) > 2M \left(1 - \frac{1}{2}\right) = M$ .

**Лемма 5.** *Точная нижняя грань значений  $|f(z)|$  достигается, т. е. существует такое  $z_0$ , что  $|f(z_0)| \leq |f(z)|$  при всех  $z$ .*

**Доказательство.** Обозначим точную нижнюю грань  $|f(z)|$  через  $m$ . Возьмем последовательность  $m + \frac{1}{k}$ ,  $k = 1, 2, \dots$ , стремящуюся к  $m$  сверху. Каждое из этих чисел не является нижней гранью значений  $|f(z)|$ , ибо  $m$  — точная нижняя грань. Поэтому найдутся  $z_k$  такие, что  $|f(z_k)| < m + \frac{1}{k}$ ,  $k = 1, 2, \dots$ . Воспользуемся теперь леммой о возрастании модуля. Для  $M = m + \frac{1}{k}$  найдем такое  $R$ , что при  $|z| > R$  будет  $|f(z)| > M \geq m + \frac{1}{k}$ . Отсюда следует, что  $|z_k| \leq R$  при всех  $k$ . Последовательность  $z_k$  оказалась ограниченной, и из нее можно извлечь сходящуюся подпоследовательность  $z_{k_s}$ . Пусть ее предел равен  $z_0$ . Тогда  $\lim_{s \rightarrow \infty} |f(z_{k_s})| = |f(z_0)|$  в силу непрерывности  $|f(z)|$ . Кроме того,  $m \leq |f(z_{k_s})| \leq m + \frac{1}{k_s}$ . Поэтому  $\lim |f(z_{k_s})| = m$ . Итак  $|f(z_0)| = m$ , что и требовалось доказать.

Лемма 6 (лемма Даламбера). Пусть  $f(z)$  — полином, отличный от константы, и пусть  $f(z_1) \neq 0$ . Тогда найдется такая точка  $z_2$ , что  $|f(z_2)| < |f(z_1)|$ .

Геометрический смысл этой леммы: если на поверхности  $w = |f(z)|$  дана точка, находящаяся выше плоскости  $w = 0$ , то на ней найдется другая точка, расположенная ниже первой.

Доказательство. Расположим полином  $f(z)$  по степеням  $z - z_1$ :

$$f(z) = c_0 + c_1(z - z_1) + \dots + c_n(z - z_1)^n.$$

Тогда  $c_0 = f(z_1) \neq 0$ . Идея доказательства состоит в том, чтобы за счет первого отличного от нуля слагаемого «откусить кусочек» от  $c_0$ , а влияние дальнейших слагаемых сделать незначительным. Пусть  $c_k(z - z_1)^k$  — первое отличное от нуля слагаемое после  $c_0$ , так что  $c_1 = \dots = c_{k-1} = 0$  (если  $k > 1$ ). Такое слагаемое имеется, так как  $f(z)$  не константа. Тогда

$$\begin{aligned} f(z) &= c_0 + c_k(z - z_1)^k + c_{k+1}(z - z_1)^{k+1} + \dots + c_n(z - z_1)^n = \\ &= c_0 \left( 1 + \frac{c_k}{c_0}(z - z_1)^k + \right. \\ &\quad \left. + \frac{c_k}{c_0}(z - z_1)^k \left( \frac{c_{k+1}}{c_k}(z - z_1) + \dots + \frac{c_n}{c_k}(z - z_1)^{n-k} \right) \right) = \\ &= c_0 \left( 1 + \frac{c_k}{c_0}(z - z_1)^k + \frac{c_k}{c_0}(z - z_1)^k \varphi(z - z_1) \right). \end{aligned}$$

Здесь  $\varphi(z - z_1) = \frac{c_{k+1}}{c_k}(z - z_1) + \dots + \frac{c_n}{c_k}(z - z_1)^{n-k}$  есть полином от  $z - z_1$  с нулевым свободным членом. По лемме 1 для  $\varepsilon = 1/2$  найдется такое  $\delta$ , что  $|\varphi(z - z_1)| < 1/2$ , как только  $|z - z_1| < \delta$ .

Положим  $\frac{c_k}{c_0} = R(\cos \theta + i \sin \theta)$  и  $z - z_1 = r(\cos \varphi + i \sin \varphi)$ .

Тогда  $\frac{c_k}{c_0}(z - z_1)^k = Rr^k(\cos(\theta + k\varphi) + i \sin(\theta + k\varphi))$ . Выберем  $r$

так, что  $Rr^k < 1$ . Для этого нужно взять  $r < \sqrt[k]{1/R}$ . Далее, положим  $\theta + k\varphi = \pi$ , т. е. возьмем  $\varphi = (\pi - \theta)/k$ . При таком выборе будет  $\frac{c_k}{c_0}(z - z_1)^k = -Rr^k$ . Теперь положим  $z_2 = z_1 + r(\cos \varphi + i \sin \varphi)$

при  $r < \min(\delta, \sqrt[k]{1/R})$  и  $\varphi = (\pi - \theta)/k$ . Тогда  $f(z_2) = c_0(1 - Rr^k - Rr^k\varphi(z_2 - z_1))$  и

$$\begin{aligned} |f(z_2)| &= |c_0| \cdot |1 - Rr^k - Rr^k\varphi(z_2 - z_1)| \leq \\ &\leq |c_0| (|1 - Rr^k| + Rr^k|\varphi(z_2 - z_1)|) \leq |c_0| \left( 1 - Rr^k + \frac{1}{2} Rr^k \right) = \\ &= |c_0| \left( 1 - \frac{1}{2} Rr^k \right) < |c_0| = |f(z_1)|. \end{aligned}$$

Лемма доказана.

Заметим, что с тем же успехом мы могли взять  $\theta + k\varphi = \pi + 2\pi$  при  $t = 0, \dots, k-1$ , так что при  $k > 1$  (т. е. в случае, когда  $z_1$  — корень кратности  $k-1$  полинома  $f'(z)$ ) имеется  $k$  направлений спуска по поверхности  $w = |f(z)|$ . Они разделяются  $k$  направлениями подъема при  $\theta + k\varphi = 2\pi$ ,  $s = 0, \dots, k-1$ . Действительно, в этих направлениях  $\frac{c_k}{c_0}(z - z_1)^k = Rr^k$  и  $|f(z)| \geq |f(z_0)|(|1 + Rr^k| - Rr^k|\varphi(z - z_1)|) \geq |f(z_0)|\left(1 + \frac{1}{2}Rr^k\right) > |f(z_0)|$ . Так что если  $z_1$  есть корень производной кратности  $k-1$ , то поверхность  $w = |f(z)|$  в окрестности точки  $z_1$  «гофрирована» так, что на ней имеется  $k$  «долин» спуска, разделенных  $k$  «хребтами» подъема.

**Теорема.** *Полином с комплексными коэффициентами, отличный от постоянной, имеет по меньшей мере один комплексный корень (т. е. поле  $\mathbb{C}$  комплексных чисел алгебраически замкнуто).*

**Доказательство.** Пусть  $f(z)$  — данный полином, отличный от константы. Пусть, далее,  $m = \inf |f(z)|$  и  $z_1$  — точка, в которой  $|f(z_1)| = m$ ; она существует по лемме 5. Тогда  $f(z_1) = 0$ , ибо иначе, согласно лемме 6, нашлась бы такая точка  $z_2$ , что  $|f(z_2)| < |f(z_1)| = \inf |f(z)|$ , что невозможно.

## § 2. Распределение корней на плоскости комплексной переменной

**1. Аргумент комплексного числа, изображение которого движется по непрерывной линии.** В этом параграфе мы несколько отступим от того уровня математической строгости, который принят в учебной математической литературе, и позволим себе чуть больше «верить своим глазам», прибегая к наглядным геометрическим представлениям.

Пусть комплексная переменная  $z$  меняется так, что ее изображение непрерывно движется по некоторой непрерывной линии, не проходящей через начало координат. Это значит, что  $z = z(t)$  есть непрерывная функция от вещественного параметра  $t$ , меняющегося в замкнутом промежутке  $a \leq t \leq b$ , причем  $z(t) \neq 0$  при

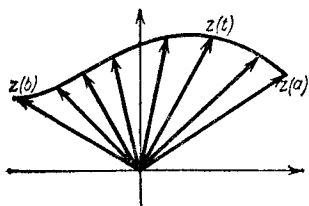


Рис. 9.

всех значениях  $t$ . Тогда радиус-вектор точки  $z(t)$  будет непрерывно поворачиваться вокруг начала координат, изменяясь по длине, но ни разу не сжимаясь в точку, и угол, который он образует с вещественной осью, т. е.  $\arg z(t)$ , можно считать тоже изменяющимся непрерывно (рис. 9). Таким образом, выбрав каким-либо способом значение аргумента числа  $z(a)$  в начале пути, можно выбрать значения аргумента  $z(t)$  при всех  $t$  так, чтобы в целом функция  $\arg z(t)$  оказалась непрерывной функцией параметра  $t$ . (Читатель,

несколько искушенный в началах математического анализа, в состоянии дать более строгое доказательство этого утверждения, например по такой схеме. Пусть  $r = \inf |z(t)|$ . Тогда  $r > 0$ , ибо непрерывная функция  $|z(t)|$  на замкнутом промежутке  $[a, b]$  достигает своей нижней грани. В силу равномерной непрерывности непрерывной на  $[a, b]$  функции, можно разбить промежуток  $[a, b]$  на конечное число интервалов так, что в пределах каждого из них колебание компонент  $x(t)$  и  $y(t)$  функции  $z(t)$  не превосходит  $\frac{1}{2}r$ . Тогда  $z(t)$  на каждом таком интервале изменяется не более чем в двух смежных координатных квадрантах, и здесь справедливость утверждения очевидна. Остается согласовать выбор аргумента на границах интервалов.)

Предположение о том, что  $z(t)$  не обращается в нуль, существенно. Так, например, пусть  $z(t) = t$  при  $-1 \leq t \leq 1$ . При  $t < 0$  аргумент  $z(t)$  будет равен нечетному кратному  $\pi$ , а при  $t > 0$  — четному кратному. Выбор значений аргумента здесь нельзя так согласовать, чтобы сохранить непрерывность при  $t = 0$ .

Пусть теперь имеется несколько непрерывных комплексных функций  $z_1(t), \dots, z_k(t)$  от вещественной переменной  $t$ ,  $a \leq t \leq b$ , каждая из которых не обращается в нуль ни в какой точке данного промежутка. Тогда их произведение  $z(t) = z_1(t) \dots z_k(t)$  — тоже непрерывная функция, не обращающаяся в нуль на этом промежутке. Выберем значения аргументов  $z_1(t), \dots, z_k(t)$  и  $z(t)$  при  $t = a$  так, чтобы аргумент  $z(a)$  был равен сумме аргументов  $z_1(a), \dots, z_k(a)$  (а не отличался от нее на четное кратное  $\pi$ ). Тогда, при непрерывном изменении аргументов, равенство  $\arg z(t) = \arg z_1(t) + \dots + \arg z_k(t)$  сохранится при всех  $t$ ,  $a \leq t \leq b$ . Действительно, разность  $\arg z(t) - (\arg z_1(t) + \dots + \arg z_k(t))$  может принимать лишь значения 0 и четные кратные  $\pi$ , причем равна 0 при  $t = a$ . Но, будучи непрерывной функцией, она не может изменяться скачками и потому остается равной нулю при всех  $t$ .

Пусть теперь линия, по которой двигается  $z$ , замкнута. Это значит, по-прежнему, что  $z = z(t)$  — непрерывная функция от вещественной переменной  $t$ ,  $a \leq t \leq b$ , и  $z(b) = z(a)$ . В этом случае, при непрерывном изменении аргумента, мы можем получить при  $t = b$  значение аргумента, отличное от значения при  $t = a$ . Разность значений аргумента может равняться только целому кратному  $k \cdot 2\pi$  числа  $2\pi$ . Коэффициент  $k$  имеет ясный геометрический смысл. Он равен числу полных оборотов вокруг начала координат радиус-вектора точки  $z(t)$  при обходе этой точкой ли-

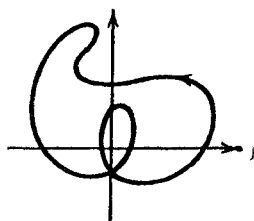


Рис. 10.

нии в направлении возрастания параметра  $t$ , с учетом знака в соответствии с направлением обхода.

Так, для приращения аргумента  $z(t)$  на рис. 10 при указанном направлении обхода  $k = 2$ , при противоположном  $k = -2$ .

**2. Принцип аргумента.** Пусть функция  $z = z(t)$  непрерывна при  $a \leq t \leq b$ ,  $z(a) = z(b)$  и, за исключением этого случая,  $z(t_1) \neq z(t_2)$  при  $t_1 \neq t_2$ . В этой ситуации  $z$  описывает простой замкнутый контур, т. е. непрерывную замкнутую линию без самопересечений. Имеет место замечательная топологическая теорема Жордана о том, что простой замкнутый контур разбивает плоскость



Рис. 11.

на две связные части — внутри и вне контура (фигура на плоскости называется связной, если любые две ее точки можно соединить непрерывной линией, целиком лежащей на ней). Теорема Жордана тривиальна для окружности — точки ее внешней части характеризуются тем, что расстояние от них до центра больше радиуса,

точки внутренней — тем, что это расстояние меньше радиуса. Теорема «на глаз» очевидна, если контур несложен, но наглядность теряется для более сложных контуров (см. рис. 11), особенно, если от контура ничего не требовать, кроме непрерывности.

**Лемма.** Пусть  $z$  проходит простой замкнутый контур в положительном направлении. Тогда приращение аргумента  $z - z_1$  равно  $2\pi$  или 0 в зависимости от того, где находится  $z_1$  — внутри или вне контура.

**Доказательство.** Ограничимся геометрически наглядным случаем выпуклого контура, например окружности. Пусть  $z_1$  находится внутри контура (рис. 12). Число  $z - z_1$  изображается

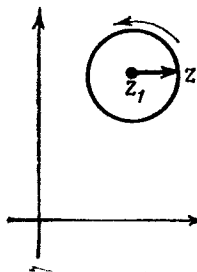


Рис. 12.

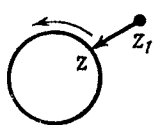


Рис. 13.

вектором, исходящим из точки  $z_1$  в точку  $z$ . Ясно, что когда  $z$  обойдет контур один раз в положительном направлении, вектор  $z - z_1$  обернется вокруг своего начала один раз, тоже в положительном направлении, и приращение аргумента  $z - z_1$  равно  $2\pi$ .

Пусть теперь  $z_1$  находится снаружи контура (рис. 13). Тогда колебание аргумента  $z - z_1$

не превосходит  $\pi$ , так что приращение аргумента может быть равно только нулю.

Лемма остается верной для произвольного простого замкнутого контура, но ее доказательство в общем случае довольно

сложно. Для дальнейшего нам нужен только случай выпуклого контура, в частности окружности.

**Теорема (принцип аргумента).** *Дан простой замкнутый контур и полином  $f(z)$ , не имеющий корней на контуре. Тогда число корней полинома внутри контура (с учетом кратностей) равно  $\frac{1}{2\pi} \Delta \arg f(z)$ , где  $\Delta \arg f(z)$  есть приращение аргумента  $f(z)$ , вычисленное в предположении, что  $z$  проходит данный контур один раз в положительном направлении.*

**Доказательство.** Над полем  $\mathbb{C}$  каждый полином может быть разложен на линейные множители, соответствующие корням. Пусть  $f(z) = a_0(z - z_1) \dots (z - z_n)$  — такое разложение. При обходе переменной  $z$  контура области все сомножители правой части и их произведение  $f(z)$  меняются непрерывно. Можно считать, что  $\arg f(z) = \arg a_0 + \arg(z - z_1) + \dots + \arg(z - z_n)$ , и, следовательно,  $\Delta \arg f(z) = \Delta \arg(z - z_1) + \dots + \Delta \arg(z - z_n)$ . Здесь приращения отсчитываются при однократном обходе  $z$  по контуру области. Слагаемые в правой части равны  $2\pi$  или 0, в зависимости от того, лежит ли соответствующий корень  $z_i$  внутри или вне контура. Поэтому  $\Delta \arg f(z) = m \cdot 2\pi$ , где  $m$  — число корней, расположенных внутри контура, что и доказывает теорему.

Теорема позволяет фактически найти число корней в данной области, ограниченной простым замкнутым контуром. На контуре нужно взять достаточно густую сетку точек, в каждой точке вычислить значение полинома, нанести их на чертеж и проследить за приращением аргумента. Правда, заранее неизвестно, насколько густую сетку точек нужно взять.

**3. Теорема Руше.** Имеются случаи, когда принцип аргумента позволяет найти число корней полинома в области почти без вычислений.

Рассмотрим пример. Требуется узнать, сколько корней имеет полином  $z^5 + 5z^2 - 3$  внутри единичного круга  $|z| \leq 1$ . На контуре  $z = e^{it}$ ,  $0 \leq t \leq 2\pi$ , второе слагаемое  $5z^2 = 5e^{2it}$  преобладает по модулю над остальными, ибо  $|5z^2| = 5$ , а  $|z^5 - 3| \leq 1 + 3 = 4$ . Ясно, что пока  $z$  обходит один раз единичную окружность в положительном направлении,  $5z^2$  обойдет окружность радиуса 5 два раза, а  $f(z)$ , будучи «привязан» к  $5z^2$  вектором, изображающим  $z^5 - 3$ , длина которого не превосходит 4, вынужден тоже обойти вокруг начала два раза. Поэтому полином  $z^5 + 5z^2 - 3$  имеет внутри единичного круга два корня.

Пусть теперь требуется узнать число корней этого полинома в круге радиуса 2. Преобладающим слагаемым на контуре  $z = 2e^{it}$ ,  $0 \leq t \leq \pi$ , оказывается  $z^5 = 32e^{5it}$ , модуль которого равен 32. Сумма остальных слагаемых  $5z^2 - 3$  по модулю не превосходит  $5 \cdot 2^2 + 3 = 23$ . Слагаемое  $z^5$  обходит начало координат 5 раз, и  $f(z)$ , отходя от  $z^5$  не более чем на 23 единицы, тоже обходит начало 5 раз. Число корней полинома в круге радиуса 2 равно 5.

Итак, мы узнали, что  $z^5 + 5z^2 - 3$  имеет 2 корня в единичном круге и 3 корня в кольце между окружностями  $|z| = 1$  и  $|z| = 2$ .

Приведем теперь теорему, частными случаями которой являются только что приведенные рассуждения.

**Теорема (Руше).** Пусть полином  $f(z) = f_1(z) + f_2(z)$  представляется в виде суммы двух полиномов, и на контуре области выполнено неравенство  $|f_2(z)| < |f_1(z)|$ . Тогда число корней полиномов  $f(z)$  и  $f_1(z)$  внутри области одинаково.

**Доказательство.** Прежде всего убедимся в том, что к полиномам  $f_1(z)$  и  $f(z)$  можно применить принцип аргумента. Из неравенств  $|f_1(z)| > |f_2(z)|$  и  $|f(z)| \geq |f_1(z)| - |f_2(z)| > 0$ , справедливых для всех  $z$  на контуре, следует что  $f_1(z)$  и  $f(z)$  не обращаются в 0 на контуре. Далее,  $f(z) = f_1(z) \left[ 1 + \frac{f_2(z)}{f_1(z)} \right]$ , так что

$\Delta \arg f(z) = \Delta \arg f_1(z) + \Delta \arg \left( 1 + \frac{f_2(z)}{f_1(z)} \right)$ , пока  $z$  проходит контур области. Далее, из  $\left| \frac{f_2(z)}{f_1(z)} \right| < 1$  следует, что  $1 + \frac{f_2(z)}{f_1(z)}$  имеет значения, лежащие внутри круга с центром в точке 1 и с единичным радиусом, так что все они находятся в правой полуплоскости. Вектор, исходящий из 0 в точку  $1 + \frac{f_2(z)}{f_1(z)}$ , не может повернуться вокруг начала, так что  $\Delta \arg \left( 1 + \frac{f_2(z)}{f_1(z)} \right) = 0$ . Следовательно,  $\Delta \arg f(z) = \Delta \arg f_1(z)$ .

Согласно принципу аргумента, число корней полиномов  $f_1(z)$  и  $f(z)$  внутри области одинаково, что и требовалось доказать.

**4. Непрерывность корней полинома.** Пусть дан полином  $f_0(z)$ . Покажем, что его корни меняются непрерывно при изменении коэффициентов. Именно, при достаточно малом изменении коэффициентов корни меняются сколь угодно мало, но только кратные корни могут распадаться, превращаясь в совокупность корней в количестве (с учетом кратностей), равном кратности исходного корня.

Действительно, пусть  $z_0$  — корень кратности  $k$  для полинома  $f_0(z)$  и пусть  $f(z) = f_0(z) + g(z)$  — полином, полученный из  $f_0(z)$  малым изменением его коэффициентов. Окружим корень  $z_0$  сколь угодно малой окружностью, причем настолько малой, чтобы в ограниченном ею круге не было корней полинома  $f_0(z)$ , кроме  $z_0$ . Пусть  $m = \inf |f_0(z)|$  при  $z$ , меняющемся на окружности. Так как функция  $|f(z)|$  непрерывна и не обращается на окружности в нуль,  $m > 0$ . Возьмем коэффициенты полинома  $g(z)$  столь малыми, что на окружности  $|g(z)| < m$ . Тогда на этой окружности выполнено условие теоремы Руше, и полином  $f(z)$  имеет столько же корней внутри круга (с учетом кратностей), сколько их имеет  $f_0(z)$ , т. е.  $k$ .

В частности, простой корень при малом изменении коэффициентов немного перемещается, оставаясь простым. Если коэффици-

циенты зависят от вещественного параметра  $t$ , являясь не только непрерывными, но и дифференцируемыми функциями, то простые корни имеют производные по  $t$ , именно,  $\frac{dz_0}{dt} = -\frac{1}{f'_0(z_0)} \cdot \frac{\partial f_0}{\partial t} \Big|_{z=z_0}$ .

В точках, где эта производная отлична от нуля, корень перемещается по гладкой кривой. Картина усложняется, когда корни «сталкиваются», превращаясь при некотором значении  $t$  в кратный корень. Рассмотрим простой пример. Пусть  $f(z) = z^2 - 2z + t$  при  $0 \leq t \leq 2$ . При  $t = 0$  корни равны 0 и 2. Далее,  $z_{1,2} = 1 \pm \sqrt{1-t}$ . При изменении  $t$  от 0 до 1 корни сближаются и, при  $t = 1$ , сливаются при значении  $z = 1$  (рис. 14). При дальнейшем увеличении  $t$  корни становятся комплексными и расходятся вдоль прямой  $\operatorname{Re} z = 1$ . У нас нет никаких оснований считать, который из корней пошел вверх: тот, который пришел слева, или тот, который пришел справа. Корни после столкновения как бы теряют индивидуальность.

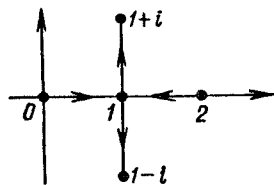


Рис. 14.

### § 3. Распределение вещественных корней полинома с вещественными коэффициентами

**1. Ограничение вещественных корней полинома с вещественными коэффициентами.** Лемма о возрастании модуля (§ 1) дает средство для ограничения всех корней по модулю сверху. Именно, если для  $M = 0$  найти такое  $R$ , что  $|f(z)| > M = 0$ , как только  $|z| > R$ , то, очевидно, за пределами круга радиуса  $R$  полином  $f(z)$  не имеет корней, и поэтому все его корни не превосходят  $R$  по модулю.

Для вещественных корней полиномов с вещественными коэффициентами можно указать другие оценки, которые иногда оказываются лучше. Приведем одну из них.

**Теорема (оценка Маклорена).** Пусть  $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \in \mathbb{R}[x]$ , причем  $a_0 > 0$ . Если  $f(x)$  не имеет отрицательных коэффициентов, то отсутствуют положительные корни, так что верхней оценкой для вещественных корней оказывается число 0. Пусть отрицательные коэффициенты имеются,  $m$  — номер первого по порядку отрицательного коэффициента и  $A$  — максимум модулей отрицательных коэффициентов. Тогда вещественные корни

$f(x)$  не превосходят  $1 + \sqrt[m]{\frac{A}{a_0}}$ .

**Доказательство.** Пусть все коэффициенты неотрицательны и  $x > 0$ . Тогда  $f(x) > 0$ , так что  $f(x)$  не имеет положительных корней. Пусть теперь отрицательные коэффициенты есть и  $x \geq$

$\geq 1 + \sqrt[m]{\frac{A}{a_0}}$ . Имеем:  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{m-1}x^{n-m+1} + \dots + a_n$ . Подчеркнутые слагаемые, если они есть, неотрицательны при  $x > 0$ , и потому

$$f(x) \geq a_0x^n + a_mx^{n-m} + \dots + a_n.$$

При  $k \geq m$  будет  $a_k \geq -A$ , следовательно,

$$\begin{aligned} f(x) &\geq a_0x^n - A(x^{n-m} + \dots + 1) = a_0x^n - A \frac{x^{n-m+1} - 1}{x - 1} = \\ &= \frac{x^{n-m+1}(a_0x^{m-1}(x-1) - A)}{x-1} + \frac{A}{x-1} > \\ &> \frac{x^{n-m+1}(a_0x^{m-1}(x-1) - A)}{x-1} \geq \frac{x^{n-m+1}(a_0(x-1)^m - A)}{x-1} \geq \\ &\geq \frac{x^{n-m+1}}{x-1} \left( a_0 \left( \sqrt[m]{\frac{A}{a_0}} \right)^m - A \right) = 0. \end{aligned}$$

Итак, при  $x \geq 1 + \sqrt[m]{\frac{A}{a_0}}$  будет  $f(x) > 0$ , так что все вещественные корни не превосходят  $1 + \sqrt[m]{\frac{A}{a_0}}$ , что и требовалось доказать.

При помощи оценки корней сверху легко получить и оценку снизу. Для этого достаточно рассмотреть полином

$$g(x) = (-1)^n f(-x) = a_0x^n - a_1x^{n-1} + a_2x^{n-2} + \dots + (-1)^n a_n.$$

Корни этого полинома равны корням полинома  $f$  с обратным знаком, так что из оценки корней его сверху,  $-x_i < M$ , получим оценку снизу для корней исходного полинома:  $x_i > -M$ .

**Пример.** Найти оценки сверху и снизу для корней полинома

$$f(x) = x^5 + 3x^3 - 4x^2 - 2x + 4.$$

Сверху:  $x_i < 1 + \sqrt[5]{4} < 3$ .

Снизу: составим  $g(x) = x^5 + 3x^3 + 4x^2 - 2x - 4$ , имеем  $-x_i < 1 + \sqrt[5]{4} < 3$ .

Итак,  $-3 < x_i < 3$ .

Оценка Маклорена довольно грубая. Имеется много других приемов оценивания вещественных корней полиномов с вещественными коэффициентами. Мы не будем на этом останавливаться.

**2. Теорема Штурма.** Здесь будет решена следующая задача. Дан полином с вещественными коэффициентами и дан промежуток на вещественной оси. Требуется узнать, сколько корней имеет полином на этом промежутке. Способ решения этой задачи осно-

ван на принципе счетчика. К переменной  $x$ ,двигающейся от левого конца промежутка, будет «приделан счетчик», стрелка которого поворачивается на одно деление, как только  $x$  проходит через корень полинома. Тогда число корней полинома на интервале равно разности показаний счетчика в начале и в конце интервала. Роль показаний счетчика будет играть число перемен знаков среди значений некоторой конечной последовательности (последовательности Штурма) вспомогательных полиномов. Под числом перемен знаков в некоторой последовательности вещественных чисел понимается число пар соседних элементов последовательности, имеющих противоположные знаки, причем нулевые члены исключаются из последовательности.

Последовательность  $f_0, f_1, \dots, f_k$  Штурма полиномов, построенных для данного полинома  $f = f_0$ , удовлетворяет следующим требованиям при значениях  $x$  из данного интервала  $(a, b)$ :

1. Последний полином  $f_k$  не обращается в нуль.
2. Два соседних полинома не обращаются в нуль одновременно.

3. Если некоторый полином  $f_i$ ,  $1 \leq i \leq k-1$ , обращается в нуль в некоторой точке  $x_0$ , то соседние полиномы  $f_{i-1}$  и  $f_{i+1}$  имеют в  $x_0$  значения противоположных знаков.

4. Произведение  $f_0 f_1$  меняет знак с минуса на плюс, когда  $x$ , возрастая, проходит через корень полинома  $f_0$ .

*Теорема Штурма. Число корней полинома  $f(x)$  в промежутке  $[a, b]$  равно числу перемен знаков в значениях полиномов ряда Штурма при  $x = a$  минус число перемен знаков при  $x = b$ . Предполагается, что концы промежутка не являются корнями  $f(x)$ .*

Тем самым ряд Штурма играет роль «счетчика» корней.

Доказательство проводится по принципу счетчика. Рассмотрим промежуток  $[a, b]$ . На нем имеются корни начального полинома  $f_0 = f$  и корни других полиномов ряда Штурма. Мы докажем, что число перемен знаков в значениях полиномов ряда Штурма изменяется, только когда  $x$  проходит через корень начального полинома, и тогда это число уменьшается на 1. Ясно, что полином, в силу непрерывности, может изменить знак, только когда  $x$  проходит через корень полинома. Поэтому нам нужно проследить, что происходит со знаками и с числом перемен знаков при переходе через корень начального полинома и через корни других полиномов Штурма. Пусть  $x_0$  является корнем некоторого полинома  $f_i(x)$  ряда Штурма и не является корнем начального полинома. Может случиться, что кроме полинома  $f_i(x)$  некоторые другие полиномы тоже обращаются в нуль при  $x_0$ . Допустим, для определенности, что таким полиномом является  $f_j(x)$ . Пусть все остальные полиномы ряда Штурма не обращаются в 0 в точке  $x_0$ . Выберем промежуток  $(x_0 - \delta, x_0 + \delta)$  настолько малым, что в нем не содержится ни одного корня полиномов ряда Штурма, кроме  $x_0$ , и про-

следим за изменением числа перемен знаков, когда  $x$  проходит этот промежуток. С этой целью рассмотрим следующую таблицу:

	$f_0$	$f_1$	...	$f_{i-1}$	$f_i$	$f_{i+1}$	...	$f_{j-1}$	$f_j$	$f_{j+1}$	...	$f_k$
$x_0 - \delta < x < x_0$				$\sigma$	$\sigma$ $-\sigma$	$-\sigma$		$\sigma_1$		$-\sigma_1$		
$x = x_0$				$\sigma$	0	$-\sigma$		$\sigma_1$	0	$-\sigma_1$		
$x_0 < x < x_0 + \delta$				$\sigma$	$\sigma$ $-\sigma$	$-\sigma$		$\sigma_1$		$-\sigma_1$		

Полиномы  $f_0, \dots, f_{i-1}, f_{i+1}, \dots, f_{j-1}, f_{j+1}, \dots, f_k$  в нуль не обращаются, и их знаки не изменяются на всем промежутке  $(x_0 - \delta, x_0 + \delta)$ , следовательно, и число перемен знаков среди пар, не включающих  $f_i$  и  $f_j$ , не изменяется. Пусть  $f_{i-1}(x_0)$  имеет знак  $\sigma$  (+ или -). Этот знак сохраняется на всем промежутке  $(x_0 - \delta, x_0 + \delta)$ . По третьему свойству полиномов Штурма полином  $f_{i+1}$  имеет знак  $-\sigma$ . Какие бы знаки ни имел полином  $f_i$  слева и справа от  $x_0$ , число перемен знаков в отрезке  $f_{i-1}, f_i, f_{i+1}$  ряда Штурма остается равным 1 и не изменяется. Такая же картина имеет место на отрезке  $f_{j-1}, f_j, f_{j+1}$ . Таким образом, когда  $x$  проходит по промежутку, не содержащему корней начального полинома  $f_0 = f$ , но, быть может, содержащему корни других полиномов ряда, число перемен знаков среди значений полиномов ряда Штурма не изменяется.

Пусть теперь  $x_0$  — корень начального полинома  $f_0$ . Возможно, что кроме него при  $x_0$  обращаются в нуль какие-либо другие полиномы. Положим, что  $f_i(x_0) = 0$ . Рассмотрим снова таблицу распределения знаков:

	$f_0$	$f_1$	...	$f_{i-1}$	$f_i$	$f_{i+1}$	...	$f_k$
$x_0 - \delta < x < x_0$	$-\sigma_1$	$\sigma_1$		$\sigma$		$-\sigma$		
$x = x_0$	0	$\sigma_1$		$\sigma$	0	$-\sigma$		
$x_0 < x < x_0 + \delta$	$\sigma_1$	$\sigma_1$		$\sigma$		$-\sigma$		

На участке  $f_{i-1}, f_i, f_{i+1}$  ряда Штурма картина распределения знаков будет такая же, как в предыдущем случае, так что, хотя знак полинома  $f_i$  может измениться, число перемен знаков на этом участке не изменится. Полином  $f_1$  в точке  $x_0$  не обращается в 0, согласно второму свойству ряда Штурма. Пусть  $\sigma_1$  — знак  $f_1(x_0)$ . Этот знак полином  $f_1$  сохраняет на всем промежутке  $(x_0 - \delta, x_0 + \delta)$ . Согласно четвертому свойству ряда Штурма знак  $f_0(x)$  до  $x_0$  противоположен знаку  $f_1(x)$ , а после  $x_0$  знаки  $f_0(x)$  и  $f_1(x)$

одинаковы. Таким образом, на участке  $f_0, f_1$  ряда Штурма, а следовательно, и во всем ряду Штурма число перемен знаков уменьшается на единицу (счетчик повернулся на одно деление).

Сопоставляя все сказанное, делаем вывод, что при изменении  $x$  от  $a$  до  $b$  число перемен знаков среди значений полиномов ряда Штурма уменьшается на столько единиц, сколько корней полинома  $f_0(x)$  лежит между  $a$  и  $b$ , что и доказывает теорему Штурма.

Из рассмотрения второй таблицы мы видим, что число перемен знаков при корне  $x_0$  начального полинома такое же, как направо от корня, и на единицу меньше, чем налево от корня. Принимая это во внимание, мы можем в теореме Штурма снять предположение, что  $f_0$  не имеет корней на концах промежутка. Если начало  $a$  является корнем, то при отходе от него вправо число перемен знаков не изменится, а если конец  $b$  является корнем, то при подходе к нему слева в последний момент число перемен знаков уменьшится на одну единицу. Таким образом, разность числа перемен знаков значений полиномов ряда Штурма в начале и в конце промежутка равна числу корней полинома  $f$  на этом промежутке, исключая левый конец (если он является корнем) и включая правый (если он является корнем).

**3. Построение ряда Штурма.** Заметим прежде всего, что если полином имеет на  $(a, b)$  корень  $x_0$  четной кратности, то для него построение ряда Штурма невозможно. Действительно, нужно, чтобы  $f_1(x_0) \neq 0$ , так что знак полинома  $f_1(x)$  должен сохраняться в окрестности  $x_0$ . Так как  $x_0$  — корень четной кратности для  $f_0(x)$ , полином  $f_0(x)$  тоже не меняет знака в окрестности  $x_0$ , так что  $f_0(x)f_1(x)$  не может изменить знак, как это должно быть согласно последнему требованию. Однако удовлетворить этому требованию можно всегда. Именно, верно следующее

*Предложение. Произведение полинома  $f(x) \in \mathbb{R}[x]$  на его производную меняет знак с минуса на плюс, когда  $x$ , возрастая, проходит через корень  $f(x)$ .*

**Доказательство.** Пусть  $x_0$  — корень полинома  $f(x)$  кратности  $k$ , так что  $f(x) = (x - x_0)^k g(x)$  и  $g(x_0) \neq 0$ . Тогда

$$\begin{aligned} f'(x) &= k(x - x_0)^{k-1} g(x) + (x - x_0)^k g'(x) = \\ &= (x - x_0)^{k-1} (kg(x) + (x - x_0)g'(x)), \end{aligned}$$

$$\text{так что } f(x)f'(x) = (x - x_0)^{2k-1} [k(g(x))^2 + (x - x_0)g(x)g'(x)] = \\ = (x - x_0)^{2k-1} F(x).$$

Имеем  $F(x_0) = k[g(x_0)]^2 > 0$  и, следовательно,  $F(x)$  остается положительным в окрестности  $x_0$ . Но  $(x - x_0)^{2k-1}$  меняет знак с минуса на плюс, когда  $x$  проходит через  $x_0$ . Следовательно, то же самое будет и для произведения  $(x - x_0)^{2k-1} F(x) = f(x)f'(x)$ .

Далее будем считать, что полином  $f$  не имеет кратных корней и, следовательно, взаимно прост со своей производной.

За полином  $f_1(x)$  ряда Штурма примем производную полинома  $f(x) = f_0(x)$ . Затем применим к полиномам  $f_0(x)$  и  $f_1(x)$  алгоритм

Евклида, меняя на каждом шагу знак остатка на обратный. Полученные последовательные остатки примем за полиномы  $f_2, f_3, \dots, f_k$ . В силу взаимной простоты  $f_0$  и  $f_1$  последний полином  $f_k \neq 0$  есть константа. Таким образом, эти полиномы связаны соотношениями

$$\begin{aligned} f_0 &= f_1 g_1 - f_2, \\ f_1 &= f_2 g_2 - f_3, \\ &\dots \dots \dots \\ f_{k-2} &= f_{k-1} g_{k-1} - f_k. \end{aligned}$$

Проверим, что построенные полиномы удовлетворяют всем требованиям ряда Штурма. Последний полином не обращается в нуль, так как он есть отличная от нуля константа. Из соотношения  $f_{i-1}(x) = f_i(x)q(x) - f_{i+1}(x)$  следует, что если  $f_{i-1}(x_0) = f_i(x_0) = 0$ , то и  $f_{i+1}(x_0) = 0$ , но тогда и  $f_{i+2}(x_0) = 0$  и т. д., наконец  $f_k(x_0) = 0$ , что невозможно. Итак, два соседних полинома ряда одновременно в 0 не обращаются. Далее, если  $f_i(x_0) = 0$ , то  $f_{i-1}(x_0) = -f_{i+1}(x_0)$ , так что они имеют противоположные знаки. Итак, три первых требования ряда Штурма выполнены.

Заметим, что они были бы выполнены, если в качестве  $f_1(x)$  взять любой полином, взаимно простой с  $f(x) = f_0(x)$ .

Наконец, четвертое требование выполнено при  $f_1(x) = f'(x)$  в силу доказанного предложения.

Заметим еще, что свойства ряда Штурма сохраняются, если полиномы умножить на любые положительные константы. Это замечание полезно при решении примеров.

Пример 1.  $f(x) = x^3 - 7x - 7$ .

Возьмем  $f_1(x) = f'(x) = 3x^2 - 7$ . При делении  $3f(x)$  на  $f_1(x)$  в остатке получим  $-14x - 21$ , так что в качестве  $f_2$  можно взять  $2x + 3$ . При делении  $4f_1(x) = 12x^2 - 28$  на  $f_2$  получим в остатке  $-1$ , так что  $f_3 = 1$ . Таблица распределения знаков

	$f_0$	$f_1$	$f_2$	$f_3$
$-\infty$	—	+	—	+
$-2$	—	+	—	+
$-1$	—	—	+	+
$0$	—	—	+	+
$+\infty$	+	+	+	+

показывает, что имеется один положительный корень и два отрицательных в интервале  $(-2, -1)$ . Для уточнения расположения корней вычислим  $f(-3/2) = 1/8 > 0$ , так что мы можем заключить, уже не обращаясь к ряду Штурма, что корни лежат по одному в интервалах  $(-2, -3/2)$  и  $(-3/2, -1)$ . Для уточнения положения положительного корня заметим, что  $f(3) = -1 < 0$ ,  $f(4) = 29 \geq 0$ , следовательно, корень лежит в интервале  $(3, 4)$ .

Пример 2.  $f(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$ .

Здесь мы несколько отступим от описанного выше приема построения ряда Штурма. Полином  $f(x)$  не имеет положительных корней, так что все его вещественные корни, если они есть, лежат в интервале  $(-M, -\delta)$ , где  $M$  достаточно большое и  $\delta$  достаточно малое положительные числа. Именно для этого интервала мы будем строить полиномы Штурма. Имеем  $f'(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \dots + \frac{x^{n-1}}{(n-1)!}$ , так что  $f(x) = f'(x) - \left(-\frac{x^n}{n!}\right)$ . Положим  $f_0 = f$ ,  $f_1 = f'$  и  $f_2 = -\frac{x^n}{n!}$ . Очевидно, что все требования для ряда Штурма на интервале  $(-M, -\delta)$  выполнены. Таблица распределения знаков

	$f_0$	$f_1$	$f_2$
$-M$	$(-1)^n$	$(-1)^{n-1}$	$(-1)^{n-1}$
$-\delta$	$+$	$+$	$(-1)^{n-1}$

показывает одну переменную знаков при  $-M$  и одну или нуль перемен при  $-\delta$ , в соответствии с четностью или нечетностью  $n$ . Следовательно, полином  $f$  имеет один вещественный (отрицательный) корень при нечетном  $n$  и не имеет вещественных корней при четном  $n$ .

#### § 4. Обобщенная теорема Штурма

**1. Индекс полинома с вещественными коэффициентами относительно другого полинома.** Пусть  $f$  и  $g$  — два взаимно простых полинома с вещественными коэффициентами. Скажем, что вещественный корень  $x_0$  полинома  $f$  есть корень первого типа относительно  $g$ , если произведение  $f(x)g(x)$  меняет знак с минуса на плюс, когда  $x$ , возрастая, проходит через  $x_0$ , и, соответственно,  $x_0$  есть корень второго типа, если  $f(x)g(x)$  меняет знак с плюса на минус. Ясно, что корни первого и второго типа являются корнями нечетной кратности ибо, в силу взаимной простоты  $f$  и  $g$ , если  $f(x_0) = 0$ , то  $g(x_0) \neq 0$ , и знак  $f(x)g(x)$  меняется, только если меняется знак  $f(x)$ , что имеет место, только если  $x_0$  есть корень нечетной кратности.

**Индексом** на промежутке  $[a, b]$  полинома  $f$ , такого, что  $f(a) \neq 0$ ,  $f(b) \neq 0$ , относительно полинома  $g$  называется разность числа корней  $f$  первого и второго типа относительно  $g$  (кратные корни считаются по одному разу, корни четной кратности оставляются без внимания).

**2. Обобщение теоремы Штурма.** Пусть для взаимно простых полиномов  $f$  и  $g$  с вещественными коэффициентами построен ряд

полиномов  $f_0 = f, f_1 = g, f_2, \dots, f_k$ , удовлетворяющий первым трем требованиям ряда Штурма на некотором промежутке  $[a, b]$ . В частности, такой ряд можно построить при помощи алгоритма Евклида с изменением знаков остатков на обратный:

$$\begin{aligned} f_0 &= f_1 g_1 - f_2, \\ f_1 &= f_2 g_2 - f_3, \\ &\dots \dots \dots \\ f_{k-2} &= f_{k-1} g_{k-1} - f_k, \\ f_k &= \text{const.} \end{aligned}$$

Так построенный ряд полиномов будем по-прежнему называть *рядом Штурма*.

**Теорема.** Допустим, что  $f(x)$  не обращается в нуль на концах промежутка  $[a, b]$ . Разность числа перемен знаков в значениях полиномов ряда Штурма в начале и в конце промежутка равна индексу полинома  $f$  относительно полинома  $g$ .

**Доказательство.** Ясно, что так же, как при доказательстве теоремы п. 2 § 3, возможное изменение знаков промежуточных полиномов ряда не влечет за собой изменение числа перемен знаков. Оно может произойти только за счет пары полиномов  $f_0, f_1$ . Здесь могут представиться четыре случая:

	$f_0$	$f_1$	$f_0$	$f_1$	$f_0$	$f_1$	$f_0$	$f_1$
$x < x_0$	$-\sigma$	$\sigma$	$\sigma$	$\sigma$	$\sigma$	$\sigma$	$-\sigma$	$\sigma$
$x = x_0$	0	$\sigma$	0	$\sigma$	0	$\sigma$	0	$\sigma$
$x > x_0$	$\sigma$	$\sigma$	$-\sigma$	$\sigma$	$\sigma$	$\sigma$	$-\sigma$	$\sigma$

В первом случае  $x_0$  есть корень первого типа, а число перемен знаков уменьшается на единицу. Во втором  $x_0$  есть корень второго типа, и число перемен знаков увеличивается на единицу. В третьем и четвертом случаях  $x_0$  есть корень четной кратности, а число перемен знаков не изменяется. Следовательно, пока  $x$  переходит от  $a$  к  $b$ , число перемен знаков уменьшается на столько единиц, сколько имеется в промежутке корней первого типа, и увеличивается на столько единиц, сколько есть корней второго типа. Таким образом, разность числа перемен знаков в начале и в конце промежутка равна индексу  $f$  относительно  $g$ .

**3. Полиномы с разделяющимися корнями.** Пусть имеется последовательность полиномов  $p_0, p_1, \dots, p_n$ , степени которых равны, соответственно  $0, 1, \dots, n$ , старшие коэффициенты положительны, и имеются трехчленные соотношения:

$$p_k(x) = (\alpha_k x + \beta_k) p_{k-1}(x) - \gamma_k p_{k-2}(x) \quad \text{при} \quad \gamma_k > 0,$$

$k = 2, 3, \dots, n$ . Соотношения эти показывают, что полиномы  $p_n, p_{n-1}, \dots, p_0$  составляют ряд Штурма, полученный исходя из

$f_0 = p_n$  и  $f_1 = p_{n-1}$  посредством алгоритма Евклида, причем алгоритм Евклида протекает «без вырождения», т. е. степень каждого последующего остатка на единицу меньше степени предыдущего.

Распределение знаков, очевидно, дается следующей таблицей:

	$p_n$	$p_{n-1}$	$\dots$	$p_1$	$p_0$
$-\infty$	$(-1)^n$	$(-1)^{n-1}$	$\dots$	$-$	$+$
$+\infty$	$+$	$+$	$\dots$	$+$	$+$

так что число перемен знаков при  $-\infty$  равно  $n$  и при  $+\infty$  равно 0. Это значит, что все корни полинома  $p_n$  вещественны и все первого типа по отношению к  $p_{n-1}$ . Последнее значит, что произведение  $p_n p_{n-1}$  меняет знак с минуса на плюс каждый раз, когда  $x$ , возрастающая, проходит через корень полинома  $p_n$ . Следовательно, между соседними корнями  $p_n$  произведение  $p_n p_{n-1}$  должно изменить знак с плюса на минус, что возможно только при переходе через корень  $p_{n-1}$ . Таким образом, между соседними корнями полинома  $p_n$  имеется корень полинома  $p_{n-1}$ . Так как число корней полинома  $p_{n-1}$  равно  $n-1$  и число интервалов между соседними корнями полинома  $p_n$  тоже равно  $n-1$ , в каждом таком интервале лежит только один корень полинома  $p_{n-1}$ . Про такое расположение корней двух полиномов говорят, что корни *разделяются*.

Из сказанного ясно также, что корни всех полиномов  $p_1, p_2, \dots$  вещественны и корни соседних полиномов разделяются.

Интересно заметить, что установленная связь между свойствами ряда Штурма для пары полиномов и тем, что их корни вещественны и разделяются, обратима. Именно, если имеются два полинома  $f_0$  и  $f_1$  степеней  $n$  и  $n-1$  соответственно, с положительными старшими коэффициентами и с вещественными разделяющимися корнями, то алгоритм Евклида для построения ряда Штурма проходит без вырождения, так что все неполные частные имеют первую степень и старшие коэффициенты всех полиномов ряда Штурма положительные. Действительно, пусть  $x_1, x_2, \dots, x_n$  — корни полинома  $f_0$ , а  $\xi_1, \dots, \xi_{n-1}$  — корни полинома  $f_1$ , причем

$$x_1 < \xi_1 < x_2 < \dots < x_{n-1} < \xi_{n-1} < x_n.$$

Для полинома  $f_0 f_1$  степени  $2n-1$  числа  $x_1, \xi_1, x_2, \dots, \xi_{n-1}, x_n$  будут корнями, причем простыми, ибо их число равно степени полинома. Поэтому  $f_0 f_1$  меняет знак каждый раз, когда  $x$  проходит через эти корни. При достаточно больших по модулю отрицательных значениях  $x$  полином  $f_0 f_1$  принимает отрицательные значения. Поэтому первая перемена знака, когда  $x$  проходит через  $x_1$ , будет с минуса на плюс. Следующая, при переходе через  $\xi_1$ , будет с плюса на минус и т. д. Таким образом, при переходе через все корни  $x_1, \dots, x_n$  полинома  $f_0$  полином  $f_0 f_1$  меняет знак с минуса на плюс, так что все корни  $f_0$  имеют первый тип по отношению к  $f_1$ . Следовательно, разность числа перемен знаков в значениях ряда

Штурма, построенного исходя из  $f_0$  и  $f_1$  при помощи алгоритма Евклида, при  $-\infty$  и  $+\infty$  равна  $n$ , что возможно только в случае, если алгоритм проходит без вырождения и старшие коэффициенты всех полиномов ряда Штурма положительны.

**4. Число корней полинома в полуплоскости.** В теории дифференциальных уравнений и в ее приложениях важную роль играет распределение корней полинома в левой и правой полуплоскостях плоскости комплексной переменной  $z$ . Технически удобнее исследовать этот вопрос для верхней и нижней полуплоскости; первая задача сводится ко второй посредством замены  $z = iu$ .

Пусть  $f(z) = a_0 z^n + (a_1 + b_1 i) z^{n-1} + \dots + a_n + b_n i$  — полином с вещественными  $a_i$  и  $b_i$ ,  $a_0 > 0$ . Положим

$$g(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \quad \text{и} \quad h(x) = b_1 x^{n-1} + \dots + b_n.$$

Будем считать, что  $f(z)$  не имеет вещественных корней. Это равносильно тому, что  $g(x)$  и  $h(x)$  не имеют общих вещественных корней, так что если они не взаимно просты, то их наибольший общий делитель не имеет вещественных корней и, следовательно, не меняет знак при изменении  $x$  по всей вещественной оси.

Пусть  $x$  двигается по всей вещественной оси от  $-\infty$  к  $+\infty$ . Тогда  $f(x) = g(x) + ih(x)$  будет описывать некоторую непрерывную линию на плоскости, не проходящую через начало координат.

При  $x \rightarrow +\infty$  и  $x \rightarrow -\infty$   $\operatorname{tg} \arg f(x) = \frac{h(x)}{g(x)} \rightarrow 0$ , так что аргумент  $f(x)$  при  $x \rightarrow +\infty$  и  $x \rightarrow -\infty$  стремится к целому кратному  $\pi$ , и приращение аргумента  $f(x)$  при прохождении  $x$  по всех вещественной оси равно целому кратному  $\pi$ . Это значит, что линия, по которой перемещается  $f(x)$ , совершает целое число полуоборотов вокруг начала координат.

Разложим  $f(z)$  на линейные множители над  $\mathbb{C}$ :

$$f(z) = a_0 (z - z_1) (z - z_2) \dots (z - z_n).$$

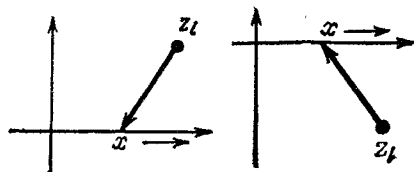


Рис. 15.

Все  $z_i$  лежат или выше, или ниже вещественной оси. Ясно, что  $\Delta \arg(x - z_i) = 0 - (-\pi) = \pi$ , если  $z_i$  выше вещественной оси, и  $\Delta \arg(x - z_i) = 0 - \pi = -\pi$ , если  $z_i$  ниже вещественной оси (см. рис. 15). Следовательно,  $\Delta \arg f(x) = \pi(n_1 - n_2)$ , где  $n_1$  — число корней  $f(z)$  в верхней полуплоскости,  $n_2$  — в нижней (с учетом кратностей).

Число полуоборотов  $\frac{1}{n} \Delta \arg f(x)$  можно подсчитать при помощи следующих геометрически наглядных соображений. Кривая, по которой перемещается  $f(x)$ , при каждом полуобороте должна пересекать ось ординат. Это будет происходить каждый раз, когда

$x$  проходит через корень нечетной кратности полинома  $g(x)$ . Линия, изображающая  $f(x)$ , может пересекать ось ординат в положительном направлении, переходя из первой четверти во вторую или из третьей в четвертую, или в отрицательном направлении (из второй четверти в первую или из четвертой в третью; рис. 16). Интуитивно ясно, что число полуоборотов вокруг начала равно разности числа положительных пересечений линии  $f(x)$  с осью ординат и числа отрицательных пересечений (в предположении, что число полуоборотов в отрицательном направлении считается отрицательным числом).

Более подробно это можно пояснить следующим образом. С вектором из начала координат в  $f(x)$  свяжем вектор единичной длины того же направления, его конец будет перемещаться по единичной окружности. Приращение аргумента  $f(x)$ , разумеется, равно приращению аргумента соответствующего единичного вектора. Ясно, что если единичный вектор проходит некоторую дугу окружности и затем возвращается обратно, то такое перемещение можно исключить без изменения суммарного приращения аргумента.

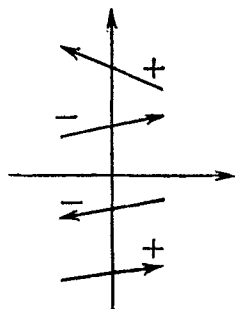


Рис. 16.

Пометим последовательные пересечения точкой  $f(x)$  оси ординат последовательностью знаков  $+$  и  $-$ , в соответствии с направлением этого пересечения. Пусть в получившейся записи окажутся рядом  $+$  и  $-$ . Это значит, что  $f(x)$  перешел из первой четверти во вторую (или из третьей в четвертую) и возвратился из второй четверти в первую (соответственно, из четвертой в третью), ибо попасть в противоположную четверть, не пересекая оси ординат,  $f(x)$  не может. Соответствующий единичный вектор тоже идет вспять, и часть пути, содержащую обе точки пересечения, можно исключить. Аналогично можно исключить последовательность  $-+$ . После таких преобразований мы придем к движению, в котором все пересечения имеют один и тот же знак, и их число (с учетом знаков) равно разности числа положительных и числа отрицательных пересечений. Но если все пересечения имеют одинаковое направление, то их число, очевидно, равно числу полуоборотов в том же направлении.

Если имеет место при  $x = x_0$  положительное пересечение линии  $f(x)$  с осью ординат, то либо  $h(x_0) > 0$  и  $g(x)$  меняет знак с плюса на минус, либо  $h(x_0) < 0$  и  $g(x)$  меняет знак с минуса на плюс. В обоих случаях  $g(x)h(x)$  меняет знак с минуса на плюс, т. е.  $x_0$  является корнем  $g(x)$  второго типа. Соответственно, если при  $x = x_0$  имеет место отрицательное пересечение, то  $x_0$  является корнем  $g(x)$  первого типа относительно  $h(x)$ .

Сопоставляя все сказанное, получим, что разность  $n_1 - n_2$  числа корней  $f(x)$  в верхней и нижней полуплоскостях равно взятому со

знаком минус индексу полинома  $g(x)$  относительно  $h(x)$  на всей прямой  $(-\infty, +\infty)$ .

Определить индекс можно при помощи ряда Штурма, составленного посредством алгоритма Евклида. Если окажется, что  $g$  и  $h$  не взаимно просты, то за последний полином ряда следует взять наибольший общий делитель  $g$  и  $h$ , который не имеет вещественных корней и, следовательно, не меняет знака при  $-\infty < x < +\infty$ .

**Пример 1.**  $g(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{R}[x]$ ,  $a_0 > 0$ , и  $g(x)$  не имеет кратных корней. Рассмотрим полином  $f(z) = g(z) + i\lambda g'(z)$ , где  $\lambda$  — вещественный параметр, и выясним расположение его корней.

Пусть  $g$  имеет  $s$  вещественных корней и  $t$  пар сопряженных комплексных, так что  $s + 2t = n$ . Пусть  $\lambda > 0$ . Ясно, что индекс  $g(x)$  относительно  $\lambda g'(x)$  такой же, как относительно  $g'(x)$ . Все вещественные корни  $g(x)$  являются корнями первого типа относительно  $g'(x)$ , так что индекс  $g$  относительно  $g'$  равен  $s$ . Следовательно,  $n_1 - n_2 = -s$ , где  $n_1$  и  $n_2$  — число корней полинома  $f(z)$  в верхней и нижней плоскости. Вместе с  $n_1 + n_2 = n = s + 2t$  это дает  $n_1 = t$  и  $n_2 = s + t$ . При  $\lambda < 0$  получим  $n_1 = s + t$  и  $n_2 = t$ .

При непрерывном изменении  $\lambda$  корни  $f(z)$  меняются непрерывно, и их пути не пересекают вещественную ось при  $\lambda \neq 0$ , поэтому они только при переходе  $\lambda$  через 0 могут переходить из верхней полуплоскости в нижнюю и обратно. При этом  $t$  корней  $g(z)$  (т. е. корни  $f(z)$  при  $\lambda = 0$ ), лежащих в верхней полуплоскости, при изменении  $\lambda$  будут оставаться в верхней полуплоскости,  $t$  корней, лежащих в нижней полуплоскости, останутся в нижней. Что касается  $s$  вещественных корней  $g(z)$ , то при  $\lambda > 0$  они опустятся вниз, а при  $\lambda < 0$  поднимутся вверх.

**Пример 2.** Узнать, сколько корней в левой полуплоскости имеет полином  $f(z) = z^3 + 2z^2 + 4z + 2$ .

Сделав замену  $z = iu$  и умножив на  $-i$ , придем к полиному  $\varphi(u) = u^3 - 2iu^2 - 4u + 2i = u^3 - 4u + i(-2u^2 + 2)$ , который имеет в верхней полуплоскости столько же корней, сколько  $f(z)$  имеет в левой полуплоскости. Применяя алгоритм Евклида к  $u^3 - 4u$  и  $-2u^2 + 2$ , построим для них ряд Штурма:  $u^3 - 4u$ ,  $-u^2 + 1$ ,  $u$ ,  $-1$ . Получаем, что индекс  $u^3 - 4u$  относительно  $-2u^2 + 2$  на промежутке  $(-\infty, +\infty)$  равен  $-3$ . Значит, все три корня полинома  $\varphi(u)$  лежат в верхней полуплоскости и, следовательно, все корни  $f(z)$  находятся в левой полуплоскости.

## § 5. Приближенное вычисление корней полинома

**1. Метод десятичных испытаний.** Допустим, что мы нашли интервал  $(c, c + 1)$ ,  $c \in \mathbb{Z}$ , в котором находится один простой корень полинома  $f(x) \in \mathbb{R}[x]$ . Значения полинома на концах интервала имеют разные знаки. Разделим интервал на 10 равных частей и

выберем ту часть, в которой находится корень. Эта часть характеризуется тем, что  $f(x)$  на ее концах имеет разные знаки. Этот интервал снова разделим на 10 частей и выберем ту часть, в которой находится корень. После этого шага процесса мы получим корень с точностью до  $10^{-2}$ , но можно продолжить процесс дальше для достижения большей точности.

При фактических вычислениях можно увеличивать на каждом шагу интервал в 10 раз. В этом варианте процесс выглядит так. Пусть корень  $x_1$  полинома  $f(x) = a_0x^n + \dots + a_n$  находится в интервале  $(c, c+1)$ . Разложим  $f(x)$  по степеням  $x-c$ :  $f(x) = b_0(x-c)^n + b_1(x-c)^{n-1} + \dots + b_n$ , что делается по схеме Хорнера, и перейдем к полиному  $f_1(y) = 10^n f(x)$  после замены  $x-c = y/10$ . Этот полином имеет корень в интервале  $(0, 10)$ ; заключаем его между  $c_1$  и  $c_1+1$  и повторяем процесс. После двух шагов получаем:  $x_1 = c + \frac{c_1}{10} + \frac{z}{100}$  и  $c_2 < z < c_2 + 1$ , так что корень известен с точностью до  $10^{-2}$ .

Пример. Легко видеть, что полином  $f(x) = x^3 - x - 1$  имеет только один вещественный корень, и он заключен в интервале  $(1, 2)$ . Вычислить корень этого полинома с точностью до  $10^{-2}$ .

Разложим  $f(x)$  по степеням  $x-1$ . Получим по схеме Хорнера  $f(x) = (x-1)^3 + 3(x-1)^2 + 2(x-1) - 1$ . Заменяем  $x = 1 + \frac{y}{10}$  и умножим на  $10^3$ . Получим  $f_1(y) = y^3 + 30y^2 + 200y - 1000$ . Посредством проб получим, что  $3 < y_1 < 4$ . Разлагаем  $f_1(y)$  по степеням  $y-3$ . Получим  $f_1(y) = (y-3)^3 + 39(y-3)^2 + 407(y-3) - 103$ . После замены  $y = 3 + \frac{z}{10}$  и умножения на  $10^3$  получим  $f_2(z) = z^3 + 390z^2 + 40700z - 103000$ , откуда найдем для корня:  $2 < z_1 < 3$ . Итак, мы получили  $1,32 < x < 1,33$ .

Описанный метод удобен для вычисления с невысокой точностью корней полинома небольшой степени с небольшими коэффициентами. Его недостаток — быстрый рост коэффициентов от шага к шагу.

**2. Метод непрерывных дробей.** Пусть для полинома  $f(x)$  снова известно, что он имеет один простой корень  $x_1$  в интервале  $(c, c+1)$ . Разложим  $f(x)$  по степеням  $x-c$ :  $f(x) = b_0(x-c)^n + \dots + b_n$ . Мы знаем, что  $x_1 - c$  лежит в интервале  $(0, 1)$ . Сделаем инверсию этого интервала посредством замены  $x-c = 1/y$  и умножим на  $y^n$ . Получим  $y^n f(x) = b_n y^n + \dots + b_0$ . На этом этапе коэффициенты не изменяются, но только записываются в обратном порядке. Корень  $y_1$  построенного полинома лежит в интервале  $(1, +\infty)$ . Заключим его между двумя соседними целыми числами,  $c_1 < y_1 < c_1 + 1$ , и повторим процесс. Пусть  $y_1 = c_1 + \frac{1}{z_1}$ ,  $c_2 < z_1 < c_2 + 1$ ,  $z_1 = c_2 + \frac{1}{t_1}$  и  $c_3 < t_1 < c_3 + 1$ . Тогда для корня

$x_1$  будет

$$x_1 = c + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{t_1}}},$$

причем известно, что  $c_3 < t_1 < c_3 + 1$ . Заменяя  $t_1$  на  $c_3$  и  $c_3 + 1$  и учитывая характер изменения  $x$  при этих заменах (заменяя  $t_1$  на  $c_3$ , мы увеличиваем  $\frac{1}{t_1}$ , уменьшаем  $\frac{1}{c_2 + \frac{1}{t_1}}$  и увеличиваем  $x_1$ ;

заменяя  $t_1$  на  $c_3 + 1$ , мы уменьшаем  $x_1$ ), получим границы для  $x_1$ :

$$c + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{c_3 + 1}}} < x_1 < c + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{c_3}}}.$$

Выражения, которые здесь участвуют, носят название непрерывных дробей.

Пример. Применим метод непрерывных дробей к уточнению значения корня полинома  $x^3 - x - 1$ ,  $1 < x_1 < 2$ .

Разложим полином по степеням  $x - 1$ . Получим  $(x - 1)^3 + 3(x - 1)^2 + 2(x - 1) - 1$ . Теперь делаем замену  $x - 1 = 1/y$  и умножаем на  $-y^3$ . Получим  $y^3 - 2y^2 - 3y - 1$ . Корень этого полинома заключен в интервале  $(3, 4)$ . Разложение по степеням  $(y - 3)$  дает  $(y - 3)^3 + 7(y - 3)^2 + 12(y - 3) - 1$ . Замена  $y - 3 = 1/z$  и умножение на  $-z^3$  дает  $z^3 - 12z^2 - 7z - 1$ . Корень этого полинома, очевидно, больше 12 и, как легко видеть, меньше 13. Разложение по степеням  $z - 12$  дает  $(z - 12)^3 + 24(z - 12)^2 + 137(z - 12) - 85$ , после замены  $z - 12 = 1/t$  и умножения на  $-t^3$  получим  $35t^3 - 137t^2 - 24t - 1$  и для корня  $t_1$  этого полинома  $1 < t_1 < 2$ . Итак:

$$x_1 = 1 + \frac{1}{3 + \frac{1}{12 + \frac{1}{t_1}}}, \quad \text{где } 1 < t_1 < 2.$$

Отсюда получаем границы для  $x_1$ :

$$1 + \frac{1}{3 + \frac{1}{12 + \frac{1}{2}}} < x_1 < 1 + \frac{1}{3 + \frac{1}{12 + \frac{1}{1}}},$$

т. е.  $1 \frac{25}{77} < x_1 < 1 \frac{13}{40}$ .

Границы эти довольно тесные. Действительно,

$$1 \frac{13}{40} - 1 \frac{25}{77} = \frac{1}{3080}.$$

Таким образом,  $1 \frac{13}{40} = 1,325$  есть приближение к корню с избытком и отличается от корня меньше чем на 0,00033. Можно доказать, что разность таким образом построенных приближений всегда равна 1, деленной на произведение знаменателей.

Приведем еще один пример, чтобы показать одно интересное явление. Вычислим  $\sqrt{2}$  как корень полинома  $x^2 - 2$ , лежащий в интервале (1, 2). Разложим полином по степеням  $x - 1$  и сделаем замену  $x - 1 = 1/y$ . После умножения на  $-y^2$  получим полином  $y^2 - 2y - 1$ . Этот полином имеет корень в интервале (2, 3). Разложение по степеням  $y - 2$  и замена  $y - 2 = 1/z$  дают, после умножения на  $-z^2$ ,  $z^2 - 2z - 1$ . Мы получили для  $y$  и  $z$  полиномы с одинаковыми коэффициентами и нас интересуют корни из одного и того же интервала (2, 3). Следовательно, процесс будет далее повторяться без изменения, так что

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}}$$

Периодичность при разложении в непрерывную дробь имеет место для всех квадратичных иррациональностей, т. е. для чисел вида  $\frac{a + \sqrt{d}}{b}$  при целых  $a, b, d$ , причем  $d > 0$  и  $d$  не является квадратом целого числа. Это явление было обнаружено и доказано еще Эйлером.

Читателю, у которого еще сохранилось любопытство, рекомендуем найти несколько приближений к  $\sqrt[3]{6}$ . Здесь, конечно, периодичности не будет, но на 6-м шагу произойдет неожиданное событие.

**3. Способ Ньютона.** Этот способ основан на «основном принципе дифференциального исчисления», который, в нестрогих терминах, заключается в том, что график всякой «приличной» функции на малом промежутке изменения независимой переменной мало отличается от прямой, именно, касательной в одной из точек. Пусть  $c$  — корень дважды дифференцируемой функции и  $x_0$  — достаточно хорошее приближение к корню. Тогда имеет место приближенное равенство

$$f(x) = f(x_0) + f'(x_0)(x - x_0)$$

для всех  $x$ , достаточно близких к  $x_0$ . Полагая  $x = c$ , получим

$$0 = f(c) = f(x_0) + f'(x_0)(c - x_0),$$

откуда для  $c$  получаем приближенное значение

$$c \approx x_0 - \frac{f(x_0)}{f'(x_0)} = x_1.$$

Вообще говоря,  $x_1$  должно быть лучшим приближением к  $c$ , чем исходное приближение  $x_0$ .

По приближению  $x_1$  мы можем найти приближение  $x_2$  по формуле  $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)}$  и т. д. Если последовательность  $x_1, x_2, \dots$  сходится, то она сходится к корню полинома  $f$ . Действительно, пусть  $x_k \rightarrow \alpha$  при  $k \rightarrow \infty$ . Переходя к пределу в равенстве  $x_k = x_{k-1} - \frac{f(x_{k-1})}{f'(x_{k-1})}$ , получим  $\alpha = \alpha - \frac{f(\alpha)}{f'(\alpha)}$ , откуда  $f(\alpha) = 0$ .

Для того чтобы выяснить, насколько близко к  $c$  должно подходить исходное приближение  $x_0$ , произведем оценку, учитывая погрешность исходного приближенного равенства, для чего рассмотрим формулу Тейлора с остаточным членом в интегральной форме:

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + \int_{x_0}^x f''(\xi)(x - \xi) d\xi,$$

или, после подстановки в интеграле  $\xi = x - t(x - x_0)$ ,

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + (x - x_0)^2 \int_0^1 f''(x - t(x - x_0))t dt.$$

Положив  $x = c$ , получим

$$0 = f(c) = f(x_0) + (c - x_0)f'(x_0) + (c - x_0)^2 \int_0^1 f''(c - t(c - x_0))t dt.$$

Поделим это равенство на  $f'(x_0)$  и перенесем первые два члена в левую часть. Получим

$$x_0 - c - \frac{f(x_0)}{f'(x_0)} = \frac{(c - x_0)^2}{f'(x_0)} \int_0^1 f''(c - t(c - x_0))t dt.$$

В левой части выражение  $x_0 - \frac{f(x_0)}{f'(x_0)}$  равно приближению  $x_1$ . Итак,

$$x_1 - c = \frac{(c - x_0)^2}{f'(x_0)} \int_0^1 f''(c - t(c - x_0))t dt.$$

Пусть  $x_0$  выбирается в окрестности точки  $c$ , и в этой окрестности модуль  $f'(x)$  ограничен снизу числом  $m$  и модуль  $f''(x)$

ограничен сверху числом  $M$ . Тогда

$$|x_1 - c| \leq \frac{|x_0 - c|^2}{m} M \int_0^1 t \, dt = \frac{M}{2m} |x_0 - c|^2.$$

Умножив на  $\frac{M}{2m}$ , получим

$$\frac{M}{2m} |x_1 - c| \leq \left( \frac{M}{2m} |x_0 - c| \right)^2.$$

Поэтому, если  $\frac{M}{2m} |x_0 - c| \leq q < 1$ , то  $\frac{M}{2m} |x_1 - c| \leq q^2$ . Для дальнейших приближений  $\frac{M}{2m} |x_2 - c| \leq q^4$ , ...,  $\frac{M}{2m} |x_k - c| \leq q^{2^k}$ .

Таким образом, в этом предположении имеет место быстрая сходимость приближений к корню  $c$ . Такого рода сходимость, когда погрешность приближения равна по порядку квадрату погрешности предыдущего приближения, носит название квадратичной сходимости.

Для полиномов все проведенные выше рассуждения имеют силу не только для вычисления вещественных корней полиномов с вещественными коэффициентами, но и для комплексных корней полиномов с комплексными коэффициентами.

Для вещественных функций имеются ситуации, когда нет необходимости выбирать начальное приближение очень близко к корню. Пусть на интервале  $(a, b)$  первая и вторая производные функции  $f$  не меняют знак, а значения  $f$  на концах интервала имеют противоположные знаки. В этих предположениях функция  $f$  имеет на интервале единственный корень  $c$ .

Допустим, для определенности, что  $f'$  и  $f''$  положительны на интервале  $(a, b)$ . Это значит, что  $f$  возрастает и выпуклость ее графика направлена вниз (рис. 17).

Возьмем начальное приближение  $x_0$  справа от корня (например,  $x_0 = b$ ). Геометрически очевидно, что следующее приближение  $x_1$  будет ближе к  $c$  чем  $x_0$  и останется справа от  $c$ . Подтвердим это вычислением:

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}.$$

В силу возрастания  $f$  заключаем, что  $f(x_0) > 0$ , но и  $f'(x_0) > 0$  по условию, следовательно,  $x_1 < x_0$ . Далее,

$$x_1 - c = \frac{(c - x_0)^2}{f'(x_0)} \int_0^1 f''(c - t(c - x_0)) t \, dt > 0,$$

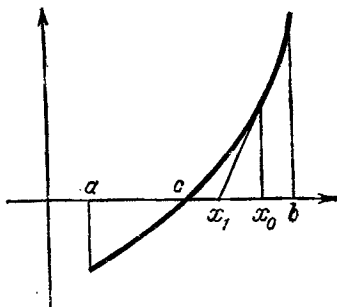


Рис. 17.

ибо  $c \leq c - t(c - x_0) \leq x_0$ , а  $f''$  положительна на всем интервале  $(a, b)$ .

Вычисляя далее последовательные приближения  $x_2, x_3, \dots$ , мы получим убывающую последовательность, ограниченную снизу

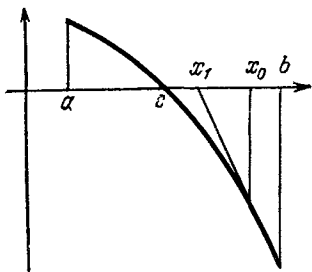


Рис. 18.

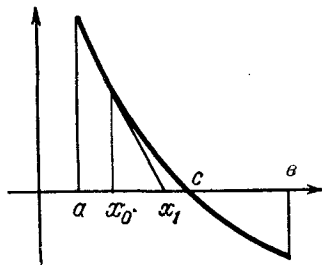


Рис. 19.

числом  $c$ . Она сходится и, как мы видели выше, сходится к корню  $f$ , который на промежутке  $(a, b)$  только один, именно,  $c$ .

Легко видеть, что если  $f'$  и  $f''$  отрицательны на промежутке  $(a, b)$ , то начинать приближения тоже следует справа от корня (рис. 18). Если же  $f'$  и  $f''$  сохраняют на  $(a, b)$  противоположные знаки, то приближения следует начинать слева (рис. 19, 20).

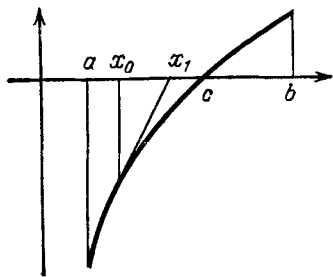


Рис. 20.

Пример 1. Найти приближения к  $\sqrt{2}$ , т. е. к положительному корню полинома  $f = x^2 - 2$ .

Здесь  $f' = 2x$ ,  $f'' = 2$ , так что  $f'$  и  $f''$  положительны на  $(0, +\infty)$ . В качестве начального приближения можно взять любое число, большее  $\sqrt{2}$ . В качестве  $m$  можно взять 2,8, а  $M = 2$ . Поэтому

$$x_k - \sqrt{2} < (x_{k-1} - \sqrt{2})^2 / 2,8.$$

В качестве  $x_0$  возьмем  $3/2$ .

Погрешность  $x_0$  не превосходит 0,1. Следующее приближение  $x_1$  равно  $17/12$ . Его погрешность не превосходит  $0,01/2,8 \approx 0,003$ . Следующее приближение  $x_2$  равно  $577/408$ . Его погрешность не превосходит  $0,003^2/2,8 \approx 0,000003$ . Разложение в десятичную дробь дает

$$577/408 = 1,414215 \dots$$

вместо  $\sqrt{2} = 1,414213 \dots$

Пример 2. Уточнить значение корня полинома  $f = x^3 - x - 1$ , зная, что  $1,3 < x < 1,4$ .

Здесь  $f' = 3x^2 - 1 > 5$ ,  $f'' = 6x < 8,4$ ,  $M/2m \approx 0,84 < 1$ . Начиная с приближения  $x_0 = 1,4$  с погрешностью меньше 0,1, мы придем к приближению  $x_1$ , погрешность которого меньше 0,01, сле-

дующее приближение  $x_2$  будет иметь погрешность меньше 0,0001, следующее  $x_3$  даст 8 верных десятичных знаков после запятой. Посмотрим, как уточняется приближение  $x_0 = 1,325 = 53/40$ , погрешность которого меньше  $1/3000$ . Для него  $x_1 = 180877/136540$  (в обыкновенных дробях). Оно приближает корень с точностью до  $1/9000000$ , т. е. с точностью до одной единицы седьмого знака после запятой. В десятичных дробях  $x_1 = 1,3247180\dots$

Метод Ньютона может применяться и к системам уравнений.

Пример. Решить приближенно систему

$$x^2 - y - 1 = 0,$$

$$y^2 - x - 2 = 0.$$

Построив графики, найдем приближенно координаты их точки пересечения при положительных  $x$  и  $y$ . Получим начальное приближение  $x_0 = 1,7$ ,  $y_0 = 2$ . При этом приближении невязка в первом уравнении равна  $-0,11$ , во втором  $0,3$ . Положим  $x = 1,7 + h$ ,  $y = 2 + k$ . После подстановки получим

$$3,4h + h^2 - k - 0,11 = 0,$$

$$-h + 4k + k^2 + 0,3 = 0.$$

Числа  $h$  и  $k$  малы. Отбросив их квадраты, получим линейную систему

$$3,4h - k - 0,11 = 0,$$

$$-h + 4k + 0,3 = 0,$$

откуда найдем приближенные значения для  $h$  и  $k$ , которые дадут следующее приближение  $(x_1, y_1)$  к  $(x, y)$ . Именно,  $h = 0,015$ ,  $k = -0,059$ , так что  $x_1 = 1,715$ ,  $y_1 = 1,941$ . Невязки этого приближения равны  $0,000225$  и  $0,52481$ , значительно меньше невязок для  $x_0, y_0$ .

ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП

§ 1. Простейшие сведения

**1. Об ассоциативности.** Пусть  $M$  — множество, в котором определена бинарная операция, сопоставляющая каждой упорядоченной паре  $a, b$  элементов из  $M$  третий элемент — их «произведение»  $ab$ . Из упорядоченной тройки  $abc$  элементов из  $M$  можно построить два произведения  $(ab)c$  и  $a(bc)$ , из четверки  $a, b, c, d$  — уже пять:  $((ab)c)d, (a(bc))d, (ab)(cd), a(b(cd))$  и  $a((bc)d)$ , из пятерки элементов — уже 14 и т. д. (Можно доказать, что число осмысленных расстановок скобок в упорядоченной совокупности из  $n$  элементов равно  $(2n-2)!/(n!(n-1)!)$ .) Ассоциативность действия означает, что оба произведения  $(ab)c$  и  $a(bc)$  тройки элементов  $a, b, c$  равны.

**Предложение 1.** Если действие в  $M$  ассоциативно, т. е.  $M$  есть полугруппа, то произведение упорядоченной совокупности  $a_1, a_2, \dots, a_n$  элементов не зависит от способа расстановки скобок, т. е. от порядка выполнения бинарных операций.

**Доказательство.** Назовем произведение  $(\dots((a_1a_2)a_3)a_4\dots)$ , в котором сомножители присоединяются последовательно по одному слева направо, левонормированным. Докажем по индукции, что произведение с любой расстановкой скобок равно левонормированному. Для  $n=3$  это верно в силу ассоциативности. Пусть  $n>3$  и уже установлена справедливость предложения для произведений из  $m$  элементов при  $m \leq n-1$ . Рассмотрим произведение  $n$  элементов  $a_1a_2 \dots a_n$  с какой-то расстановкой скобок (мы ее не пытаемся записать). Так как действие бинарно, это произведение равно произведению двух произведений  $a_1a_2 \dots a_k$  и  $a_{k+1} \dots a_n$ , с какими-то расстановками скобок. В силу индуктивного предположения оба эти сомножителя равны левонормированным произведениям. Если  $k=n-1$ , то рассматриваемое произведение равно  $(a_1a_2 \dots a_{n-1})a_n$  и получается из левонормированного произведения  $a_1a_2 \dots a_{n-1}$  присоединением справа еще одного сомножителя  $a_n$ , так что оно само левонормированно. Если же  $k < n-1$ , то

$$(a_1a_2 \dots a_k)(a_{k+1} \dots a_n) = (a_1a_2 \dots a_k)((a_{k+1} \dots a_{n-1})a_n)$$

и, в силу ассоциативности, равно  $((a_1a_2 \dots a_k)(a_{k+1} \dots a_{n-1}))a_n$ . В силу индуктивного предположения  $(a_1a_2 \dots a_k)(a_{k+1} \dots a_{n-1})$  равно левонормированному произведению  $a_1a_2 \dots a_{n-1}$ , и после

присоединения  $a_n$  получается снова левонормированное произведение. Предложение доказано.

Доказанное предложение дает возможность при записи «длинных» произведений в полугруппе не расставлять скобок, указывающих порядок выполнения бинарной операции.

В частности, произведение  $n$  равных сомножителей не зависит от способа расстановки скобок, так что имеет определенный смысл выражение  $a^n$  (или  $na$  при аддитивной записи) и  $a^m \cdot a^k = a^{m+k}$ .

**2. Аксиомы группы.** В первой главе мы определили группу как полугруппу (т. е. множество с бинарным ассоциативным действием), в которой существует нейтральный элемент  $e$  — такой, что  $ae = ea = a$  при любом  $a$ , и для любого  $a$  существует обратный элемент  $a^{-1}$  — такой, что  $a^{-1}a = aa^{-1} = e$ .

Убедимся в том, что эти аксиомы группы можно несколько ослабить.

*Предложение 2. Если в полугруппе существует левый нейтральный элемент  $e$ , т. е. такой, что  $ea = a$  при любом  $a$ , и для любого элемента  $a$  существует левый обратный  $a'$ , т. е. такой, что  $a'a = e$ , то полугруппа является группой.*

Именно эти требования были приняты в классической аксиоматике теории групп.

**Доказательство.** Докажем, что левый нейтральный элемент  $e$  является и правым нейтральным, т. е.  $ae = a$  при любом  $a$ . С этой целью рассмотрим произведение  $a''a'aa'a$ , где  $a'$  — левый обратный для  $a$ ,  $a''$  — левый обратный для  $a'$ , и подсчитаем его двумя способами. Во-первых,  $a''a'aa'a = ((a''a')a)(a'a) = (ea)e = ae$ . Во-вторых,  $a''a'aa'a = a''((a'a)a')a = a''(ea')a = a''a'a = (a''a')a = ea = a$ . Итак,  $ae = a$  при любом  $a$ .

Теперь докажем, что левый обратный  $a'$  элемента  $a$  является и правым обратным для  $a$ , т. е.  $aa' = e$ . С этой целью рассмотрим элемент  $a''a'aa'$ . Во-первых,  $a''a'aa' = ((a''a')a)a' = (ea)a' = aa'$ . Во-вторых,  $a''a'aa' = a''((a'a)a') = a''(ea') = a''a' = e$ . Итак,  $aa' = e$ , т. е.  $a'$  есть правый обратный для  $a$ .

В дальнейшем в мультипликативной записи вместо  $a'$  будем писать  $a^{-1}$ .

*Предложение 3. Если в полугруппе имеется левый нейтральный элемент  $e$  и правый нейтральный элемент  $e'$ , то они совпадают.*

Действительно,  $ee' = e'$ , так как  $e$  — левый нейтральный элемент и  $ee' = e$ , так как  $e'$  — правый нейтральный элемент.

Отсюда следует, что в условиях предложения 3 полугруппа содержит только один левый нейтральный элемент, ибо любой левый нейтральный элемент равен выбранному правому нейтральному элементу  $e'$  и, по аналогичной причине, в этих условиях полугруппа содержит единственный правый нейтральный элемент. В частности, в группе существует только один нейтральный элемент. При

использовании мультипликативной записи нейтральный элемент группы будем называть единицей группы и обозначать 1.

**Предложение 4.** В группе уравнение  $ax = b$  при данных  $a$  и  $b$  имеет единственное решение  $x = a^{-1}b$ . Уравнение  $ya = b$  имеет единственное решение  $y = ba^{-1}$ .

Действительно, положим  $x = a^{-1}b$ ; тогда  $ax = a(a^{-1}b) = b$ . Обратно, если  $ax = b$ , то  $a^{-1}ax = a^{-1}b$  и  $x = a^{-1}b$ . Этим доказано существование и единственность решения уравнения  $ax = b$ . Уравнение  $ya = b$  рассматривается аналогично.

Из предложения 4 непосредственно следует единственность обратного элемента для любого элемента группы.

Группа (полугруппа) называется *конечной*, если она состоит из конечного числа элементов. Число элементов конечной группы (полугруппы) называется ее *порядком*.

Приведем несколько примеров групп сверх тех примеров, которые приводились в § 3 гл. I. Невырожденные квадратные матрицы с вещественными элементами, очевидно, образуют группу относительно умножения. Эта группа неабелева и бесконечная. Невырожденные матрицы с элементами из конечного поля тоже образуют неабелеву группу, но эта группа конечна. Выяснение ее порядка является не очень простой задачей. Множество всех подстановок  $n$  элементов образует конечную неабелеву (при  $n > 2$ ) группу порядка  $n!$ . Эта группа называется *симметрической группой*.

**3. Умножение подмножеств группы.** Пусть  $G$  — группа,  $A$  и  $B$  — два подмножества ее элементов. *Произведением*  $AB$  этих подмножеств называется множество произведений  $ab$ , где  $a \in A$ ,  $b \in B$ . Ясно, что имеет место свойство ассоциативности  $(AB)C = A(BC)$ , ибо оба эти произведения составлены из элементов  $abc = (ab)c = a(bc)$ ,  $a \in A$ ,  $b \in B$ ,  $c \in C$ . Если одно из подмножеств состоит из одного элемента, например  $B = \{b\}$ , то произведение  $AB$  обозначается  $Ab$ , т. е. в этом контексте нет необходимости отличать элемент от составленного из него одноэлементного множества.

Введем еще одно обозначение. Через  $A^{-1}$  обозначим множество всех элементов, обратных к элементам множества  $A$ . Заметим, что  $A^{-1}$  отнюдь не является обратным к  $A$  в смысле умножения подмножеств группы.

**4. Подгруппы.** Подмножество  $H$  элементов группы  $G$  называется *подгруппой*, если оно само образует группу относительно действия в  $G$ . Из этого определения следует, что если  $a, b \in H$ , то  $ab \in H$ . Ясно, далее, что единица  $1$  является единицей  $G$ , ибо если  $ea = a$ ,  $e, a \in H$ , то  $e = aa^{-1} = 1 \in G$ . Таким образом, единица группы  $G$  принадлежит любой ее подгруппе. Ясно также, в силу единственности обратного элемента в группе, что обратный элемент для любого элемента подгруппы будет для него обратным и во всей группе.

Предложение 5. Если подмножество  $H$  элементов группы  $G$  содержит вместе с двумя элементами  $a, b$  их произведение  $ab$  и вместе с каждым элементом  $a$  его обратный  $a^{-1}$ , то  $H$  есть подгруппа  $G$ .

Действительно, надо лишь показать, что  $H$  обладает единицей. Но единица  $G$  равна  $aa^{-1}$  при  $a \in H$  и, следовательно, принадлежит  $H$  согласно условиям предложения.

5. **Классы смежности.** Множество  $Ha$ , где  $H$  — подгруппа группы  $G$  и  $a$  — некоторый элемент из  $G$ , называется *левым классом смежности* группы  $G$  по подгруппе  $H$ . Между элементами подгруппы  $H$  и элементами левого класса смежности  $Ha$  имеется естественное взаимно однозначное соответствие  $z \mapsto za = u$ ,  $u \mapsto ua^{-1} = z$ . Если подгруппа  $H$  конечна, то число элементов в каждом левом классе смежности равно порядку  $H$ .

Предложение 6. Два левых класса смежности группы  $G$  по подгруппе  $H$  либо совпадают, либо не имеют общих элементов.

Доказательство. Нужно установить, что если два левых класса смежности имеют общий элемент, то они совпадают. Пусть  $x \in Ha$  и  $x \in Hb$ . Рассмотрим класс смежности  $Hx$ . Так как  $x \in Ha$ , то  $x = za$  при некотором  $z \in H$  и  $Hx = Hza \subset Ha$ . Но  $a = z^{-1}x$ , так что  $Ha = Hz^{-1}x \subset Hx$ . Следовательно,  $Ha = Hx$ . Аналогично,  $Hb = Hx$ , так что  $Ha = Hb$ , что и требовалось доказать.

Попутно выяснилось полезное свойство:  $Ha = Hx$  при любом  $x \in Ha$ , т. е. в качестве элемента, порождающего как правый множитель класс смежности, можно взять любой элемент из этого класса.

Теорема 7. Группа является дизъюнктивным объединением левых классов смежности по подгруппе.

(Дизъюнктивное объединение — это объединение множеств, попарно не имеющих общих элементов.)

Справедливость теоремы непосредственно следует из предложения 6, ибо любой элемент группы  $a$  принадлежит некоторому классу смежности, именно,  $Ha$ , а различные классы не имеют общих элементов.

Указанное в теореме разбиение группы называется разложением группы по подгруппе.

Если число левых классов смежности в разложении  $G$  по  $H$  конечно, то это число называется *индексом* подгруппы  $H$  в группе  $G$  и обозначается  $(G : H)$ . Разумеется, если группа  $G$  конечна, то индекс любой ее подгруппы конечен.

Предложение 8. Пусть  $G \supset H \supset K$ , причем  $H$  и  $K$  — подгруппы в  $G$ . Если  $H$  в  $G$  имеет конечный индекс и  $K$  в  $H$  имеет конечный индекс, то  $K$  в  $G$  имеет конечный индекс и

$$(G : K) = (G : H)(H : K).$$

**Доказательство.** Пусть  $G = \bigcup Ha_i$ ,  $i = 1, 2, \dots, h$ , и  $H = \bigcup Kb_j$ ,  $j = 1, \dots, k$ , — разложения  $G$  по  $H$  и  $H$  по  $K$ . Тогда  $G = \bigcup Kb_j a_i$ . Нужно показать, что классы смежности  $Kb_j a_i$  попарно не имеют общих элементов. Если  $Kb_{i_1} a_{i_1}$  и  $Kb_{i_2} a_{i_2}$  содержат общий элемент, то  $Ha_{i_1}$  и  $Ha_{i_2}$  содержат общий элемент, ибо  $Kb_{j_1}$  и  $Kb_{j_2}$  содержатся в  $H$ . Следовательно,  $i_1 = i_2$ . Но тогда  $Kb_{j_1} = Kb_{j_2}$ , что возможно только при  $j_1 = j_2$ . Итак,  $G$  есть дизъюнктное объединение классов смежности  $Kb_j a_i$ . Их число равно  $hk = (G:H)(H:K)$ , т. е.  $(G:K) = (G:H)(H:K)$ .

Если подгруппа состоит только из одного единичного элемента, то классами смежности являются одноэлементные множества из элементов группы, так что индекс  $(G:1)$  равен порядку группы  $G$ .

Полагая  $K = \{1\}$  в предложении 8, получим  $(G:1) = (G:H)(H:1)$ . Это означает, что порядок конечной группы  $G$  делится на порядок ее подгруппы  $H$  и частное от их деления равно  $(G:H)$ , т. е. индексу  $H$  в  $G$ . (Эту важную теорему легко доказать непосредственно, без ссылки на предложение 8, прямо из разложения группы по подгруппе и того, что число элементов в любом классе смежности одинаково и равно порядку подгруппы.)

Наряду с левыми классами смежности можно рассматривать правые классы смежности  $aH$ , и для них тоже справедлива теорема о разложении группы по подгруппе. Между левыми и правыми классами смежности имеется естественное взаимно однозначное соответствие. Именно, отображение  $a \mapsto a^{-1}$  есть взаимно однозначное отображение группы на себя и это отображение переводит левые классы смежности в правые. Действительно, левый класс  $Ha$  состоит из элементов  $za$  при  $z \in H$  и обратные элементы  $a^{-1}z^{-1}$  заполняют правый класс смежности  $a^{-1}H$ . Поэтому если для группы  $H$  имеется конечное число левых классов смежности, то столько же будет и правых, так что определение индекса подгруппы при помощи левых или правых классов смежности дает одно и то же.

**6. Циклические группы.** Группа, составленная положительными и отрицательными степенями одного элемента  $a$ , называется *циклической группой*. Говорят, это элемент  $a$  порождает такую группу. Ясно, что элемент  $a^{-1}$  тоже можно считать порождающим. Элементы  $\dots, a^{-n}, \dots, a^{-1}, 1, a, \dots, a^n, \dots$  могут быть все попарно различны. В этом случае группа называется *бесконечной* (или *свободной*) *циклической*. Примером свободной циклической группы может служить группа целых чисел относительно сложения. Любая свободная циклическая группа ей изоморфна, изоморфизм задается соответствием  $n \mapsto a^n$ , ибо при умножении степеней элемента  $a$  показатели складываются.

Но возможно, что среди элементов циклической группы имеются равные. Если  $a^k = a^m$  при  $k > m$ , то  $a^{k-m} = 1$ , так что в этом случае некоторая степень  $a$  натуральным показателем порождает

щего элемента равна 1. Наименьший натуральный показатель, обладающий этим свойством, называется *порядком* элемента  $a$ . Если порядок равен числу  $n$ , то среди элементов  $1, a, \dots, a^{n-1}$  нет равных, ибо если бы нашлись равные, то разность показателей дала бы натуральный показатель, меньший чем  $n$ , обращающий степень  $a$  в единицу. Всякий же элемент  $a^m$  равен одному из  $1, a, \dots, a^{n-1}$ , именно,  $a^r$ , где  $r$  — остаток от деления  $m$  на  $n$ . Таким образом, порядок группы, порожденной элементом порядка  $n$ , тоже равен  $n$ .

**7. Циклические подгруппы группы.** Пусть  $G$  — данная группа. Любой ее элемент порождает некоторую циклическую подгруппу. Если  $G$  — конечная группа, то и все ее циклические подгруппы конечны. Порядок группы  $G$  делится на порядок ее любой подгруппы, в частности, на порядок любой циклической подгруппы. Этот порядок равен порядку порождающего элемента. Таким образом, верна следующая важная теорема.

**Теорема 9.** *Порядок конечной группы делится на порядок любого ее элемента.*

Пусть  $G$  — конечная группа порядка  $m$  и  $a$  — некоторый ее элемент порядка  $k$ . Тогда  $m = kl$  при целом  $l$  и  $a^m = (a^k)^l = 1$ . Следовательно, верно следующее предложение.

**Предложение 10.** *Любой элемент конечной группы при возведении в степень порядка группы дает единицу.*

Это предложение не потребовало для своего доказательства особенно глубоких соображений. Однако из него непосредственно следует такой, казалось бы, нетривиальный факт, как теорема Эйлера. Действительно, примитивные классы вычетов по модулю  $m$  образуют группу относительно умножения и порядок этой группы равен значению  $\varphi(m)$  функции Эйлера. Следовательно, для любого примитивного класса  $a$  имеет место равенство  $\bar{a}^{\varphi(m)} = \bar{1}$  или, на языке сравнений,  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Заметим, что при доказательстве теоремы Эйлера в гл. I мы использовали коммутативность умножения, в то время как в предложении 10 коммутативность группы не предполагается.

## § 2. Нормальные подгруппы и факторгруппы

**1. Определение.** Элемент  $b$  группы  $G$  называется *сопряженным* с элементом  $a$ , если существует  $c \in G$  такой, что  $b = c^{-1}ac$ .

Подгруппа  $H$  группы  $G$  называется *нормальной* (или инвариантной, или нормальным делителем группы  $G$ ), если она вместе с каждым элементом содержит все сопряженные.

В абелевой группе любая подгруппа нормальна, так как в такой группе при любых  $a$  и  $c$  будет  $c^{-1}ac = a$ .

В группе квадратных невырожденных матриц над некоторым полем множество матриц с определителем 1 образует нормальную подгруппу. Действительно, если  $\det A = 1$ , то  $\det A^{-1} = 1$ , и если

$\det B = 1$ , то  $\det AB = 1$ . Далее, при любой невырожденной  $C$  будет  $\det(C^{-1}AC) = \det A = 1$ . Группа ортогональных матриц — подгруппа в группе всех вещественных невырожденных матриц, но эта подгруппа не является нормальной, ибо, например,  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  ортогональна, но  $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -4 & -3 \end{pmatrix}$  не ортогональна.

Из определения нормальной подгруппы ясно, что нормальная подгруппа  $H$  группы  $G$  является нормальной подгруппой для любой подгруппы  $K$ , содержащей  $H$ . Действительно, если  $a \in H$  и включение  $c^{-1}ac \in H$  выполняется при всех  $c \in G$ , то оно подавно будет выполняться при всех  $c \in K$ .

## 2. Классы смежности по нормальной подгруппе и факторгруппа.

Предложение 1. Пусть  $H$  — нормальная подгруппа группы  $G$  и  $c$  — какой-либо элемент  $G$ . Тогда  $c^{-1}Hc = H$ .

Действительно, по определению нормальной подгруппы,  $c^{-1}Hc \subset H$ . Пусть теперь  $a$  — любой элемент  $H$ . Тогда  $cas^{-1} = (c^{-1})^{-1}ac^{-1} \in H$  и  $a = c^{-1}(cas^{-1})c \in c^{-1}Hc$ . Поэтому  $H \subset c^{-1}Hc$  и, следовательно,  $c^{-1}Hc = H$ .

Предложение 2. Если  $H$  — нормальная подгруппа группы  $G$  и  $c \in G$ , то  $Hc = cH$ .

Непосредственно следует из  $c^{-1}Hc = H$ . Достаточно умножить слева на  $c$ .

Предложение 3. Классы смежности по нормальной подгруппе образуют группу относительно умножения подмножеств группы. Единицей этой группы является сама нормальная подгруппа.

Доказательство. Пусть  $G$  — группа и  $H$  — ее нормальная подгруппа. Рассмотрим произведение двух классов смежности  $Ha$  и  $Hb$ , причем воспользуемся ассоциативностью умножения подмножеств и предложением 2. Имеем:  $Ha \cdot Hb = H(aH)b = H(Ha)b = (HH)ab = Hab$ . Таким образом, произведение двух классов смежности оказалось классом смежности. Ассоциативность этого умножения нам уже известна. Далее,  $H(Ha) = (HH)a = Ha$  и  $(Ha)H = H(aH) = H(Ha) = Ha$ , так что  $H$  есть единица при этом умножении. Наконец,  $(Ha^{-1})(Ha) = Ha^{-1}a = H$  и  $(Ha)(Ha^{-1}) = Haa^{-1} = H$ , так что  $Ha^{-1}$  есть обратный элемент для  $Ha$ . Предложение доказано.

Группа, образованная классами смежности группы  $G$  по нормальной подгруппе  $H$ , называется факторгруппой  $G$  по  $H$  и обозначается  $G/H$ .

Мы уже встречались с факторгруппами. Так, классы целых чисел по модулю  $m$  по отношению к действию сложения составляли факторгруппу всех целых чисел по подгруппе чисел, кратных модулю  $m$ . Аналогичная ситуация имела место в других случаях, когда мы рассматривали сравнения и классы сравнений.

Само определение факторгруппы тоже можно сформулировать в терминах сравнений. Именно, назовем два элемента  $a_1$  и  $a_2$  группы  $G$  *сравнимыми по нормальной подгруппе  $H$* , если  $a_1 a_2^{-1} \in H$  или, что то же самое,  $a_1 \in H a_2$ , т. е.  $a_1$  и  $a_2$  принадлежат к одному классу смежности по  $H$ . Тогда, если  $a_1 \equiv a_2 (H)$  и  $b_1 \equiv b_2 (H)$ , то  $a_1 b_1 \equiv a_2 b_2 (H)$ , ибо  $a_1 = z_1 a_2$ ,  $b_1 = z_2 b_2$  при  $z_1, z_2 \in H$  и  $a_1 b_1 = z_1 a_2 z_2 b_2 = z_1 (a_2 z_2 a_2^{-1}) a_2 b_2 = z_3 a_2 b_2$  при  $z_3 = z_1 (a_2 z_2 a_2^{-1}) \in H$ , т. е.  $a_1 b_1 \equiv a_2 b_2$ . Поэтому, если определить произведение классов как класс, содержащий произведение каких-либо представителей из этих классов, определение будет корректным. Оно, разумеется, совпадает с определением произведения классов смежности как элементов факторгруппы.

### § 3. Гомоморфизм

**1. Определение.** Пусть  $G$  — группа и  $S$  — другая группа (или полугруппа). Пусть каждому элементу  $a$  из  $G$  сопоставлен некоторый элемент из  $S$ , т. е. дано отображение  $G$  в  $S$ . Отображение  $\varphi$  называется *гомоморфным* или *гомоморфизмом*  $G$  в  $S$ , если произведению элементов из  $G$  соответствует произведение их образов, т. е.  $\varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2)$ , где  $\varphi(a)$  — образ  $a \in G$  при отображении  $\varphi$ . При этом, вообще говоря, не предполагается, что образы элементов  $G$  заполняют все  $S$ , и не предполагается, что различным элементам из  $G$  соответствуют обязательно различные элементы из  $S$ , т. е. при гомоморфном отображении элементам из  $G$  разрешается «склеиваться».

Предложение 1. *Гомоморфным образом  $\varphi(G)$  группы  $G$  является группа. Образом единицы группы  $G$  является единица образа и взаимно обратным элементам  $G$  соответствуют взаимно обратные образы.*

**Доказательство.** Равенство  $\varphi(ab) = \varphi(a)\varphi(b)$  означает, что произведение двух элементов из  $\varphi(G)$  принадлежит  $\varphi(G)$ . Ассоциативность следует из ассоциативности в  $G$  и  $S$ . Равенство  $\varphi(a) = \varphi(1a) = \varphi(1)\varphi(a)$  показывает, что  $\varphi(1)$  есть левая единица для  $\varphi(G)$ . Наконец,  $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1)$  показывает, что  $\varphi(a^{-1})$  есть левый обратный элемент для  $\varphi(a)$  в  $\varphi(G)$ . Этого уже достаточно (предложение 2 из § 1) для заключения, что  $\varphi(G)$  есть группа. Чтобы избежать ссылки на довольно сложно доказываемое предложение 2, достаточно было бы рассмотреть еще равенства  $\varphi(a) = \varphi(a1) = \varphi(a)\varphi(1)$  и  $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1)$ .

Заметим, что если  $S$  есть только полугруппа, а не группа, то  $\varphi(1)$  не обязана быть единицей для всей  $S$ . Однако  $\varphi(1)$  является единицей для  $\varphi(G)$  или для любой группы, содержащейся в  $S$  и содержащей  $\varphi(G)$ .

Введем еще два полезных термина. Гомоморфизм группы  $G$ , образом которого является все множество  $S$ , называется гомоморфизмом  $G$  на  $S$  («на» вместо «в») или *эпиморфизмом*. Гомоморфизм  $G$  в  $S$ , при котором различным элементам из  $G$  сопоставляются различные элементы в  $S$ , называется *мономорфизмом* или *вложением*  $G$  в  $S$ . Ясно, что при мономорфизме имеется взаимно однозначное соответствие между элементами  $G$  и их образами, сохраняющееся при умножении, так что при мономорфизме  $\varphi$  группа  $G$  и ее образ  $\varphi(G)$  изоморфны. Гомоморфизм  $G$  в  $S$ , являющийся одновременно эпиморфизмом и мономорфизмом, есть, очевидно, изоморфизм  $G$  и  $S$ .

**2. Первая теорема о гомоморфизме.** Пусть  $\varphi$  — гомоморфное отображение группы  $G$  на группу  $S$ . Множество всех элементов из  $G$ , имеющих один и тот же образ  $x \in S$ , называется *полным прообразом* элемента  $x$  и обозначается  $\varphi^{-1}(x)$  (следует помнить, что  $\varphi^{-1}(x)$  является, вообще говоря, множеством элементов  $G$ , а не одним элементом). Полный прообраз единицы группы  $S$  называется *ядром* гомоморфизма.

**Предложение 2.** *Ядро гомоморфизма  $\varphi$  группы  $G$  на группу  $S$  является нормальной подгруппой группы  $G$ .*

**Доказательство.** Введем обозначение  $H$  для ядра. Если  $a \in H$ , то  $a^{-1} \in H$ , ибо  $\varphi(a^{-1}) = (\varphi(a))^{-1} = 1$ . Если  $a \in H$  и  $b \in H$ , то  $ab \in H$ , ибо  $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$ . Наконец, если  $a \in H$  и  $c \in G$ , то  $c^{-1}ac \in H$ , ибо  $\varphi(c^{-1}ac) = \varphi(c)^{-1}\varphi(a)\varphi(c) = \varphi(c)^{-1} \cdot 1 \cdot \varphi(c) = 1$ .

**Предложение 3.** *В условиях предложения 2 полные прообразы элементов из  $S$  являются классами смежности по ядру гомоморфизма.*

**Доказательство.** Если  $a$  и  $b$  принадлежат одному классу смежности по  $H$ , то  $b = za$  при  $z \in H$ , и тогда  $\varphi(b) = \varphi(z)\varphi(a) = 1 \cdot \varphi(a) = \varphi(a)$ . Обратно, если  $\varphi(a) = \varphi(b)$ , то  $\varphi(ab^{-1}) = 1$ , так что  $ab^{-1} \in H$ ,  $a \in Hb$  и, конечно,  $b \in Hb$ .

**Теорема 4** (первая теорема о гомоморфизме). *Гомоморфный образ группы изоморфен ее факторгруппе по ядру гомоморфизма. (Формулировка этой теоремы является пугалом для неосведомленных, так как состоит практически из одних терминов.)*

**Доказательство.** Между образами при гомоморфизме и элементами факторгруппы имеется взаимно однозначное соответствие, в силу предложения 3. Оно сохраняется при умножении, ибо

$$\varphi((Ha)(Hb)) = \varphi(Ha)\varphi(Hb).$$

Естественно встает вопрос — любая ли нормальная подгруппа может быть принята за ядро гомоморфизма. Ответ положительный. Отображение группы  $G$  на факторгруппу  $G/H$  по нормальной подгруппе  $H$ , заключающееся в том, что каждому элементу группы  $G$  сопоставляется содержащий его класс смежности, есть

гомоморфизм, и его ядро совпадает с  $H$ . Это непосредственно следует из определения умножения классов смежности как элементов факторгруппы. Этот гомоморфизм  $G$  на  $G/H$  называется *естественным* гомоморфизмом. Первая теорема о гомоморфизме утверждает, что любой гомоморфизм в основном (формальнее — с точностью до изоморфизма) не отличается от естественного гомоморфизма группы на ее факторгруппу по ядру гомоморфизма.

Рассмотрим примеры.

**Пример 1.** Пусть дана циклическая группа  $G$  порядка  $n = mk$ . Пусть  $H$  — ее подгруппа, порожденная элементом  $a^k$ , где  $a$  — элемент, порождающий  $G$ . Ясно, что порядок  $a^k$  равен  $m$ , и порожденная им группа состоит из элементов  $1, a^k, a^{2k}, \dots, a^{(m-1)k}$ . Представителями смежных классов  $G$  по  $H$  могут служить  $1, a, \dots, a^{k-1}$ . Умножение смежных классов сводится к сложению показателей по модулю  $k$ , ибо  $a^k$  порождает  $H$ . Таким образом, здесь факторгруппа изоморфна циклической группе порядка  $k$ .

**Пример 2.** Пусть  $G$  — группа по умножению невырожденных квадратных матриц над полем  $P$ ,  $S$  — полугруппа элементов поля  $P$  относительно умножения и  $\phi$  — сопоставление каждой матрице из  $G$  ее определителя. Это отображение есть гомоморфизм, так как определитель произведения матриц равен произведению определителей. Здесь образ состоит из всех элементов поля  $P$ , кроме нуля, ибо любой элемент  $a$  из  $P$  есть определитель матрицы, отличающейся от единичной тем, что одна из единиц на диагонали заменена на  $a$ . Ядром отображения является группа матриц с определителем 1, так что эта группа есть нормальная подгруппа группы всех невырожденных матриц (в этом мы убедились раньше прямым подсчетом). Классы смежности по ядру составляют матрицы, имеющие один и тот же определитель.

### 3. Гомоморфные образы подгрупп.

**Предложение 5.** Пусть  $H$  и  $K$  — подгруппы группы  $G$ , причем  $H$  — нормальная подгруппа. Тогда  $HK$  является подгруппой  $G$  и  $HK = KH$ .

**Доказательство.** Пусть  $ab \in HK$ , причем  $a \in H$ ,  $b \in K$ . Тогда  $(ab)^{-1} = b^{-1}a^{-1} = (b^{-1}a^{-1}b)b^{-1}$ , причем  $b^{-1}a^{-1}b \in H$ , ибо  $H$  — нормальная подгруппа, и  $b^{-1} \in K$ . Следовательно,  $(ab)^{-1} \in HK$ . Далее, пусть  $a_1b_1$  и  $a_2b_2$  принадлежат  $HK$ , причем  $a_1$  и  $a_2$  принадлежат  $H$ ,  $b_1$  и  $b_2$  принадлежат  $K$ . Тогда  $(a_1b_1) \cdot (a_2b_2) = (a_1b_1a_2b_1^{-1})b_1b_2$ , где  $a_1b_1a_2b_1^{-1} \in H$  в силу нормальности  $H$  и  $b_1b_2 \in K$ , так что  $(a_1b_1)(a_2b_2) \in HK$ . Предложение доказано.

Заметим, что произведение двух подгрупп, из которых ни одна не является нормальной, вообще говоря, не обязано быть подгруппой. Так, если  $H$  состоит из диагональных невырожденных матриц  $\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$ , а  $K$  состоит из трех матриц:  $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ , ее квадрата  $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$  и ее куба  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , то  $HK$  состоит из матриц вида

$\begin{pmatrix} 0 & b_1 \\ -b_2 & -b_2 \end{pmatrix}$ ,  $\begin{pmatrix} -b_1 & -b_1 \\ b_2 & 0 \end{pmatrix}$  и  $\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$ . Объединение этих трех множеств матриц не образует группы, ибо при  $b_1 \neq b_2$  матрица

$$\begin{pmatrix} 0 & b_1 \\ -b_2 & -b_2 \end{pmatrix} \cdot \begin{pmatrix} -b_1 & -b_1 \\ b_2 & 0 \end{pmatrix} = \begin{pmatrix} b_1 b_2 & 0 \\ b_1 b_2 - b_2^2 & b_1 b_2 \end{pmatrix}$$

не входит в это множество.

**Теорема 6** (вторая теорема о гомоморфизме). Пусть  $H$  и  $K$  — подгруппы группы  $G$ , причем  $H$  — нормальная подгруппа. Тогда  $HK/H$  изоморфна  $K/K \cap H$ .

**Доказательство.** Рассмотрим какой-либо гомоморфизм  $\varphi$  группы  $G$  на группу  $S$  с ядром  $H$ , например, естественный гомоморфизм  $G$  на  $G/H$ . Образы элементов подгруппы  $K$  составят, очевидно, некоторую подгруппу  $P$  группы  $S$ , являющуюся гомоморфным образом  $K$  при отображении  $\varphi'$ , совпадающем с  $\varphi$  на  $K$ . Ядром отображения  $\varphi'$  является, очевидно, пересечение  $K \cap H$  группы  $K$  с ядром  $H$  гомоморфизма  $\varphi$ . Поэтому  $P$  изоморфна  $K/K \cap H$ . С другой стороны, если  $z \in P$  является образом элемента  $s \in K$ , то полный прообраз  $\varphi^{-1}(z)$  есть смежный класс  $Hs$ , и объединение всех этих прообразов есть подгруппа  $HK$  группы  $G$ . Поэтому образ  $HK$  при гомоморфизме  $\varphi$  снова совпадает с  $P$  и, так как ядро  $H$  гомоморфизма  $\varphi$  содержится в группе  $HK$ , группа  $P$  изоморфна  $HK/H$ . Отсюда уже следует, что факторгруппы  $K/K \cap H$  и  $HK/H$  изоморфны, что и требовалось доказать.

**4. Подгруппы факторгруппы.** Пусть  $H$  — нормальная подгруппа группы  $G$  и  $K$  — какая-либо промежуточная подгруппа, т. е.  $G \supset K \supset H$ . Тогда  $H$  есть нормальная подгруппа для  $K$  и факторгруппа  $K/H$  имеет смысл. Ясно, что  $K/H$  есть подгруппа группы  $G/H$ .

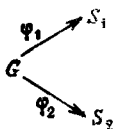
Если же задана некоторая подгруппа  $L$  факторгруппы  $G/H$ , то, «рассыпав на элементы  $G$ » классы смежности, из которых составлена  $L$  (точнее — построив объединение элементов, составляющих классы смежности, из которых состоит  $L$ ), мы получим множество  $K$  элементов группы  $G$ , которое, очевидно, будет подгруппой группы  $G$  и  $K/H = L$ . Таким образом, между подгруппами факторгруппы  $G/H$  и промежуточными между  $G$  и  $H$  подгруппами имеется естественное взаимно однозначное соответствие.

### 5. Третья теорема о гомоморфизме.

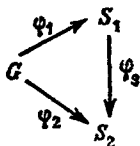
**Теорема 7.** Пусть имеются два гомоморфизма  $\varphi_1$  и  $\varphi_2$  группы  $G$  на группы  $S_1$  и  $S_2$ , причем ядро  $\varphi_2$  содержит ядро  $\varphi_1$ . Тогда существует гомоморфизм  $\varphi_3$  группы  $S_1$  на группу  $S_2$  такой, что  $\varphi_3 \varphi_1 = \varphi_2$  (т. е.  $\varphi_3(\varphi_1(a)) = \varphi_2(a)$  при любом  $a \in G$ ).

Переформулируем эту теорему в понятиях и терминах, имеющих широкое применение в некоторых разделах современной

алгебры. Изобразим эпиморфизмы  $\varphi_1$  и  $\varphi_2$  стрелками:



Получится рисунок, называющийся *диаграммой* с отображениями. В теореме утверждается, что если ядро  $\varphi_1$  содержится в ядре  $\varphi_2$ , то существует эпиморфизм  $\varphi_3$  группы  $S_1$  на  $S_2$  такой, что  $\varphi_3\varphi_1 = \varphi_2$ . В терминах диаграмм это означает, что исходную диаграмму можно замкнуть эпиморфизмом  $\varphi_3$ , т. е. перейти к диаграмме,



причем так, что получившаяся диаграмма будет *коммутативной*, т. е. при «движении» из  $G$  в  $S_2$  по стрелке  $\varphi_2$  и по составному пути, состоящему из стрелок  $\varphi_1$  и  $\varphi_3$ , будет получаться одинаковый результат.

Употребление коммутативных диаграмм очень облегчает рассуждения в ситуациях, где одновременно рассматривается много отображений (в частности, гомоморфизмов). В нашей достаточно простой ситуации в использовании языка диаграмм необходимости нет.

**Доказательство теоремы.** Возьмем любой элемент  $z \in S_1$  и любой его прообраз  $a \in G$ . Все прообразы элемента  $z$  отличаются множителями из ядра  $\varphi_1$  и, так как ядро  $\varphi_1$  содержится в ядре  $\varphi_2$ , их образы в  $S_2$  будут совпадать с  $\varphi_2(a)$ . Таким образом, мы построили отображение  $S_1$  в  $S_2$ . Обозначим его через  $\varphi_3$ , т. е. положим  $\varphi_3(z) = \varphi_2(a)$ . Ввиду того, что любой элемент  $a \in G$  является прообразом некоторого  $z = \varphi_1(a) \in S_1$ , мы видим, что  $\varphi_2(a) = \varphi_3(\varphi_1(a))$ , так что  $\varphi_3\varphi_1 = \varphi_2$ . Произведению  $z_1z_2$  элементов из  $S_1$  соответствует произведение  $a_1a_2$  их прообразов с точностью до множителей из ядра  $\varphi_1$ , содержащегося в ядре  $\varphi_2$ , так что  $\varphi_3(z_1z_2) = \varphi_2(a_1a_2) = \varphi_2(a_1)\varphi_2(a_2) = \varphi_3(z_1)\varphi_3(z_2)$ , т. е.  $\varphi_3$  есть гомоморфизм  $S_1$  в  $S_2$ . Наконец, любой элемент  $y$  из  $S_2$  есть образ  $\varphi_2(a)$  некоторого элемента из  $G$ , и  $a$ , в свою очередь, есть прообраз некоторого  $z \in S_1$ . Поэтому любой элемент  $y \in S_2$  есть  $\varphi_3(z)$  при  $z \in S_1$ , так что  $\varphi_3$  есть гомоморфизм  $S_1$  на  $S_2$ , т. е. эпиморфизм. Теорема доказана. (Рассуждения, составившие доказательство теоремы, удобно проследить на диаграмме.)

Пусть теперь  $\varphi_1$  и  $\varphi_2$  — естественные гомоморфизмы группы  $G$  на факторгруппы  $G/H_1$  и  $G/H_2$ , причем  $H_2 \supset H_1$ . Тогда  $\varphi_3$  из тео-

ремы 6 есть гомоморфизм  $G/H_1$  на  $G/H_2$ . Ясно, что его ядром является  $H_2/H_1$ . Поэтому верна следующая теорема.

**Теорема 8.** Пусть  $G \supset H_2 \supset H_1$ , где  $H_1$  и  $H_2$  — нормальные подгруппы в группе  $G$ . Тогда  $H_2/H_1$  есть нормальная подгруппа группы  $G/H_1$  и  $(G/H_1)/(H_2/H_1)$  изоморфна  $G/H_2$ .

Разумеется, теорему 8 нетрудно доказать и непосредственно, исходя из рассмотрения классов смежности, из которых составлены упомянутые в условии факторгруппы.

Теорему 7 можно рассматривать также как следующее свойство «универсальности» факторгруппы. Пусть  $H$  — нормальная подгруппа группы  $G$ . Тогда любой образ  $\bar{G}$  при гомоморфизме, при котором элементы группы  $H$  отображаются в единицу, является гомоморфным образом группы  $G/H$ . Для того чтобы в этом убедиться, достаточно положить, что  $\varphi_1$  есть естественный гомоморфизм  $G$  на  $G/H$  и  $\varphi_2$  — какой-то гомоморфизм, при котором элементы  $H$  отображаются в единицу. Тогда ядро  $\varphi_2$  содержит  $H$ , т. е. ядро  $\varphi_1$ , и по теореме 7 образ  $\varphi_2$  есть гомоморфный образ факторгруппы  $G/H$ .

**6. Наименьшая подгруппа, содержащая данное множество элементов.**

**Предложение 9.** Пусть дана группа  $G$  и некоторое множество  $S$  ее элементов. Тогда существует наименьшая подгруппа группы  $G$ , содержащая множество  $S$  (т. е. содержащаяся во всякой другой подгруппе, содержащей  $S$ ).

Мы дадим два доказательства этого предложения.

**1-е доказательство.** Из свойств, характеризующих подгруппу (предложение 5 из § 1), ясно, что пересечение любого множества подгрупп группы  $G$  есть подгруппа группы  $G$ . Рассмотрим множество всех подгрупп, содержащих  $S$ . Оно непусто, так как ему принадлежит сама группа  $G$ . Пересечение всех подгрупп этого множества является подгруппой. Она содержит  $S$  и содержится в любой подгруппе, содержащей  $S$ .

**2-е доказательство.** Рассмотрим множество  $T = S \cup S^{-1}$ . Множество  $T$  содержит  $S$  и вместе с каждым своим элементом содержит его обратный. Пусть  $H$  есть множество всех (конечных, разумеется) произведений  $a_1 a_2 \dots a_k$  элементов множества  $T$ . Ясно, что произведение двух элементов из  $H$  снова принадлежит  $H$  и элемент, обратный к элементу  $a_1 a_2 \dots a_k$  из  $H$ , тоже принадлежит  $H$ , ибо  $(a_1 a_2 \dots a_k)^{-1} = a_k^{-1} \dots a_2^{-1} a_1^{-1}$ , а множество  $T$  вместе с каждым элементом содержит обратный. Таким образом,  $H$  есть подгруппа группы  $G$ . Далее,  $H$  содержит  $S$ , ибо среди его элементов имеются все «одноэлементные произведения»  $a \in T$ , в частности, элементы из  $S$ . Наконец, любая подгруппа, содержащая  $S$ , содержит и множество обратных элементов  $S^{-1}$ , тем самым и множество  $T$  и все произведения, составленные из элементов  $T$ , т. е. всю подгруппу  $H$ .

Возможно, что наименьшая подгруппа, содержащая множество  $S$ , есть вся группа  $G$ . В этом случае говорят, что множество  $S$  порождает группу  $G$  и элементы множества  $S$  называются *порождающими*  $G$  или *образующими*. Так, циклическая группа порождается одним элементом. Нетрудно видеть, что для симметрической группы  $S_n$  всех подстановок  $n$  элементов можно взять две образующих — транспозицию  $\sigma = (1, 2)$  и круговую подстановку  $\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix}$  всех элементов. Действительно,  $\tau^{-1}\sigma\tau = (2, 3)$ ,  $\tau^{-1}(2, 3)\tau = (3, 4)$  и т. д. Таким образом, в группе, порожденной подстановками  $\sigma$  и  $\tau$ , содержатся все транспозиции соседних элементов, следовательно, и все транспозиции и все подстановки. Группа, которая порождается конечным множеством образующих, называется *конечно порожденной*. Класс конечно порожденных групп довольно обширен, и в него входят, очевидно, все конечные группы.

**7. Наименьшая нормальная подгруппа, содержащая данное множество элементов.**

**Предложение 10.** Пусть дана группа  $G$  и некоторое множество  $S$  ее элементов. Тогда существует наименьшая нормальная подгруппа группы  $G$ , содержащая множество  $S$ .

**Доказательство.** Рассмотрим множество  $T = S \cup S^{-1}$  и множество  $U$ , состоящее из всех элементов  $T$  и всех с ними сопряженных в  $G$ . Множество  $U$  содержит вместе с каждым элементом обратный и все с ним сопряженные, ибо  $(c^{-1}ac)^{-1} = c^{-1}a^{-1}c$  и  $c_2^{-1}(c_1^{-1}ac_1)c_2 = (c_1c_2)^{-1}a(c_1c_2)$ . Пусть  $H$  есть множество всех произведений  $a_1a_2 \dots a_k$  элементов множества  $U$ . Тогда  $H$  есть подгруппа группы  $G$  и, более того, нормальная подгруппа, ибо при любом  $c \in G$  будет  $c^{-1}(a_1a_2 \dots a_k)c = (c^{-1}a_1c)(c^{-1}a_2c) \dots (c^{-1}a_kc)$ . Конечно,  $H$  содержит  $S$ . Далее, каждая нормальная подгруппа, содержащая  $S$ , должна содержать все обратные элементы к элементам  $S$ , все сопряженные в  $G$  с элементами из  $S$  и с обратными к ним элементами и все их произведения, т. е. всю группу  $H$ . Таким образом,  $H$  есть наименьшая из нормальных подгрупп группы  $G$ , содержащих множество  $S$ .

Предложение 10 можно было доказать аналогично первому доказательству предложения 9. Для этого надо воспользоваться очевидным фактом, что пересечение любого множества нормальных подгрупп есть нормальная подгруппа, затем рассмотреть множество всех нормальных подгрупп, содержащих  $S$ , и взять их пересечение. Это и будет, очевидно, наименьшая из нормальных подгрупп, содержащих  $S$ .

Построенная нормальная подгруппа  $H$  обладает тем свойством, что гомоморфизм группы  $G$  с ядром  $H$  отображает все элементы из  $S$  в единицу. Более того, гомоморфизм с ядром  $H$  обладает следующим свойством универсальности: любой гомоморфный образ

группы  $G$ , в котором образами всех элементов из  $S$  является 1, есть гомоморфный образ группы  $G/H$  (т. е. образа группы  $G$  при гомоморфизме с ядром  $H$ ).

Действительно, ядро  $H_1$  гомоморфизма, при котором все элементы из  $S$  отображаются в 1, содержит  $S$ ,  $S^{-1}$  и, следовательно,  $T$ ,  $U$  и все произведения элементов из  $U$ , т. е. всю нормальную подгруппу  $H$ . Следовательно, образ  $G$  при гомоморфизме с ядром  $H_1$  есть гомоморфный образ группы  $G/H$ , в силу замечания об универсальности факторгруппы, которое было сделано в связи с теоремами 7 и 8.

**8. Коммутант группы.** Выражение  $aba^{-1}b^{-1}$ , где  $a$  и  $b$  — элементы группы  $G$ , носит название *коммутатора* элементов  $a$  и  $b$ . Пусть  $aba^{-1}b^{-1} = z$ . Тогда  $ab = zba$ , так что коммутатор  $z$  играет роль как бы поправочного множителя при перестановке элементов  $a$  и  $b$ . Поэтому для того чтобы  $a$  и  $b$  были перестановочны, необходимо и достаточно, чтобы их коммутатор был равен 1. Подмножество группы  $G$ , состоящее из всевозможных коммутаторов и их конечных произведений, носит название *коммутанта* группы  $G$ . Так как элемент, обратный к коммутатору:  $(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$  сам является коммутатором, коммутант есть подгруппа группы  $G$ , порожденная множеством коммутаторов. Далее, элемент  $c^{-1}(aba^{-1}b^{-1})c$ , сопряженный с коммутатором, есть тоже коммутатор. Действительно,  $c^{-1}(aba^{-1}b^{-1})c = (c^{-1}ac)(c^{-1}bc)(c^{-1}ac)^{-1}(c^{-1}bc)^{-1}$ . Поэтому коммутант есть нормальная группа группы  $G$ . Его принято обозначать  $[G, G]$ .

Факторгруппа группы  $G$  по коммутанту абелева. Действительно, все коммутаторы элементов группы  $G$  находятся в ядре естественного гомоморфизма группы  $G$  на факторгруппу по коммутанту и, следовательно, образы любых двух элементов группы  $G$  имеют единичный коммутатор, т. е. коммутируют.

При любом гомоморфизме  $\varphi$  группы  $G$  в абелеву группу образ является гомоморфным образом факторгруппы по коммутанту. Действительно, коммутаторы всех элементов  $G$  при гомоморфизме  $\varphi$  отображаются в 1, т. е. принадлежат ядру гомоморфизма, которое, тем самым, содержит коммутант. В силу свойства универсальности факторгруппы отсюда следует, что образ группы  $G$  при гомоморфизме  $\varphi$  есть гомоморфный образ факторгруппы по коммутанту.

**9. Центр группы.** *Центром* группы  $G$  называется множество ее элементов, каждый из которых коммутирует со всеми элементами группы  $G$ .

Пусть  $a$  принадлежит центру и  $c$  — произвольный элемент группы  $G$ . Тогда  $ac = ca$ . Умножив это равенство слева и справа на  $a^{-1}$ , получим  $ca^{-1} = a^{-1}c$ , так что  $a^{-1}$  тоже принадлежит центру. Далее, если  $a$  и  $b$  принадлежат центру, то при произвольном  $c \in G$   $abc = acb = cab$ , т. е.  $ab$  тоже принадлежит центру. Та-

ким образом, центр есть подгруппа группы  $G$ . Из равенства  $c^{-1}ac = a$  при любом  $c \in G$  следует, что центр является нормальной подгруппой группы  $G$ .

#### § 4. Прямое произведение групп

**1. Внешнее прямое произведение.** Пусть имеются две группы  $G_1$  и  $G_2$ . Рассмотрим их декартово произведение, т. е. множество пар  $\{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}$ . Введем для них «покомпонентное» умножение:  $(x_1, x_2)(y_1, y_2) \stackrel{\text{def}}{=} (x_1y_1, x_2y_2)$ . Свойство ассоциативности, очевидно, имеет место, так как оно имеет место в компонентах. Элемент  $(1, 1)$  является единицей относительно введенного умножения. Для  $(x_1, x_2)$  обратным будет, очевидно,  $(x_1^{-1}, x_2^{-1})$ . Таким образом, декартово произведение групп превращено в группу, которая называется *внешним прямым произведением* групп  $G_1$  и  $G_2$  и обозначается  $G_1 \times G_2$ .

Выясним некоторые свойства внешнего прямого произведения.

1. Множество элементов вида  $(x, 1)$  есть нормальная подгруппа группы  $G_1 \times G_2$ , изоморфная группе  $G_1$ .

То, что элементы вида  $(x_1, 1)$  образуют подгруппу, очевидно. Столь же очевиден ее изоморфизм с группой  $G_1$  в силу соответствия  $(x_1, 1) \leftrightarrow x_1$ . Подгруппу, образованную элементами вида  $(x_1, 1)$ , обозначим  $\tilde{G}_1$ .

Из цепочки равенств

$$\begin{aligned} (y_1, y_2)^{-1}(x_1, 1)(y_1, y_2) &= (y_1^{-1}, y_2^{-1})(x_1, 1)(y_1, y_2) = \\ &= (y_1^{-1}x_1y_1, y_2^{-1}1y_2) = (y_1^{-1}x_1y_1, 1) \end{aligned}$$

следует, что  $\tilde{G}_1$  — нормальная подгруппа в  $G_1 \times G_2$ .

2. Множество элементов вида  $(1, x_2)$  есть нормальная подгруппа группы  $G_1 \times G_2$ , изоморфная  $G_2$ .

Это свойство ничем, кроме обозначений, не отличается от предыдущего. Подгруппа, образованная элементами вида  $(1, x_2)$ , обозначается  $\tilde{G}_2$ .

3. Элементы из подгрупп  $\tilde{G}_1$  и  $\tilde{G}_2$ , соответственно, коммутируют при умножении.

Действительно,  $(x_1, 1)(1, x_2) = (x_1, x_2)$  и  $(1, x_2)(x_1, 1) = (x_1, x_2)$ .

4.  $\tilde{G}_1 \cap \tilde{G}_2 = 1$ . Очевидно.

5.  $\tilde{G}_1\tilde{G}_2 = G_1 \times G_2$ .

Действительно, любой элемент  $(x_1, x_2)$  из  $G_1 \times G_2$  равен  $(x_1, 1)(1, x_2)$ .

**2. Разложение группы в прямое произведение.** По большей части прямые произведения возникают при изучении конкретных классов групп.

**Предложение 1.** Пусть в группе  $G$  имеются две нормальные подгруппы  $H_1$  и  $H_2$  такие, что  $H_1 \cap H_2 = 1$ . Тогда элементы из  $H_1$  коммутируют с элементами из  $H_2$ .

**Доказательство.** Пусть  $x_1 \in H_1$  и  $x_2 \in H_2$ . Рассмотрим их коммутатор  $z = x_1 x_2 x_1^{-1} x_2^{-1}$ . При расстановке скобок  $z = x_1 (x_2 x_1^{-1} x_2^{-1})$  становится ясно, что  $z \in H_1$ , ибо первый множитель принадлежит  $H_1$  по условию, а второй принадлежит  $H_1$ , ибо  $x_1^{-1} \in H_1$  и  $H_1$  — нормальная подгруппа. Расстановка скобок  $z = (x_1 x_2 x_1^{-1}) x_2$  из аналогичных рассуждений дает  $z \in H_2$ . Но  $H_1$  и  $H_2$  имеют единственный общий элемент — единицу. Следовательно,  $x_1 x_2 x_1^{-1} x_2^{-1} = 1$  и  $x_1 x_2 = x_2 x_1$ .

**Теорема 2.** Пусть в группе  $G$  имеются две нормальные подгруппы  $H_1$  и  $H_2$  такие, что  $H_1 \cap H_2 = 1$  и  $H_1 H_2 = G$ . Тогда  $G$  изоморфна прямому произведению  $H_1$  и  $H_2$ .

**Доказательство.** Рассмотрим внешнее прямое произведение  $H_1 \times H_2$  и сопоставим каждой паре  $(x_1, x_2) \in H_1 \times H_2$  элемент  $x_1 x_2$  группы  $G$ . Это отображение гомоморфно. Действительно, произведению пар  $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$  сопоставляется элемент  $x_1 y_1 x_2 y_2 \in G$ . Но в силу предложения 1,  $y_1 x_2 = x_2 y_1$ , так что  $x_1 y_1 x_2 y_2 = x_1 x_2 y_1 y_2 = (x_1 x_2)(y_1 y_2)$ , т. е. образ произведения пар равен произведению образов. Это отображение является отображением на всю группу  $G$ , ибо  $G = H_1 H_2$ . Оно взаимно однозначно, ибо если  $x_1 x_2 = y_1 y_2$  при  $x_1, y_1 \in H_1$  и  $x_2, y_2 \in H_2$ , то  $y_1^{-1} x_1 = y_2 x_2^{-1}$ . Левая часть принадлежит  $H_1$ , правая  $H_2$ , следовательно  $y_1^{-1} x_1 = y_2 x_2^{-1} = 1$ , ибо  $H_1 \cap H_2 = 1$ , и  $x_1 = y_1$ ,  $x_2 = y_2$ . Таким образом, отображение  $(x_1, x_2) \rightarrow x_1 x_2$  оказывается действительно изоморфизмом групп  $H_1 \times H_2$  и  $G$ .

В этой ситуации говорят, что  $G$  разлагается в прямое произведение нормальных подгрупп  $H_1$  и  $H_2$ , и произведение  $H_1 H_2$  в этом случае называют *внутренним прямым произведением* нормальных подгрупп  $H_1$  и  $H_2$ .

Понятие прямого произведения естественно обобщается на произвольное конечное множество групп. Именно, (внешним) *прямым произведением* групп  $G_1, G_2, \dots, G_k$  называется множество строк  $(x_1, x_2, \dots, x_k)$  при  $x_i \in G_i$  с покомпонентным умножением:

$$(x_1, x_2, \dots, x_k)(y_1, y_2, \dots, y_k) \stackrel{\text{def}}{=} (x_1 y_1, x_2 y_2, \dots, x_k y_k).$$

Легко видеть, что это множество есть группа с единицей  $(1, 1, \dots, 1)$ . Прямое произведение обозначается  $G_1 \times G_2 \times \dots \times G_k$ .

Имеют место следующие свойства.

1. Множество элементов вида  $(1, 1, \dots, x_i, 1, \dots, 1)$  образует нормальную подгруппу группы  $G_1 \times G_2 \times \dots \times G_k$ , изоморфную группе  $G_i$ . Обозначим ее  $\tilde{G}_i$ .

2. Произведение  $\tilde{G}_1 \tilde{G}_2 \dots \tilde{G}_k$  равно  $G_1 \times G_2 \times \dots \times G_k$ .

3. Элементы групп  $\tilde{G}_i$  и  $\tilde{G}_j$  при  $i \neq j$  коммутируют.

4. Пересечение каждой группы  $\tilde{G}_i$  с произведением всех остальных  $\tilde{G}_j$ ,  $j \neq i$ , состоит только из 1.

Внутреннее прямое произведение определяется аналогично разобранному выше случаю  $k = 2$ . Именно:

**Теорема 3.** Пусть группа  $G$  имеет нормальные подгруппы  $H_1, H_2, \dots, H_k$  такие, что  $H_1 H_2 \dots H_k = G$  и при любом  $i$  пересечение подгруппы  $H_i$  с произведением  $H_1 \dots H_{i-1} H_{i+1} \dots H_k$  состоит только из 1. Тогда  $G$  изоморфна прямому произведению  $H_1 \times \dots \times H_k$ .

**Доказательство.** В силу предложения 1 элементы из разных подгрупп  $H_i$  и  $H_j$  коммутируют. Сопоставим элементу  $(x_1, x_2, \dots, x_k) \in H_1 \times H_2 \times \dots \times H_k$  элемент  $x_1 x_2 \dots x_k$ . Это отображение гомоморфно:  $x_1 x_2 \dots x_k y_1 y_2 \dots y_k = x_1 y_1 x_2 y_2 \dots x_k y_k$ , ибо элементы  $x_i$  и  $y_j$ , при  $i \neq j$ , коммутируют. Оно эпиморфно, ибо  $H_1 H_2 \dots H_k = G$ . Оно мономорфно, ибо из равенства  $x_1 \dots \dots x_{i-1} x_i x_{i+1} \dots x_k = y_1 \dots y_{i-1} y_i y_{i+1} \dots y_k$  следует, в силу коммутирования элементов из разных  $H_j$ , что  $x_i y_i^{-1} = y_1 x_1^{-1} \dots \dots y_{i-1} x_{i-1}^{-1} y_{i+1} x_{i+1}^{-1} \dots y_k x_k^{-1}$ . Левая часть принадлежит  $H_i$ , правая — произведению всех  $H_j$  при  $j \neq i$ . Поэтому обе части равны 1 и  $x_i = y_i$ , и это верно для всех  $i = 1, 2, \dots, k$ . Итак рассматриваемое отображение есть изоморфизм.

**3. Прямое произведение факторгрупп.** Пусть  $H_1, H_2, \dots, H_k$  — подгруппы групп  $G_1, G_2, \dots, G_k$ . Внешнее прямое произведение  $H_1 \times H_2 \times \dots \times H_k$  есть, очевидно, подгруппа группы  $G_1 \times G_2 \times \dots \times G_k$ . Если  $H_i$  являются нормальными подгруппами групп  $G_i$ , то  $H_1 \times H_2 \times \dots \times H_k$  есть нормальная подгруппа группы  $G_1 \times G_2 \times \dots \times G_k$ .

**Предложение 4.** Факторгруппа группы  $G_1 \times G_2 \times \dots \times G_k$  по  $H_1 \times H_2 \times \dots \times H_k$  равна  $(G_1/H_1) \times (G_2/H_2) \times \dots \times (G_k/H_k)$ .

**Доказательство.** Смежные классы группы  $G_1 \times G_2 \times \dots \times G_k$  по  $H_1 \times H_2 \times \dots \times H_k$  образованы последовательностями  $(z_1 a_1, z_2 a_2, \dots, z_k a_k)$ , где  $z_i$  пробегает  $H_i$ , а  $a_i$  — фиксированные элементы из  $G_i$ . Эти множества естественно рассматривать как последовательности классов смежности  $(H_1 a_1, H_2 a_2, \dots, H_k a_k)$ . Покомпонентное умножение элементов этих множеств сводится к покомпонентному умножению классов смежности, т. е. элементов факторгрупп  $G_i/H_i$ . Тем самым предложение доказано.

## § 5. Группы преобразований

**1. Определения.** Пусть задано некоторое множество  $M$  и группа  $G$ , «действующая» на элементы этого множества. Точнее, это значит, что определено действие (мы будем обозначать его как умножение), сопоставляющее элементу из  $M$  и элементу из  $G$  новый элемент из  $M$ . При этом требуется выполнение следующих аксиом:

1.  $m \cdot 1 = m$  при любом  $m \in M$ ; 1 обозначает единицу группы  $G$ .

2.  $m(z_1 z_2) = (m z_1) z_2$  при любых  $m \in M$ ,  $z_1$  и  $z_2$  из  $G$ .

Здесь элементы записываются как операторы, действующие на элементы из  $M$  справа. Принята также левая запись, при которой действие  $z \in G$  на  $m \in M$  записывается в форме  $zm$ . При левой записи аксиомы записываются в виде:

1.  $1 \cdot m = m$ .
2.  $(z_1 z_2) m = z_1 (z_2 m)$ .

Правая и левая записи совершенно равносильны, но в действии произведения элементов группы на  $m \in M$  имеется разница. При правой записи первым действующим является левый сомножитель, а затем действует правый. При левой записи наоборот первым действующим является правый сомножитель. В этом параграфе мы будем пользоваться правой записью. Иногда будем применять левую, и фактически это уже было сделано в другой ситуации при рассмотрении гомоморфизмов.

Множество  $M$ , на котором определено действие группы  $G$ , носит название  *$G$ -операторного множества*, или, короче,  *$G$ -множества*. Его элементы будем называть *точками*.

Пусть  $m$  — некоторый элемент из  $M$ . Множество  $mG$ , т. е. множество всех  $mz$  при  $z \in G$ , называется *орбитой*, порожденной точкой  $m$ . Точка  $m_1$ , лежащая на орбите, порожденной точкой  $m$ , порождает ту же орбиту. Действительно, пусть  $m_1 = mz_1$ . Тогда  $m_1 G = (mz_1)G = m(z_1 G) = mG$ . Таким образом, орбиты могут либо совпадать, либо не иметь общих элементов. Тем самым  $G$ -множество разбивается на орбиты. Каждая орбита, в свою очередь, является  $G$ -операторным множеством, состоящим из одной орбиты, именно, себя самой. Если  $G$ -множество  $M$  состоит из одной орбиты, то говорят, что  $G$  действует на  $M$  *транзитивно*, а само множество  $M$  называют *однородным пространством* по отношению к группе  $G$ .

Рассмотрим некоторые примеры.

**Пример 1.**  $M$  — множество точек на плоскости,  $G$  — группа векторов относительно сложения. Действие вектора на точку определяется как перенос точки на этот вектор.

Ясно, что здесь одна орбита, так что множество точек на плоскости является однородным пространством по отношению к переносам на векторы, т. е. параллельным переносам.

**Пример 2.**  $M$  — множество точек на плоскости,  $G$  — группа всех движений плоскости.

Это тоже однородное пространство.

**Пример 3.**  $M$  — множество точек на плоскости,  $G$  — группа вращений вокруг фиксированной точки  $O$ .

Здесь орбитами будут окружности с центром в  $O$  и сама точка  $O$ .

**2. Классы сопряженных элементов.** В качестве множества  $M$  возьмем саму группу  $G$  и действие элемента  $z \in G$  на элемент  $a \in G$  определим как сопряжение  $z^{-1}az$ . Здесь записывать такое действие в виде правого умножения неудобно, получится путаница

с обычным умножением в группе, поэтому оператор сопряжения поднимем в показатель, т. е. будем записывать  $z^{-1}az = a^z$ . Выполнение аксиом легко проверяется:

$$a^1 = 1^{-1}a1 = a,$$

$$a^{z_1 z_2} = z_2^{-1} z_1^{-1} a z_1 z_2 = z_2^{-1} (z_1^{-1} a z_1) z_2 = z_2^{-1} (a^{z_1}) z_2 = (a^{z_1})^{z_2}.$$

Орбиты в этой ситуации называются *классами сопряженных элементов*. Среди них имеются состоящие из одного элемента. Таков класс, порожденный единицей, ибо  $z^{-1}1z = 1$  при всех  $z$ . Такими же будут классы, составленные из каждого элемента центра, ибо если  $a$  принадлежит центру, то  $a^z = z^{-1}az = z^{-1}za = a$  при любом  $z \in G$ .

**3. Строение однородных пространств.** Рассмотрим еще один очень важный пример внутри самой теории групп.

Пусть  $G$  — группа и  $H$  — некоторая ее подгруппа. Рассмотрим множество левых классов смежности  $Ha$ , определив на этом множестве действие группы  $G$  как правое умножение на ее элементы, т. е. положив  $(Ha)z = Haz$  для  $z \in G$ . Это действие действительно переводит левые классы смежности в левые классы смежности, и выполнение аксиом  $G$ -операторного множества тривиально.

Все классы смежности составляют одну орбиту, ибо  $Ha_2 = (Ha_1)a_1^{-1}a_2$ , т. е. множество левых классов смежности образует однородное пространство по отношению к правым умножениям на элементы группы  $G$ .

Важность этого примера состоит в том, что пространство классов смежности является изоморфной моделью для любого однородного  $G$ -пространства.

Уточним сказанное.

Скажем, что  $G_1$ -операторное множество  $M_1$  и  $G_2$ -операторное множество  $M_2$  *изоморфны*, если группы  $G_1$  и  $G_2$  изоморфны и имеется взаимно однозначное соответствие между элементами  $M_1$  и  $M_2$ , сохраняющееся при применении соответствующих друг другу элементов групп  $G_1$  и  $G_2$ .

**Теорема 1.** *Любое однородное  $G$ -пространство  $M$  изоморфно пространству классов смежности по некоторой подгруппе.*

**Доказательство.** Пусть  $m_0$  — некоторая точка пространства  $M$ . Рассмотрим множество  $H$  всех элементов группы  $G$  таких, которые не изменяют  $m_0$ , т. е. таких  $z \in G$ , что  $m_0 z = m_0$ . Очевидно, что такие элементы образуют подгруппу группы  $G$ , ибо если  $m_0 z = m_0$ , то  $m_0 z z^{-1} = m_0 z^{-1}$ , т. е.  $m_0 z^{-1} = m_0$ , и если  $m_0 z_1 = m_0$  и  $m_0 z_2 = m_0$ , то  $m_0 (z_1 z_2) = (m_0 z_1) z_2 = m_0 z_2 = m_0$ . Подгруппа  $H$  называется *стабилизатором точки  $m_0$* . Возьмем теперь любую другую точку  $m_1$ . Так как  $M$  однородно, т. е. состоит из одной орбиты, найдется элемент  $x \in G$  такой, что  $m_0 x = m_1$ . Выясним, какие еще элементы преобразуют  $m_0$  в  $m_1$ . Пусть  $m_0 y = m_1$ . Тогда

$m_0xy^{-1} = m_1y^{-1} = m_0$ , так что  $xy^{-1} \in H$  и  $x \in Hy$ . Таким образом, элементы из  $G$ , одинаково преобразующие точку  $m_0$ , принадлежат одному левому классу смежности по стабилизатору. Обратно, если элементы  $x$  и  $y$  принадлежат одному левому классу смежности по стабилизатору, то  $m_0x = m_0y$ . Таким образом, между точками однородного пространства  $M$  и левыми классами смежности по стабилизатору имеется взаимно однозначное соответствие. Оно сохраняется при умножении справа на элементы  $G$ . Действительно, если  $m_1 = m_0x$ , то точке  $m_1$  соответствует класс  $Hx$ . Пусть  $m_2 = m_1y = m_0xy$ . Этой точке соответствует класс  $Hxy = (Hx)y$ . Теорема 1 доказана.

Сделаем одно замечание. Мы установили, что однородное пространство изоморфно пространству левых классов смежности по стабилизатору некоторой точки  $m_0$ , выбранной произвольно. Но у разных точек стабилизаторы различны. Почему же выбор точек  $m_0$  произволен? Для того чтобы в этом разобраться, выясним, как связаны стабилизаторы различных точек. Пусть, как и раньше, стабилизатор точки  $m_0$  обозначен  $H$ . Для любой другой точки  $m_1$  имеем  $m_1 = m_0x$  при некотором  $x \in G$ . Равенство  $m_1z = m_1$  равносильно равенствам  $m_0xz = m_0x$ ,  $m_0xzx^{-1} = m_0$ , что имеет место в том и только в том случае, если  $xzx^{-1} \in H$ , т. е.  $z \in x^{-1}Hx$ . Таким образом, стабилизатор точки  $m_1$  есть  $x^{-1}Hx$ .

Изоморфное отображение группы  $G$  на себя называется *автоморфизмом* группы. Отображение  $a \mapsto x^{-1}ax$  при фиксированном  $x \in G$  есть, очевидно, отображение  $G$  на себя, причем изоморфное, ибо  $x^{-1}a_1a_2x = (x^{-1}a_1x)(x^{-1}a_2x)$ , т. е. оно является автоморфизмом. Такой автоморфизм называется *внутренним*. При этом автоморфизме подгруппа  $H$  группы  $G$  переходит в сопряженную подгруппу  $x^{-1}Hx$ . Левый класс смежности  $Ha$  переходит во множество  $x^{-1}Hax = x^{-1}Hxx^{-1}ax$ , которое является левым классом смежности по подгруппе  $x^{-1}Hx$ , порожденным элементом  $x^{-1}ax$ . Ясно, что преобразование классов смежности по подгруппе  $H$ , вызванное умножением справа на  $z \in G$ , будет таким же, как преобразование классов смежности по подгруппе  $x^{-1}Hx$ , вызванное умножением справа на элемент  $x^{-1}zx$ . Поэтому пространство классов смежности по подгруппе  $H$  изоморфно пространству классов смежности по сопряженной подгруппе  $x^{-1}Hx$ .

Наличие такого изоморфизма может служить объяснением того, что при доказательстве теоремы 1 можно было взять точку  $m_0$  и ее стабилизатор произвольно.

**4. К теории подстановок.** Как уже говорилось, подстановками называются взаимно однозначные отображения на себя конечных множеств. Будем считать, что  $\{1, 2, \dots, n\}$  — множество, на котором действуют подстановки. Пусть  $\sigma$  — некоторая подстановка и  $1, \sigma, \dots, \sigma^{m-1}$  — циклическая группа, порожденная подстановкой  $\sigma$ . Множество переставляемых элементов разбивается на орбиты, и подстановка вполне определяется тем, как она действует на каждой

орбите. Пусть  $a_0$  — один из переставляемых элементов. Обозначим через  $a_1$  тот, который получается из  $a_0$  применением подстановки  $\sigma$ , через  $a_2$  тот, который получается из  $a_0$  применением  $\sigma^2$  (т. е. применением  $\sigma$  к  $a_1$ ), и т. д. При продолжении этого процесса в конце концов вернемся к элементу  $a_0$ . Таким образом, элементы орбиты, содержащей  $a_0$ , естественно располагаются в порядке  $(a_0, a_1, \dots, a_{k-1})$ , в котором подстановка  $\sigma$  переставляет элементы по кругу. Таким же образом элементы располагаются на всех орбитах. Подстановка разбивается на циклы:

$$\sigma = (a_0, a_1, \dots, a_{k-1})(b_0, b_1, \dots, b_{m-1}) \dots (c_0, c_1, \dots, c_{p-1}).$$

Если каждый цикл  $(a_0, a_1, \dots, a_{k-1})$  рассматривать как подстановку, циклически переставляющую элементы  $a_0, a_1, \dots, a_{k-1}$  и оставляющую все остальные элементы на своих местах, то мы можем рассматривать равенство

$$\sigma = (a_0, a_1, \dots, a_{k-1})(b_0, b_1, \dots, b_{m-1}) \dots (c_0, c_1, \dots, c_{p-1})$$

как разложение подстановки в произведение циклов, попарно не содержащих общих элементов.

Легко видеть, что цикл  $(a_0, a_1, \dots, a_{k-1})$  допускает такое разложение в произведение транспозиций:

$$(a_0, a_1, \dots, a_{k-1}) = (a_0, a_1)(a_0, a_2) \dots (a_0, a_{k-1}),$$

откуда следует, что цикл нечетной длины является четной подстановкой, цикл четной длины — нечетной. Поэтому четность или нечетность подстановки совпадает с четностью или нечетностью количества циклов четной длины.

**Предложение 2.** Пусть  $\sigma$  — подстановка, разложенная на циклы, и  $\tau$  — некоторая другая подстановка. Тогда, чтобы получить подстановку  $\tau^{-1}\sigma\tau$ , нужно сделать подстановку  $\tau$  в каждом цикле подстановки  $\sigma$ .

**Доказательство.** Пусть

$$\sigma = (a_0, a_1, \dots, a_{k-1})(b_0, b_1, \dots, b_{m-1}) \dots (c_0, c_1, \dots, c_{p-1}),$$

$$\tau = \begin{pmatrix} a_0 & a_1 & \dots & a_{k-1} & b_0 & b_1 & \dots & b_{m-1} & \dots & c_0 & c_1 & \dots & c_{p-1} \\ a'_0 & a'_1 & \dots & a'_{k-1} & b'_0 & b'_1 & \dots & b'_{m-1} & \dots & c'_0 & c'_1 & \dots & c'_{p-1} \end{pmatrix}.$$

Тогда

$$\tau^{-1} = \begin{pmatrix} a'_0 & a'_1 & \dots & a'_{k-1} & b'_0 & b'_1 & \dots & b'_{m-1} & \dots & c'_0 & c'_1 & \dots & c'_{p-1} \\ a_0 & a_1 & \dots & a_{k-1} & b_0 & b_1 & \dots & b_{m-1} & \dots & c_0 & c_1 & \dots & c_{p-1} \end{pmatrix}.$$

Проследим за действием подстановки  $\tau^{-1}\sigma\tau$  на элементы  $a'_0, a'_1, \dots, a'_{k-1}$  и т. д. Подстановка  $\tau^{-1}$  переводит  $a'_j$  в  $a_0$ ,  $\sigma$  переводит  $a_0$  в  $a_1$ ,  $\tau$  переводит  $a_1$  в  $a'_1$ . Следовательно,  $\tau^{-1}\sigma\tau$  переводит  $a'_0$  в  $a'_1$ .

Таким же образом прослеживается судьба элемента  $a'_1$ . Он сперва переходит в  $a_1$ , затем  $a_1$  в  $a_2$  и  $a_2$  в  $a'_2$ , так что  $a'_1$  переходит в  $a'_2$ . Наконец,  $a'_{k-1}$  переходит в  $a_{k-1}$ ,  $a_{k-1}$  в  $a_1$  и  $a_1$  в  $a'_1$ , так что цикл  $(a'_0, a'_1, \dots, a'_{k-1})$  замыкается. То же самое происходит и с остальными циклами, так что

$$\tau^{-1}\sigma\tau = (a'_0, a'_1, \dots, a'_{k-1})(b'_0, b'_1, \dots, b'_{m-1}) \dots (c'_0, c'_1, \dots, c'_{p-1}).$$

Отсюда следует

*Теорема 3. Для того чтобы две подстановки были сопряжены в симметрической группе, необходимо и достаточно, чтобы они имели разложения на циклы одинаковых порядков.*

Необходимость непосредственно следует из предложения 2. Достаточность — из того, что в симметрической группе существуют подстановки, переводящие любое расположение элементов в любое другое.

В силу этой теоремы число классов сопряженных элементов в симметрической группе  $S_n$  равно числу разбиения числа  $n$  на слагаемые, порядок которых безразличен. Так, число 5 допускает разбиения  $5 = 5$ ,  $5 = 4 + 1$ ,  $5 = 3 + 2$ ,  $5 = 3 + 1 + 1$ ,  $5 = 2 + 2 + 1$ ,  $5 = 2 + 1 + 1 + 1$  и  $5 = 1 + 1 + 1 + 1 + 1$ . Поэтому в группе  $S_5$  имеется 7 классов сопряженных элементов.

**5. Примеры из геометрии.** Пусть  $M$  — множество точек на плоскости и  $G$  — группа всех движений плоскости. Стабилизатором точки является группа вращений вокруг этой точки. Между точками плоскости и левыми классами смежности группы всех движений по группе вращений вокруг точки имеется изоморфное соответствие.

Элементарная геометрия изучает свойства геометрических фигур, остающиеся неизменными при движениях. Одно из основных понятий геометрии — расстояние между двумя точками — можно рассматривать как инвариантную величину, связывающую пару классов смежности полной группы движений плоскости по подгруппе вращений.

Можно сказать, что пара групп  $G \supset H$  определяет некоторую геометрию, в которой точками являются левые классы смежности  $G$  по  $H$ , а движениями — правые умножения классов смежности на элементы из  $G$ . Взгляд на геометрию с точки зрения теории групп был развит немецким математиком Ф. Клейном в конце 19-го века.

Геометрия Лобачевского укладывается в эту схему следующим образом. Рассматривается группа дробно линейных преобразований  $z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta}$  комплексных чисел, где  $\alpha, \beta, \gamma, \delta$  — вещественные коэффициенты, удовлетворяющие зависимости  $\alpha\delta - \beta\gamma = 1$ . Верхняя полуплоскость оказывается однородным пространством для

этой группы. Действительно, если  $z = x + yi$  при  $y > 0$ , то

$$\frac{\alpha z + \beta}{\gamma z + \delta} = \frac{\alpha y (x^2 + y^2) + (\alpha\delta + \beta\gamma)x + \beta\delta + (\alpha\delta - \beta\gamma)yi}{(\gamma x + \delta)^2 + \gamma^2 y^2},$$

так что мнимая часть числа  $\frac{\alpha z + \beta}{\gamma z + \delta}$ , равная  $\frac{y}{(\gamma x + \delta)^2 + \gamma^2 y^2}$ , положительна. Легко проследить, что для любой пары  $z, z'$  комплексных чисел с положительными мнимыми частями найдутся вещественные  $\alpha, \beta, \gamma, \delta$ ,  $\alpha\delta - \beta\gamma = 1$ , такие, что  $z' = \frac{\alpha z + \beta}{\gamma z + \delta}$ . Действительно, положив  $z' = x' + y'i$ ,  $z = x + yi$ , получим равенство, равносильное требуемому:

$$(x' + y'i)(\gamma(x + yi) + \delta) = \alpha(x + yi) + \beta.$$

Можно даже положить  $\delta = 0$ . Отделив вещественную часть от мнимой, получим два линейных однородных уравнения, связывающих  $\alpha, \beta$  и  $\gamma$ , из которых найдем

$$\alpha = \gamma \frac{xy' + x'y}{y}, \quad \beta = \frac{-\gamma y' (x^2 + y^2)}{y},$$

откуда

$$\alpha\delta - \beta\gamma = \frac{\gamma^2 y' (x^2 + y^2)}{y}.$$

Положив  $\gamma = \sqrt{\frac{y}{y'(x^2 + y^2)}}$ , получим требуемое.

Верхняя полуплоскость, в которой движения определены как указанные дробно-линейные преобразования, является моделью плоскости Лобачевского, эта модель связана с именем Пуанкаре. Стабилизатором точки  $i$  является группа, образованная преобразованиями  $z \mapsto \frac{\alpha z + \beta}{-\beta z + \alpha}$  при условии  $\alpha^2 + \beta^2 = 1$ . Следовательно, точки плоскости Лобачевского находятся в изоморфном (по отношению к группе движений) соответствии с левыми классами смежности группы дробно-линейных преобразований  $z' = \frac{\alpha z + \beta}{\gamma z + \delta}$  с вещественными  $\alpha, \beta, \gamma, \delta$  и  $\alpha\delta - \beta\gamma = 1$  по подгруппе, составленной из преобразований  $\frac{\alpha z + \beta}{-\beta z + \alpha}$  при  $\alpha^2 + \beta^2 = 1$ .

**6. Централизатор элемента и нормализатор подгруппы.** В п. 2 мы рассматривали группу  $G$  как  $G$ -операторное множество, полагая,  $a^z = z^{-1}az$  для  $a \in G$  и  $z \in G$ , т. е. рассматривая действие элементов  $G$  как соответствующие им внутренние автоморфизмы. В этой ситуации орбитами являются классы сопряженных элементов, и каждый класс является однородным пространством. Пусть  $C$  — некоторый класс сопряженных элементов и  $a \in C$ . Стабилизатором элемента  $a$  является множество всех  $z \in G$ , обладающих свойством  $z^{-1}az = a$ , т. е.  $az = za$ . Таким образом, стабилизатором элемента  $a$  является множество всех элементов группы, коммутирующих с  $a$ . Это множество образует подгруппу группы  $G$ ,

называемую *централизатором* элемента  $a$ . В силу п. 3 элементы класса сопряженных с  $a$  элементов находятся во взаимно однозначном соответствии с левыми классами смежности группы  $G$  по централизатору элемента  $a$ . В частности, если класс сопряженных элементов конечен, то число составляющих его элементов равно индексу централизатора любого элемента из этого класса.

Термин «централизатор» элемента  $a$  связан с тем, что централизатор  $a$  является наибольшей подгруппой, содержащей  $a$  в своем центре.

Элементы группы  $G$  можно рассматривать как действующие на множестве всех подгрупп группы  $G$  в виде соответствующих внутренних автоморфизмов:  $H \rightarrow z^{-1}Hz$ . В этой ситуации орбитами будут классы сопряженных подгрупп. Стабилизатором для подгруппы  $H$  является множество всех таких  $z \in G$ , что  $z^{-1}Hz = H$ . Этот стабилизатор носит название *нормализатора* группы  $H$ , ибо он является максимальной подгруппой, для которой  $H$  является нормальной подгруппой. Отсюда следует, что между сопряженными с группой  $H$  подгруппами и левыми классами смежности группы  $G$  по нормализатору  $H$  имеется взаимно однозначное соответствие, осуществляющее изоморфизм между однородными пространствами, состоящими из сопряженных с  $H$  подгрупп, и классами смежности по нормализатору.

**7. Центр  $p$ -группы.** Конечная группа называется  *$p$ -группой*, если ее порядок есть степень простого числа  $p$ . Ясно, что все подгруппы  $p$ -группы являются  $p$ -группами и индекс любой подгруппы в  $p$ -группе равен некоторой степени  $p$ .

Разобьем  $p$ -группу  $G$  порядка  $p^n$  на классы сопряженных элементов. Среди классов будут одноэлементные, образованные элементами центра, причем их число не меньше 1, ибо единица группы образует одноэлементный класс. Пусть число элементов центра равно  $t$ . Все элементы, не принадлежащие центру, порождают классы сопряженных, содержащие больше одного элемента. Пусть эти классы  $C_1, C_2, \dots, C_k$ . Число элементов в каждом таком классе есть индекс централизатора любого элемента класса и, следовательно, является степенью  $p^m$  с большим нуля показателем  $m$ .

Пусть число элементов в классе  $C_i$  равно  $p^{m_i}$ ,  $m_i > 0$ . Подсчет числа элементов группы  $G$  как суммы чисел элементов во всех классах сопряженных дает

$$p^n = t + p^{m_1} + p^{m_2} + \dots + p^{m_k}.$$

Из этого равенства заключаем, что  $t$  делится на  $p$ , и, так как  $t \geq 1$ , будет  $t \geq p$ . Таким образом, мы доказали, что любая конечная  $p$ -группа имеет нетривиальный центр. Конечно, порядок  $t$  центра равен степени  $p$ .

**8. Преобразования.** Взаимно однозначное отображение множества  $M$  на себя называется его *преобразованием*. *Тождествен-*

ное или единичное преобразование заключается в том, что каждый элемент отображается на себя. Последовательное осуществление двух преобразований равносильно третьему преобразованию, называемому их *произведением*. Умножение преобразований (в указанном смысле), очевидно, ассоциативно. Для каждого преобразования существует обратное, в силу взаимной однозначности преобразований. Для конечных множеств преобразования называются подстановками, и мы уже встречались с группой всех подстановок конечного множества — так называемой симметрической группой. Для бесконечных множеств группы всех преобразований совершенно необозримы, и рассматриваемые в математике группы преобразований выделяются посредством тех или иных достаточно сильных ограничений, связанных с особенностями строения рассматриваемых множеств.

Гомоморфное отображение группы  $G$  в группу преобразований некоторого множества называется *представлением* группы  $G$  посредством преобразований. Множество  $M$ , преобразованиями которого представляется группа  $G$ , становится  $G$ -множеством, если каждому элементу  $G$  сопоставить в качестве действия на элементы  $M$  соответствующее ему в силу гомоморфизма преобразование. В свою очередь, каждое  $G$ -множество  $M$  задает представление группы  $G$  преобразованиями.

Множество преобразований  $G$ -множества  $M$ , вызванных действиями элементов  $G$  на  $M$ , не обязано быть группой, изоморфной  $G$ . Оно, вообще говоря, является лишь гомоморфным образом группы  $G$ . Ядром гомоморфизма является множество всех элементов  $G$ , вызывающих тождественное преобразование  $M$ , т. е. пересечение стабилизаторов всех точек. Следовательно, пересечение стабилизаторов всех точек есть нормальная подгруппа группы  $G$ , и группа преобразований, вызванных элементами  $G$  на  $G$ -множестве  $M$ , изоморфна факторгруппе  $G$  по пересечению стабилизаторов всех точек множества  $M$ . Если пересечение стабилизаторов состоит только из 1, то представление группы  $G$  преобразованиями  $G$ -множества  $M$  будет *точным*, т. е. группа  $G$  будет изоморфна группе вызванных ее элементами преобразований множества  $M$ .

Если  $G$ -множество  $M$  есть однородное пространство, то стабилизаторами его точек являются все подгруппы, сопряженные со стабилизатором  $H$  одной из точек. В этом случае группа преобразований  $M$ , вызванных элементами группы  $G$ , изоморфна факторгруппе  $G$  по пересечению группы  $H$  со всеми сопряженными.

**9. Автоморфизмы группы.** Мы уже упоминали, что автоморфизмами группы называются изоморфные отображения группы  $G$  на себя. Среди автоморфизмов мы выделили внутренние автоморфизмы, вызываемые преобразованиями сопряжения посредством элементов группы.

**Предложение 4.** *Внутренние автоморфизмы образуют нормальную подгруппу группы всех автоморфизмов.*

**Доказательство.** Будем обозначать автоморфизмы как правые операторы в показателе, внутренний автоморфизм, вызванный сопряжением посредством элемента  $z$ , обозначим  $\alpha_z$ . Нужно доказать, что при любом автоморфизме  $\alpha$  автоморфизм  $\alpha^{-1}\alpha_z\alpha$  есть тоже внутренний автоморфизм. Применим автоморфизм  $\alpha^{-1}\alpha_z\alpha$  к произвольному элементу  $a$  группы. Получим:

$$(z^{-1}(a^{a^{-1}})z)^a.$$

В силу того, что  $\alpha$  — автоморфизм, это выражение равно  $(z^a)^{-1}(a^{a^{-1}})^a z^a = (z^a)^{-1} a z^a$ , так что  $\alpha^{-1}\alpha_z\alpha$  есть внутренний автоморфизм посредством элемента  $z^a$ .

Факторгруппа группы всех автоморфизмов группы по подгруппе внутренних автоморфизмов называется группой *внешних* автоморфизмов.

**Предложение 5.** *Группа внутренних автоморфизмов группы  $G$  изоморфна факторгруппе группы  $G$  по ее центру.*

**Доказательство.** Мы уже рассматривали группу  $G$  как  $G$ -множество по отношению к действию сопряжения  $a^z = z^{-1}az$ . Это действие индуцирует в  $G$  группу преобразований. Стабилизатором элемента  $a \in G$  является централизатор  $a$ , пересечение всех централизаторов есть центр  $G$ , ибо если элемент принадлежит централизаторам всех элементов, то он должен быть перестановочен со всеми элементами  $G$ , т. е. должен принадлежать центру и, конечно, каждый элемент центра принадлежит централизаторам всех элементов. В силу п. 8 группа внутренних автоморфизмов действительно изоморфна факторгруппе по центру.

Любая абелева группа не имеет нетривиальных внутренних автоморфизмов, ибо в абелевой группе  $z^{-1}az = a$  при любых  $a$  и  $z$ . Внешние же автоморфизмы есть даже у циклических групп. Бесконечная циклическая группа, порожденная элементом  $a$ , имеет лишь один нетождественный автоморфизм  $a^k \mapsto a^{-k}$ . Действительно, образующим бесконечной циклической группы будет либо  $a$ , либо  $a^{-1}$ . Ясно, однако, что любой автоморфизм должен переводить образующий в образующий. Автоморфизм  $a \mapsto a$  есть тождественный автоморфизм, автоморфизм  $a \mapsto a^{-1}$  преобразует  $a^k$  в  $a^{-k}$ .

Для конечной же циклической группы порядка  $n$  существует  $\varphi(n)$  автоморфизмов, именно, автоморфизм может преобразовать образующий  $a$  в любой другой образующий, а таковыми являются  $a^m$  при  $(m, n) = 1$ , причем  $m$  нужно рассматривать по модулю  $n$ .

Группа, центр которой состоит только из 1, и все автоморфизмы внутренние, называется совершенной. Можно доказать, что симметрические группы  $S_n$  подстановок совершенны при  $n = 3$ ,  $n = 4$ ,  $n = 5$  и  $n > 6$ . Для группы же  $S_6$  факторгруппа группы всех автоморфизмов по группе внутренних автоморфизмов имеет индекс 2. Доказательства этих предложений не очень просты.

## § 6. Свободная группа

**1. Свободная полугруппа.** Пусть задано конечное множество элементов  $a_1, a_2, \dots, a_n$ , называемых *буквами*. Это множество называется *алфавитом*. Последовательности  $a_{i_1} a_{i_2} \dots a_{i_m}$  букв алфавита называются *словами*. Присоединение к данному слову справа второго слова называется *умножением* слов. Ясно, что это действие ассоциативно, так что по отношению к нему слова составляют полугруппу. Естественно ввести в рассмотрение пустое слово. Оно играет роль единицы в полугруппе слов. Так построенная полугруппа называется *свободной полугруппой*, порожденной данным алфавитом.

**2. Свободная группа.** Свободная полугруппа, конечно, не является группой, так как произведение непустых слов непусто, так что у непустого слова не может существовать обратного.

Для построения на этом пути группы применим следующую конструкцию. К алфавиту  $S = \{a_1, a_2, \dots, a_n\}$  присоединим второй алфавит  $\bar{S} = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n\}$ . Строим слова в объединении этих алфавитов  $T = S \cup \bar{S}$  и вводим для слов в алфавите  $T$  отношение эквивалентности следующим образом. Вставкой в слово в алфавите  $T$  мы назовем присоединение между двумя буквами (или в начале слова, или в его конце) слова  $a_i \bar{a}_i$  или  $\bar{a}_i a_i$ . Сокращением слова назовем исключение из слова его части вида  $a_i \bar{a}_i$  или  $\bar{a}_i a_i$ . Два слова назовем эквивалентными, если от одного из них можно перейти ко второму посредством конечного числа вставок и сокращений. Ясно, что если два слова эквивалентны третьему, то они эквивалентны между собой, так что все слова разбиваются на непересекающиеся классы эквивалентных слов. Столь же ясно, что если слово  $A_1$  эквивалентно слову  $B_1$  и слово  $A_2$  эквивалентно слову  $B_2$ , то слово  $A_1 A_2$  эквивалентно слову  $B_1 B_2$ . Это позволяет ввести естественным образом умножение классов слов, считая произведением классов тот класс, который содержит произведение каких-либо слов из этих классов. Класс, содержащий пустое слово, является единицей при этом умножении. Ассоциативность умножения, очевидно, следует из ассоциативности умножения слов в свободной полугруппе. Классы, содержащие  $a_i$  и  $\bar{a}_i$ , взаимно обратны, ибо слова  $a_i \bar{a}_i$  и  $\bar{a}_i a_i$  превращаются в пустое слово после сокращения. Наконец для класса, содержащего любое слово, существует обратный: если класс содержит слово  $b_1, b_2, \dots, b_k$  при  $b_i \in T$ , то обратным будет класс, содержащий слово  $\bar{b}_k \dots \bar{b}_2 \bar{b}_1$  (здесь под  $\bar{a}_i$  понимается  $a_i$ ).

Итак, множество классов эквивалентных слов образует группу. Она называется конечно порожденной *свободной группой*. Классы, содержащие буквы алфавита  $S$ , являются ее образующими.

Когда речь идет об обширных классах объектов, всегда приятнее иметь дело с какими-либо стандартными представителями из

этих классов. Здесь роль таких представителей играют несократимые слова. Слово в алфавите  $T$  называется *несократимым*, если в нем не стоят рядом буквы  $a_i$  и  $\bar{a}_i$ .

**Теорема 1.** *В любом классе эквивалентных слов существует одно и только одно несократимое слово.*

**Доказательство.** То, что для любого слова найдется несократимое, ему эквивалентное, очевидно: в исходном слове нужно шаг за шагом, в каком-либо порядке, сокращать соседние «двойники»  $a_i, \bar{a}_i$ . При каждом сокращении длина слова, т. е. число составляющих слово букв, уменьшается на две единицы, так что процесс сокращения должен закончиться на несократимом слове после конечного числа сокращений.

Остается доказать, что различные несократимые слова не могут быть эквивалентны. Мы докажем это от противного. Пусть даны несократимые слова  $A$  и  $B$ , и допустим, что они эквивалентны, т. е. что существует конечная последовательность слов  $A = A_0, A_1, A_2, \dots, A_{m-1}, A_m = B$  таких, что каждое последующее слово получается из предыдущего вставкой или сокращением. Так как  $A$  и  $B$  несократимы, переход от  $A_0$  к  $A_1$  может быть только вставкой, переход от  $A_{m-1}$  к  $A_m = B$  — только сокращением. Полной высотой перехода от  $A$  к  $B$  назовем сумму длин всех промежуточных слов.

Пусть  $A_i$  — слово наибольшей длины среди слов  $A_0, A_1, \dots, A_{m-1}, A_m$ . Оно не крайнее, ибо длина  $A_1$  больше длины  $A_0$  и длина  $A_{m-1}$  больше длины  $A_m$ . Поэтому у слова  $A_i$  имеется как сосед слева  $A_{i-1}$ , так и сосед справа  $A_{i+1}$ . Переход от  $A_{i-1}$  к  $A_i$  должен быть вставкой, переход от  $A_i$  к  $A_{i+1}$  — сокращением. Здесь может представиться несколько случаев:

1. При переходе от  $A_{i-1}$  к  $A_i$  вставили  $b\bar{b}$  и при переходе от  $A_i$  к  $A_{i+1}$  вставленную пару сократили. В этом случае  $A_{i-1} = A_{i+1}$ , так что мы можем исключить из перехода слово  $A_i$  и «склеить»  $A_{i-1}$  и  $A_{i+1}$ .

2. При переходе от  $A_{i-1}$  к  $A_i$  вставили  $b\bar{b}$ , и справа от этой вставки находился элемент  $b$ , а при переходе от  $A_i$  к  $A_{i+1}$  в тройке соседних букв  $b\bar{b}b$  сократили  $b\bar{b}$ . В этом случае опять  $A_{i-1} = A_{i+1}$ . То же самое будет, если вставить  $b\bar{b}$  направо от  $\bar{b}$  и в тройке  $b\bar{b}b$  сократить  $b\bar{b}$ .

3. При переходе от  $A_{i-1}$  к  $A_i$  вставляется  $b\bar{b}$  и при переходе от  $A_i$  к  $A_{i+1}$  сокращается  $c\bar{c}$ , и эта пара не имеет общих элементов со вставленной  $b\bar{b}$ . Тогда переход от  $A_{i-1}$  к  $A_{i+1}$  можно сделать по-другому. Буквы  $c$  и  $\bar{c}$  не были вставлены при переходе от  $A_{i-1}$  к  $A_i$ , и следовательно,  $c\bar{c}$  уже присутствовало в  $A_{i-1}$ . Можно было сначала сократить  $c\bar{c}$ , получив слово  $A'_i$ , а затем вставить  $b\bar{b}$ . Длина промежуточного слова  $A'_i$  на 4 меньше длины слова  $A_i$ , так что полная высота перехода от  $A$  к  $B$  уменьшилась на 4.

Во всех случаях полная высота перехода может быть уменьшена. Это невозможно, ибо среди переходов от  $A$  к  $B$  должен

существовать переход с наименьшей полной высотой. Следовательно, эквивалентные несократимые слова равны, что и требовалось доказать.

**3. Конечно порожденные группы как гомоморфные образы свободной группы.**

**Теорема 2.** *Любая конечно порожденная группа с  $n$  образующими есть гомоморфный образ свободной группы с  $n$  образующими.*

**Доказательство.** Пусть  $u_1, u_2, \dots, u_n$  — система образующих группы  $G$ . Рассмотрим свободную группу сначала как полугруппу слов в алфавите  $a_1, a_2, \dots, a_n, \bar{a}_1, \bar{a}_2, \dots, \bar{a}_n$ . Каждому слову  $\dots a_i \dots \bar{a}_j \dots$  сопоставим элемент  $\dots u_i \dots u_j^{-1} \dots$  группы  $G$ . Ясно, что произведению слов соответствует произведение элементов группы  $G$ . Покажем, что эквивалентным словам соответствуют одинаковые элементы. Действительно, вставке  $a_i \bar{a}_i$  в слово соответствует появление сомножителя  $u_i u_i^{-1}$ , равного единице, и сокращению пары  $a_i \bar{a}_i$  соответствует исключение из произведения  $u_i u_i^{-1} = 1$ . Тем самым, построенное отображение есть гомоморфизм свободной группы на группу  $G$ .

Если некоторое слово  $\dots a_i \dots \bar{a}_j \dots$  из свободной группы входит в ядро, то соответствующий элемент  $\dots u_i \dots u_j^{-1} \dots$  группы  $G$  равен 1, т. е. элементам ядра гомоморфизма свободной группы в  $G$  соответствуют соотношения между образующими группы  $G$ .

**4. Задание группы образующими и соотношениями.**

**Теорема 3.** *Пусть дан алфавит  $a_1, \dots, a_n, \bar{a}_1, \dots, \bar{a}_n$  и слова в этом алфавите*

$$\omega_1 = v_{11} \dots v_{1k_1}, \quad \omega_2 = v_{21} \dots v_{2k_2}, \quad \dots, \quad \omega_m = v_{m1} \dots v_{mk_m}.$$

Здесь  $v_{ij}$  обозначают буквы алфавита. Тогда существует группа  $G$  с  $n$  образующими  $u_1, u_2, \dots, u_n$ , в которой выполнены соотношения

$$z_1 = x_{11} \dots x_{1k_1} = 1, \quad z_2 = x_{21} \dots x_{2k_2} = 1, \quad \dots, \quad z_m = x_{m1} \dots x_{mk_m} = 1,$$

где  $x_{ij} = u_s$ , если  $v_{ij} = a_s$ , и  $x_{ij} = u_s^{-1}$ , если  $v_{ij} = \bar{a}_s$ . Среди групп, для образующих которых выполнены указанные соотношения, существует группа  $G$ , в которой все соотношения между образующими являются следствиями данных соотношений, и эта группа обладает свойством универсальности — любая группа, в которой выполнены предписанные соотношения, является гомоморфным образом группы  $G$ .

Прежде чем доказывать теорему, необходимо выяснить, что понимается под *следствиями* из данных соотношений.

Мы считаем, что если  $z_i = x_{i1} \dots x_{ik_i} = 1$  есть соотношение, то соотношение  $z_i^{-1} = x_{ik_i}^{-1} \dots x_{i1}^{-1} = 1$  является его следствием. Если

$z_i = 1$  и  $z_j = 1$  — два соотношения, то соотношение  $z_i z_j = 1$  является их следствием, и, наконец, если  $z_i = 1$  есть соотношение, то при любом  $y \in G$  соотношение  $y^{-1} z_i y = 1$  тоже считается следствием.

**Доказательство.** Рассмотрим свободную группу с образующими  $a_1, \dots, a_n$  и в ней наименьшую нормальную подгруппу, содержащую  $w_1, w_2, \dots, w_m$ . Напомним, что эта подгруппа состоит из элементов  $w_1, w_2, \dots, w_m$ , обратных к ним элементов, сопряженных с ними и произведений всех таких элементов. Гомоморфный образ  $G$  свободной группы с так построенным ядром будет иметь предписанные соотношения. Другие соотношения будут определяться всеми элементами ядра гомоморфизма, и в силу устройства этого ядра, будут следствиями предписанных соотношений в описанном выше смысле.

Если в группе, кроме предписанных соотношений и их следствий, выполняются еще какие-либо соотношения, то ядро гомоморфизма будет содержать указанную нормальную подгруппу, и, в силу свойства универсальности факторгруппы, группа будет гомоморфным образом группы  $G$ .

Доказанная теорема дает возможность задавать группы при помощи задания образующих и соотношений между ними. Эти соотношения называются *определяющими соотношениями*. Группы, имеющие конечное число образующих и конечное число определяющих соотношений, называются *конечно определенными*. Именно такие группы часто возникают в приложениях теории групп к геометрии и топологии. Иногда определяющие соотношения таковы, что элементам группы удается дать некоторую каноническую запись, и умножение элементов в канонической записи не представляет труда. Рассмотрим примеры этого рода.

**Пример 1.** Группа задана двумя образующими  $a$  и  $b$ , связанными соотношениями  $a^2 = 1$  (т. е.  $a = a^{-1}$ ),  $b^3 = 1$  и  $aba = b^2$ . Очевидным следствием из этих соотношений является  $ab^2a = b$ . Последние два соотношения можно записать в форме  $ba = ab^2$  и  $b^2a = ab$ . Эти соотношения позволяют переносить образующий  $a$  через  $b$  или  $b^2$  справа налево, заменяя  $b$  на  $b^2$  и  $b^2$  на  $b$ . Это позволяет записать любой элемент группы в форме  $a^k b^m$  при  $k = 0, 1$  и  $m = 0, 1, 2$ . Рассматривая элементы этого вида формально, с правилами умножения, вытекающими из правила переноса  $a$  справа налево и условий  $a^2 = 1$  и  $b^3 = 1$ , нетрудно проверить, что символы  $a^k b^m$  действительно образуют группу. Она конечна, ее порядок равен 6. Легко видеть, что она изоморфна симметрической группе подстановок трех элементов. Изоморфизм дается соответствием  $a \mapsto (1, 2)$ ,  $b \mapsto (1, 2, 3)$ .

**Пример 2.** Группа задана двумя образующими  $c$  и  $a$  и соотношениями  $a^2 = 1$  и  $aca = c^{-1}$ . Здесь образующий  $c$  свободен, т. е. порождает бесконечную циклическую группу. Очевидным следствием из этих соотношений является  $ac^m a = c^{-m}$  при любом це-

лом  $m$ , т. е. преобразование сопряжения посредством  $a$  вызывает в подгруппе, порожденной образующим  $c$ , единственный нетривиальный автоморфизм. Из соотношения  $ac^m a = c^{-m}$  следует правило переноса образующего  $a$  справа налево, именно,  $c^m a = ac^{-m}$ . Это правило позволяет записать любой элемент группы в виде  $a^k c^m$  при  $k = 0, 1$  и любом целом  $m$ . Легко проследить, что символы  $a^k c^m$  при умножении с правилами, обусловленными соотношениями  $a^2 = 1$  и  $c^m a = ac^{-m}$ , действительно образуют группу. Эта группа нам еще встретится в следующем параграфе.

Однако при задании группы образующими и определяющими соотношениями имеет место одна принципиальная неприятность. Если даны два элемента группы, записанные через образующие, как узнать, равны они или нет? Вопрос легко решается, если соотношения таковы, что существует каноническая форма записи. Однако такой характер соотношений является скорее исключением, чем правилом. Проблема распознавания равенства элементов группы, заданной образующими и определяющими соотношениями, называется *проблемой тождества* в теории групп. Для свободной группы она решается благодаря канонической записи элементов в виде несократимых слов. Проблема получила положительное решение для групп с одним соотношением. Однако в 1952 г. П. С. Новиков доказал, что не существует алгоритма, позволяющего решать проблему тождества в общей постановке. Более того, им построена такая система определяющих соотношений между образующими, что не существует алгоритма для решения проблемы тождества в группе, заданной этими образующими и соотношениями. При этом доказательство потребовало точного определения того, что такое алгоритм, и привлечения средств современной математической логики.

Разумеется, несуществование общего алгоритма для любых элементов не значит, что задача не может быть решена индивидуальным приемом для заданной пары элементов. Из того, что алгоритмически неразрешима массовая проблема, не следует неразрешимость индивидуальных проблем.

По своей принципиальной значимости результат П. С. Новикова находится в одном ряду с классическими «отрицательными» результатами в математике, такими, как недоказуемость постулата Евклида о параллельных (следующая, например, из непротиворечивости геометрии Лобачевского) и неразрешимость в радикалах общих алгебраических уравнений пятой степени и выше.

## § 7. Свободные произведения групп

**1. Определение.** Пусть даны группы  $G_1, G_2, \dots, G_n$ . Составим слово из произвольных элементов групп  $G_1, G_2, \dots, G_n$  в любом порядке. Для таких слов введем действие удлинения, заключающееся во вставке в любое место единицы любой группы и в за-

мене какого-либо элемента в слове равным ему произведением двух элементов той же группы. Вставку единицы можно рассматривать как частный случай замены элемента произведением, если отождествить единицы всех групп. Тогда вставка единицы равносильна замене левого соседнего элемента  $a$  на  $a \cdot 1$  или правого соседнего  $b$  на  $1 \cdot b$ . Обратные операции — выбрасывание единицы и замена рядом стоящих элементов одной и той же группы их произведением — назовем сокращением. Два слова будем считать эквивалентными, если возможен переход от одного к другому посредством конечного числа удлинений и сокращений. Все слова разбиваются на классы эквивалентных. Ясно, что эквивалентность сомножителей влечет эквивалентность их произведений. Это позволяет определить умножение классов эквивалентных слов. Умножение ассоциативно, роль единицы играет пустое слово (или слово, составленное из единицы, которая отождествлена с единицами всех групп). Для каждого класса существует обратный, так что классы эквивалентных слов образуют группу. Эта группа называется *свободным произведением* групп  $G_1, G_2, \dots, G_n$ .

Слово называется *несократимым*, если в его составе нет единиц и нет соседних элементов из одной группы.

**Теорема.** *В каждом классе эквивалентных слов имеется одно и только одно несократимое слово.*

**Доказательство.** Для построения из данного слова несократимого достаточно выкинуть единицы и умножить рядом стоящие элементы из одной группы.

Остается доказать, что неравные несократимые слова не эквивалентны. Это мы докажем подобно доказательству аналогичного утверждения для свободной группы. Пусть  $A$  и  $B$  — различные несократимые слова, и пусть  $A = A_0, A_1, \dots, A_{m-1}, A_m = B$  — последовательность слов, в которых последующее получается из предыдущего посредством удлинения или сокращения. Переход от  $A_0$  к  $A_1$  может быть только удлинением, переход от  $A_{m-1}$  к  $A_m = B$  может быть только сокращением. Сумму длин слов  $A_1, \dots, A_{m-1}$  назовем *полной высотой* перехода. Пусть  $A_i$  — слово наибольшей длины. Оно не может быть крайним, так что у него есть два соседних  $A_{i-1}$  и  $A_{i+1}$ . Переход от  $A_{i-1}$  к  $A_i$  должен быть удлинением, от  $A_i$  к  $A_{i+1}$  — сокращением.

Могут представиться следующие случаи.

1. При переходе от  $A_{i-1}$  к  $A_i$  элемент  $b$  заменили на произведение  $b_1 b_2$  элементов той же группы, а при переходе от  $A_i$  к  $A_{i+1}$  заменили  $b_1 b_2$  на  $b$ . Ясно, что в этом случае  $A_{i-1} = A_{i+1}$ ,  $A_i$  можно исключить из перехода, а  $A_{i-1}$  и  $A_{i+1}$  — «склеить». Полная высота перехода уменьшится.

2. При переходе от  $A_{i-1}$  к  $A_i$  элемент  $b$  заменили на произведение  $b_1 b_2$ , а при переходе от  $A_i$  к  $A_{i+1}$  соединили  $b_1$  с предшествующим элементом  $a$  из той же группы. Это значит, что в слове  $A_{i-1}$  была последовательность букв  $ab$  и в слове  $A_{i+1}$  вместо нее

появилась последовательность букв  $cb_2$ , где  $c = ab_1$ . Переход от  $A_{i-1}$  к  $A_{i+1}$  можно было сделать иначе — сперва сократить, соединив  $a$  и  $b$ , а потом удлинить, вставив вместо произведения  $ab$  равное ему произведение  $cb_2$ . Промежуточное слово  $A'_i$  будет короче  $A_i$  на 2, так что полная высота уменьшится.

Аналогично рассматривается случай, когда после замены  $b$  на  $b_1b_2$  элемент  $b_2$  соединяется со следующим элементом, который должен принадлежать той же группе.

3. При переходе от  $A_{i-1}$  к  $A_i$  заменили элемент  $b$  на произведение  $b_1b_2$ , а при переходе от  $A_i$  к  $A_{i+1}$  заменили  $c_1c_2$  на их произведение  $c$  в другом месте, не затрагивая элементов  $b_1$  и  $b_2$ . В этом случае для перехода от  $A_{i-1}$  к  $A_{i+1}$  можно было сперва заменить  $c_1c_2$  на  $c$ , а потом заменить  $b$  на  $b_1b_2$ . Промежуточное слово  $A'_i$  короче слова  $A_i$  на 2. Полная высота перехода тоже уменьшилась.

Итак, при переходе от несократимого слова  $A$  к несократимому слову  $B$  всегда можно уменьшить полную высоту перехода. Мы получили противоречие, ибо безграничное уменьшение полной высоты невозможно. Таким образом, несократимые слова не могут быть эквивалентны и могут служить каноническими представителями классов, т. е. удобной записью элементов свободного произведения групп.

**2. Пример.** Рассмотрим свободное произведение двух циклических групп второго порядка с образующими  $a$  и  $b$ .

Несократимые слова состоят из чередующихся букв  $a$  и  $b$ . Положим  $ab = c$ . Тогда  $c^{-1} = ba$ ,  $c^m = abab \dots ab \neq 1$ , так что  $c$  порождает свободную циклическую группу. Элементы  $a$  и  $c$  являются образующими, ибо  $b = ac$ . Далее,  $ca = aba = ac^{-1}$ . Таким образом, свободное произведение двух циклических групп второго порядка изоморфно группе примера 2 предыдущего пункта.

Эта группа имеет простую геометрическую интерпретацию. Возьмем на плоскости две параллельные прямые  $x = 0$  и  $x = c$ . Обозначим через  $a$  отражение относительно первой прямой и через  $b$  — отражение относительно второй прямой. Ясно, что  $a^2 = b^2 = 1$ . Отражение  $a$  переводит точку с абсциссой  $x$  в точку с абсциссой  $-x$ , отражение  $b$  преобразует  $x$  в  $c - x$ . Следовательно, преобразование  $ab$  переводит  $x$  в  $c - (-x) = c + x$ , т. е.  $ab$  есть сдвиг на  $c$ . Группа сдвигов на кратные  $c$  есть свободная циклическая группа. Поэтому все произведения чередующихся букв  $a$  и  $b$  различны, т. е. группа, порожденная отражениями от двух параллельных прямых, есть свободное произведение двух циклических групп второго порядка.

## § 8. Конечные абелевы группы

**1. Разложение конечной абелевой группы в прямую сумму примарных абелевых групп.** В этом и следующем параграфах мы изложим теорию конечно порожденных абелевых групп, причем бу-

дем пользоваться аддитивной записью и соответствующей терминологией. Действие в группе будем называть сложением и обозначать знаком  $+$ , нейтральный элемент назовем нулем группы и обозначим  $0$ , вместо обратного элемента будем говорить о противоположном, вместо степеней — о кратных, вместо термина прямое произведение будем говорить прямая сумма и для обозначения прямой суммы будем использовать знак  $\oplus$ .

Пусть  $G$  — конечная абелева группа и  $a$  — ее элемент. Натуральное число  $m$  такое, что  $ma = 0$ , назовем *аннулятором элемента  $a$* . Среди аннуляторов найдется минимальный, именно, порядок элемента  $a$ .

**Предложение 1.** *Все аннуляторы элемента  $a \in G$  делятся на его порядок.*

Действительно, пусть  $m$  — порядок элемента  $a$  и  $m_1$  — какой-либо другой аннулятор. Тогда  $m_1 = mq + r$ ,  $0 \leq r \leq m - 1$ , и  $ra = = m_1a - qma = 0$ , и, следовательно,  $r = 0$ , в силу минимальности аннулятора  $m$ .

*Аннулятором группы* называется натуральное число, при умножении на которое аннулируются все элементы группы. Порядок группы принадлежит к числу ее аннуляторов. Среди аннуляторов группы существует минимальный и все аннуляторы на него делятся.

**Предложение 2.** *Пусть  $m$  — аннулятор группы  $G$  и  $m = = m_1m_2$ , причем  $m_1$  и  $m_2$  взаимно просты. Тогда  $G$  разлагается в прямую сумму двух подгрупп, одна из которых аннулируется числом  $m_1$ , другая — числом  $m_2$ .*

**Доказательство.** Пусть  $G_1$  — множество всех элементов группы  $G$ , которые аннулируются числом  $m_1$ , и  $G_2$  — то же для  $m_2$ . Ясно, что  $G_1$  и  $G_2$  — подгруппы  $G$ . Ввиду взаимной простоты  $m_1$  и  $m_2$  найдутся целые числа  $u_1$  и  $u_2$  такие, что  $m_1u_1 + m_2u_2 = 1$ . Пусть  $a \in G$ . Тогда  $a = m_1u_1a + m_2u_2a$ . Первое слагаемое  $m_1u_1a$  принадлежит  $G_2$ , ибо  $m_2m_1u_1a = 0$ . Соответственно второе принадлежит  $G_1$ . Таким образом,  $G = G_1 + G_2$ . Чтобы убедиться в том, что сумма прямая, остается установить, что  $G_1 \cap G_2 = 0$ . Пусть  $a \in \in G_1 \cap G_2$ . Из равенства  $a = m_1u_1a + m_2u_2a$  заключаем, что  $a = 0$ , ибо равны нулю оба слагаемых правой части.

Заметим, что из самого построения групп  $G_1$  и  $G_2$  следует, что они определены однозначно.

**Предложение 3.** *Пусть аннулятор  $m$  группы  $G$  разлагается в произведение  $m = m_1m_2 \dots m_k$  попарно взаимно простых сомножителей. Тогда  $G$  разлагается в прямую сумму подгрупп с аннуляторами  $m_1, m_2, \dots, m_k$ .*

Непосредственно следует из предложения 2.

Конечная абелева группа называется *примарной*, если ее аннулятор есть степень простого числа.

**Теорема 4.** *Конечная абелева группа разлагается в прямую сумму примарных подгрупп.*

Следует из предложения 3, в применении к каноническому разложению аннулятора:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

## 2. Подгруппы циклической группы.

**Предложение 5.** *Все подгруппы конечной циклической группы порядка  $m$  циклически, и их образующими являются элементы вида  $a^d$ , где  $a$  — образующий данной группы,  $d$  — делитель числа  $m$ .*

**Доказательство.** Пусть  $G$  — циклическая группа порядка  $m$  с образующим  $a$  и  $H$  — ее подгруппа. Пусть  $d$  — наименьшее натуральное число, при котором  $da \in H$ . Тогда  $m$  делится на  $d$ , ибо если  $m = dq + r$ ,  $0 \leq r \leq d - 1$ , то  $ra = ma - qda = -qda \in H$ , и, в силу минимальности  $d$ ,  $r = 0$ . Если  $ka \in H$ , то  $k$  делится на  $d$ , ибо если  $k = dq_1 + r_1$ ,  $0 \leq r_1 \leq d - 1$ , то  $r_1 a = ka - q_1 da \in H$  и  $r_1 = 0$ . Таким образом,  $da$  — образующий группы  $H$ . Порядок  $H$  равен  $m/d$ . При любом  $d$ , делящем  $m$ , элемент  $da$  порождает подгруппу  $H$  порядка  $m/d$ .

В частности, если  $m = p^\alpha$ , то все подгруппы группы  $G$  образуют цепочку  $G \supset G_1 \supset G_2 \supset \dots \supset G_{\alpha-1} \supset 0$ , где  $G_i$  — подгруппа, порожденная  $p^i a$ .

## 3. Разложение примарной абелевой группы в прямую сумму примарных циклических групп.

**Предложение 6.** *Пусть  $H$  — подгруппа абелевой группы  $G$  и из классов смежности  $G$  по  $H$  можно извлечь по одному представителю так, что они образуют группу  $F$  (очевидно, изоморфную факторгруппе  $G/H$ ). Тогда  $G = H \oplus F$ .*

**Доказательство.**  $H + F = G$ , ибо в  $H + F$  присутствуют все элементы всех классов смежности.  $H \cap F = 0$ , ибо при естественном гомоморфизме  $G$  на  $G/H$  все элементы  $H \cap F$  отображаются в нулевой класс факторгруппы, и элемент группы  $F$ , принадлежащий нулевому классу, может быть только 0. Следовательно, по теореме 2 § 3,  $G = H \oplus F$ .

**Теорема 7.** *Примарная конечная группа  $G$  может быть разложена в прямую сумму примарных циклических групп.*

**Доказательство** проведем посредством индукции по порядку группы. Базу для индукции составляют группы простого порядка, ибо они циклически.

Пусть  $p^{\alpha_1}$  — минимальный аннулятор группы  $G$ . Тогда найдется элемент  $a_1 \in G$ , порядок которого равен  $p^{\alpha_1}$ . Пусть  $H_1$  — циклическая подгруппа, порожденная элементом  $a_1$ . Если  $H_1$  совпадает с  $G$ , то вопрос исчерпан,  $G$  сама циклическа. Пусть  $H_1$  не совпадает с  $G$ . Рассмотрим факторгруппу  $G/H_1$ . Она примарна, ее минимальный аннулятор равен  $p^\beta$  при  $\beta \leq \alpha_1$ , и ее порядок меньше порядка  $G$ . Согласно индуктивному предположению она является прямой суммой циклических групп  $\bar{H}_2, \dots, \bar{H}_k$  с образующими  $\bar{a}_2, \dots, \bar{a}_k$ . Постараемся выбрать из классов смежности такие представители

$a_2, \dots, a_k$ , чтобы их порядки совпадали с порядками  $\bar{a}_2, \dots, \bar{a}_k$ . Тогда они порождают подгруппу  $F$ , изоморфную  $G/H$ , т. е. представимую в виде прямой суммы циклических групп  $H_2, \dots, H_k$ , изоморфных  $\bar{H}_2, \dots, \bar{H}_k$ . В силу предложения 6 группа  $G$  равна  $H_1 \oplus F = H_1 \oplus H_2 \oplus \dots \oplus H_k$ .

Таким образом, для завершения доказательства теоремы нам нужно позаботиться о выборе представителей из классов  $\bar{a}_2, \dots, \bar{a}_k$ . Пусть  $p^{\alpha_2}$  — порядок  $\bar{a}_2$ . Ясно, что  $\alpha_2 \leq \beta \leq \alpha_1$ . Выберем из класса  $\bar{a}_2$  какой-либо элемент  $a'_2$ . Тогда  $p^{\alpha_2} a'_2 \in H_1$ , так что  $p^{\alpha_2} a'_2 = t a_1$  при некотором целом  $t$ . Далее,  $p^{\alpha_1 - \alpha_2} p^{\alpha_2} a'_2 = 0$ , так что  $p^{\alpha_1 - \alpha_2} t a_1 = 0$ . Это значит, что  $p^{\alpha_1 - \alpha_2} t$  делится на  $p^{\alpha_1}$  и  $t$  делится на  $p^{\alpha_2}$ ,  $t = p^{\alpha_2} t_1$ . Положим  $a_2 = a'_2 - t_1 a_1 \in \bar{a}_2$ . Тогда  $p^{\alpha_2} a_2 = p^{\alpha_2} a'_2 - p^{\alpha_2} t_1 a_1 = t a_1 - t a_1 = 0$ . Выбранный представитель  $a_2$  класса  $\bar{a}_2$  удовлетворяет поставленному требованию. Аналогично выбираются представители из классов  $\bar{a}_3, \dots, \bar{a}_k$ . Теорема доказана.

Из доказанной теоремы следует, что порядок примарной абелевой группы равен степени того же простого числа, которое входит в аннулятор. Так как порядок прямой суммы групп равен произведению порядков слагаемых, мы видим, что порядок конечной абелевой группы есть произведение степеней простых чисел, входящих в аннулятор, так что примарные сомножители канонического разложения порядка группы совпадают с порядками примарных прямых слагаемых.

**4. Инвариантность порядков циклических прямых слагаемых примарной абелевой группы.** Разложение примарной абелевой группы  $G$  в прямую сумму циклических подгрупп не однозначно, но тем не менее число прямых слагаемых и их порядки не зависят от способа разложения. Чтобы доказать это, обозначим через  $t_1$  число прямых слагаемых максимального порядка  $p^\alpha$ , через  $t_2$  — число прямых слагаемых порядка  $p^{\alpha-1}$ , ..., через  $t_\alpha$  — число прямых слагаемых порядка  $p$ . Тогда  $pG$  есть прямая сумма  $t_1$  циклических групп порядка  $p^{\alpha-1}$ ,  $t_2$  циклических групп порядка  $p^{\alpha-2}$ , ...,  $t_{\alpha-1}$  циклических групп порядка  $p$ . Поэтому  $G/pG$  есть прямая сумма групп порядка  $p$  в количестве  $t_1 + t_2 + \dots + t_\alpha$  и ее порядок равен  $p^{t_1+t_2+\dots+t_\alpha}$ . Таким же образом  $pG/p^2G$  есть прямая сумма  $t_1 + t_2 + \dots + t_{\alpha-1}$  групп порядка  $p$  и ее порядок равен  $p^{t_1+t_2+\dots+t_{\alpha-1}}$  и т. д. Таким образом, суммы  $t_1 + t_2 + \dots + t_\alpha$ ,  $t_1 + t_2 + \dots + t_{\alpha-1}$ , ...,  $t_1 + t_2, t_1$  имеют инвариантный смысл как показатели при  $p$  в порядках факторгрупп  $p^{i-1}G/p^iG$ . Следовательно, числа  $t_1, t_2, \dots, t_\alpha$  тоже инвариантны.

## § 9. Конечно порожденные абелевы группы

**1. Подгруппы конечно порожденных абелевых групп.** Пусть  $G$  — аддитивно записанная абелева группа с конечным числом образующих  $u_1, u_2, \dots, u_n$ . Тогда все ее элементы представляются в

виде

$$m_1 u_1 + m_2 u_2 + \dots + m_n u_n$$

с целыми  $m_1, m_2, \dots, m_n$ , причем такая запись может быть неоднозначной из-за наличия соотношений между образующими.

**Теорема 1.** *Подгруппа конечно порожденной абелевой группы конечно порождена, и ее образующие можно выбрать так, чтобы их число было не больше числа образующих группы.*

**Доказательство.** Пусть  $G$  — абелева группа с образующими  $u_1, u_2, \dots, u_n$  и  $H$  — ее подгруппа. Доказательство проведем методом математической индукции по числу образующих. Для групп с одним образующим  $u_1$ , т. е. для циклических групп, теорема верна, ибо всякая подгруппа конечной или бесконечной циклической группы сама циклична и порождается элементом  $ku_1$  с наименьшим натуральным  $k$ . Допустим, что теорема верна для подгрупп группы, порожденной меньше чем  $n$  образующими, и в этом предположении докажем ее для подгрупп группы с  $n$  образующими.

Рассмотрим элемент  $v_1 = m_1 u_1 + m_2 u_2 + \dots + m_n u_n \in H$  с наименьшим натуральным коэффициентом  $m_1$ . Покажем, что для любого  $v = l_1 u_1 + l_2 u_2 + \dots + l_n u_n \in H$  коэффициент  $l_1$  делится на  $m_1$ . С этой целью выполним деление с остатком:  $l_1 = m_1 q + r$ ,  $0 \leq r \leq m_1 - 1$ , и положим  $v' = v - qv_1 = ru_1 + m'_2 u_2 + \dots + m'_n u_n \in H$ , откуда заключаем, в силу минимальности  $m_1$ , что  $r = 0$ , так что  $v' = v - qv_1 = m'_2 u_2 + \dots + m'_n u_n$ . Обозначим через  $G'$  подгруппу  $G$ , порожденную  $u_2, \dots, u_n$ . Тогда  $v' \in H' = H \cap G'$ . Группа  $H'$  является подгруппой группы  $G'$ , имеющей  $n-1$  образующий. В силу индуктивного предположения,  $H'$  конечно порождена и образующие можно выбрать так, что их число не больше  $n-1$ . Пусть  $v_2, \dots, v_n$  — эти образующие (некоторые из них могут быть равны 0). Тогда  $v' = k_2 v_2 + \dots + k_n v_n$  при целых  $k_i$  и  $v = qv_1 + v' = qv_1 + k_2 v_2 + \dots + k_n v_n$ . Поэтому  $v_1, v_2, \dots, v_n$  — образующие группы  $H$  и их число равно  $n$  или меньше, если среди них есть нули. Теорема доказана.

## 2. Целочисленные унимодулярные матрицы.

**Предложение 2.** *Для того чтобы матрица  $A$  с целыми элементами имела обратную  $A^{-1}$  тоже с целыми элементами, необходимо и достаточно, чтобы  $\det A = \pm 1$ .*

**Доказательство.** Пусть  $A$  и  $A^{-1}$  имеют целые элементы. Из равенства  $AA^{-1} = E$  следует, что  $\det A \cdot \det A^{-1} = 1$ , но оба эти определителя — целые числа. Поэтому  $\det A = \pm 1$ . Это условие и достаточно, ибо союзная с  $A$  матрица, элементами которой являются алгебраические дополнения к элементам матрицы  $A$ , имеет целые элементы, а матрица  $A^{-1}$  получается из союзной делением на  $\det A = \pm 1$ , так что элементы  $A^{-1}$  — тоже целые числа.



так что  $2'$ , а вместе с ним и  $r$ , получает инвариантное истолкование, не зависящее от выбора системы свободных образующих.

### 5. Вспомогательные предложения.

**Предложение 4.** Пусть  $(a_1, a_2, \dots, a_k)$  — строка, составленная из целых чисел, и  $d$  — наибольший общий делитель чисел  $a_1, a_2, \dots, a_k$ . Существует такая целочисленная унимодулярная матрица, что

$$(a_1, a_2, \dots, a_k)M = (d, 0, \dots, 0).$$

**Доказательство.** Применим индукцию по длине строки  $k$ . Базу для индукции дает случай  $k = 2$ . Пусть  $d$  — наибольший общий делитель чисел  $a_1$  и  $a_2$ . Он допускает линейное представление  $d = a_1u + a_2v$ . Возьмем матрицу  $M = \begin{pmatrix} u & -b_2 \\ v & b_1 \end{pmatrix}$ , где  $b_1 = \frac{a_1}{d}$ ,  $b_2 = \frac{a_2}{d}$ . Матрица  $M$  унимодулярна, ибо  $ub_1 + vb_2 = \frac{ua_1 + va_2}{d} = 1$ . Далее,  $(a_1, a_2)M = (a_1u + a_2v, -a_1b_2 + a_2b_1) = (d, 0)$ . Допустим теперь, что предложение доказано для строк длины  $k - 1$ . Тогда найдется целочисленная унимодулярная матрица  $M_1$  порядка  $k - 1$  такая, что

$$(a_2, \dots, a_k)M_1 = (d_2, 0, \dots, 0),$$

где  $d_2$  — наибольший общий делитель чисел  $a_2, \dots, a_k$ . Пусть теперь  $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & M_1 \end{pmatrix}$ . Тогда

$$(a_1, a_2, \dots, a_k)M_2 = (a_1, d_2, 0, \dots, 0).$$

Далее, наибольший общий делитель чисел  $a_1$  и  $d_2$  равен  $d$ . Найдем целочисленную унимодулярную матрицу  $M_3$  второго порядка такую, что  $(a_1, d_2)M_3 = (d, 0)$ . Положим  $M_4 = \begin{pmatrix} M_3 & 0 \\ 0 & E_{k-2} \end{pmatrix}$ .  $M_4$  — тоже целочисленная унимодулярная и  $(a_1, d_2, 0, \dots, 0)M_4 = (d, 0, \dots, 0)$ . Таким образом, матрица  $M = M_2M_4$ , очевидно, целочисленная унимодулярная, дает требуемое:

$$(a_1, a_2, \dots, a_k)M = (d, 0, \dots, 0).$$

**Предложение 5.** Если числа  $a_1, a_2, \dots, a_k$  в совокупности взаимно простые, то существует целочисленная унимодулярная матрица с первой строкой  $(a_1, a_2, \dots, a_k)$ .

**Доказательство.** В предположении взаимной простоты чисел  $a_1, a_2, \dots, a_k$  будет  $d = 1$ , так что существует целочисленная унимодулярная матрица  $M$  такая, что  $(a_1, a_2, \dots, a_k)M = (1, 0, \dots, 0)$ . Тогда  $(1, 0, \dots, 0)M^{-1} = (a_1, a_2, \dots, a_k)$ . Матрица  $M^{-1}$  целочисленная унимодулярная, а последнее равенство показывает, что ее первая строка есть  $(a_1, a_2, \dots, a_k)$ .

**6. Конечно порожденные абелевы группы без кручения.** Абелева группа называется группой без кручения, если она не имеет элементов конечного порядка.



и  $\bar{a} = 0$ . Таким образом,  $G/H$  не имеет элементов конечного порядка кроме нуля и является группой без кручения. Ранг группы  $G/H$  как свободной абелевой группы называется также *рангом* группы  $G$ .

**Теорема 8.** *Конечно порожденная абелева группа  $G$  разлагается в прямую сумму группы кручения  $H$  и свободной абелевой группы с числом свободных образующих, равным рангу  $G/H$ .*

**Доказательство.** Пусть  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r$  — свободные образующие группы  $G/H$ . Возьмем произвольно элементы  $a_1 \in \bar{a}_1, a_2 \in \bar{a}_2, \dots, a_r \in \bar{a}_r$ . Элементы  $a_1, a_2, \dots, a_r$  порождают свободную подгруппу  $F$  группы  $G$ , ибо каждое соотношение  $m_1 a_1 + m_2 a_2 + \dots + m_r a_r = 0$  влечет за собой соотношения  $m_1 \bar{a}_1 + m_2 \bar{a}_2 + \dots + m_r \bar{a}_r = 0$ . Элементы группы  $F$  содержатся по одному во всех классах смежности, составляющих  $G/H$ . Согласно предложению 6 из § 8, группа  $G$  равна прямой сумме  $H$  и  $F$ .

Разумеется, разложение  $G = H + F$  не однозначно, хотя подгруппа  $H$  в  $G$  однозначно определена. Неоднозначность обусловлена тем, что элементы  $a_1, a_2, \dots, a_r$  выбираются внутри классов смежности  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r$  произвольным образом.

Из всего сказанного следует, что конечно порожденная абелева группа  $G$  разлагается в прямую сумму циклических групп, примарных конечных и бесконечных. Число бесконечных прямых слагаемых равно рангу группы  $G$ , порядки примарных конечных циклических прямых слагаемых определены группой  $G$  (точнее, ее подгруппой кручения) однозначно. Эти порядки носят название *коэффициентов кручения* группы  $G$ . Задание ранга и коэффициентов кручения определяет группу  $G$  с точностью до изоморфизма. Для любых наперед заданных значений ранга и коэффициентов кручения существует соответствующая абелева конечно порожденная группа.

# СИММЕТРИЧЕСКИЕ ПОЛИНОМЫ

## § 1. Выражение симметрических полиномов через основные

1. **Лексикографическое расположение одночленов в полиноме.** Пусть  $F(x_1, x_2, \dots, x_n)$  — полином с коэффициентами из некоторой области целостности. Расположим его по убывающим степеням буквы  $x_1$ . Одночлены, содержащие  $x_1$  в одинаковой степени, расположим по убывающим степеням буквы  $x_2$ , одночлены, содержащие  $x_1$  и  $x_2$  в одинаковых степенях, расположим по убывающим степеням буквы  $x_3$  и т. д. Одночлены расположатся в так называемом *лексикографическом* порядке, напоминающем расположение слов в словарях. Будем говорить, что предшествующий в лексикографическом порядке одночлен выше последующих. Из определения ясно, что одночлен  $Ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$  выше одночлена  $Bx_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$  в том и только в том случае, когда первая отличная от нуля среди разностей  $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \dots, \alpha_n - \beta_n$  положительна.

Одночлен, который находится на первом месте при лексикографическом упорядочении, носит название *высшего члена* полинома. Ясно, что если  $F(x_1, x_2, \dots, x_n) = a_0(x_2, x_3, \dots, x_n)x_1^{\alpha} + a_1(x_2, x_3, \dots, x_n)x_1^{\alpha-1} + \dots$ , то высшим членом полинома  $F$  является произведение  $x_1^{\alpha}$  на высший член полинома  $a_0(x_2, x_3, \dots, x_n)$ .

**Предложение 1.** *Высший член произведения двух полиномов равен произведению высших членов сомножителей.*

Для  $n = 1$  это верно. Остается применить тривиальным образом математическую индукцию, учитывая замечание, предшествующее формулировке предложения.

Предложение 1 естественно распространяется на произведение любого числа полиномов.

2. **Симметрические полиномы.** Полином  $F(x_1, x_2, \dots, x_n)$  называется симметрическим, если он не изменяется при всех перестановках входящих в него букв. Примерами симметрических полиномов могут служить так называемые степенные суммы — суммы одинаковых степеней букв. Особо важное место занимают так называемые *основные* или *элементарные* симметрические



шие члены полиномов  $f_1, f_2, \dots, f_n$  равны, соответственно  $x_1, x_1x_2, \dots, x_1x_2 \dots x_n$ .

Подходящим одночленом является  $Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3} \dots f_{n-1}^{\alpha_{n-1}-\alpha_n}f_n^{\alpha_n}$ .

В силу леммы все показатели неотрицательны, так что этот одночлен является полиномом от  $x_1, x_2, \dots, x_n$ . Его высший член равен

$$Ax_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3} \dots (x_1x_2 \dots x_{n-1})^{\alpha_{n-1}-\alpha_n}(x_1x_2 \dots x_n)^{\alpha_n} = \\ = Ax_1^{\alpha_1}x_2^{\alpha_2} \dots x_{n-1}^{\alpha_{n-1}}x_n^{\alpha_n}.$$

Число  $A$ , согласно предположению, целое, коэффициенты всех основных симметрических полиномов целые, следовательно, все коэффициенты полинома  $Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3} \dots f_{n-1}^{\alpha_{n-1}-\alpha_n}f_n^{\alpha_n}$  целые. Полином  $F_1(x_1, x_2, \dots, x_n) = F(x_1, x_2, \dots, x_n) - Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3} \dots f_{n-1}^{\alpha_{n-1}-\alpha_n}f_n^{\alpha_n}$  есть снова симметрический полином с целыми коэффициентами, но его высший член  $Bx_1^{\beta_1}x_2^{\beta_2} \dots x_n^{\beta_n}$  будет ниже высшего члена полинома  $F$ , ибо при вычитании высшие члены уменьшаемого и вычитаемого взаимно уничтожились. Процесс повторяется. Из полинома  $F_1(x_1, x_2, \dots, x_n)$  вычитается полином  $Bf_1^{\beta_1-\beta_2}f_2^{\beta_2-\beta_3} \dots f_n^{\beta_n}$ . В результате получается симметрический полином  $F_2(x_1, x_2, \dots, x_n)$ , снова с целыми коэффициентами и со старшим членом еще ниже. Процесс не может продолжаться без конца, ибо одночленов фиксированной степени (и тем более таких, которые могут быть высшими членами симметрических полиномов), каждый из которых ниже предыдущего, может быть лишь конечное число. Процесс может оборваться только на том, что при очередном вычитании получится 0.

Итак,

$$F(x_1, x_2, \dots, x_n) = Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3} \dots f_{n-1}^{\alpha_{n-1}-\alpha_n}f_n^{\alpha_n} + \\ + Bf_1^{\beta_1-\beta_2}f_2^{\beta_2-\beta_3} \dots f_{n-1}^{\beta_{n-1}-\beta_n}f_n^{\beta_n} + \dots$$

Все коэффициенты  $A, B, \dots$  будут целыми числами.

Теперь снимем предположение о том, что коэффициенты исходного полинома были целыми числами. Представим полином в виде суммы моногенных и в каждом моногенном слагаемом вынесем за скобки коэффициент, общий для всех его членов. В скобках останется полином с коэффициентами 1, и его представление через основные полиномы будет иметь целые коэффициенты, а, следовательно, коэффициенты в представлении данного моногенного слагаемого будут целыми кратными коэффициента его одночленов. Из различных моногенных слагаемых могут возникнуть подобные члены в их представлениях через основные, и, после приведения, получится полином от  $f_1, f_2, \dots, f_n$  с коэффициентами,

являющимися целочисленными линейными комбинациями коэффициентов исходного полинома. Теорема доказана полностью.

Эти же идеи позволяют доказать единственность представления симметрического полинома в виде полинома от основных симметрических полиномов.

**Предложение 3.** *Отличный от нуля полином от основных симметрических полиномов отличен от нуля и как полином от  $x_1, x_2, \dots, x_n$ .*

**Доказательство.** Пусть  $\Phi(f_1, f_2, \dots, f_n) = Af_1^{k_1}f_2^{k_2} \dots f_n^{k_n} + Bf_1^{l_1}f_2^{l_2} \dots f_n^{l_n} + \dots$ , причем среди слагаемых нет отличающихся только коэффициентом. Высший член одночлена  $Af_1^{k_1}f_2^{k_2} \dots f_n^{k_n}$  как полинома от  $x_1, x_2, \dots, x_n$  равен

$$Ax_1^{k_1+k_2+\dots+k_n}x_2^{k_2+k_3+\dots+k_n} \dots x_n^{k_n}.$$

Аналогично определяются высшие члены других одночленов. Различные одночлены имеют различные высшие члены, и самый высший из них получается лишь из одного одночлена и не имеет подобных среди членов других слагаемых. Поэтому  $\Phi(f_1, f_2, \dots, f_n)$ , не равный нулю как полином от  $f_1, f_2, \dots, f_n$ , не может стать равным нулю как полином от  $x_1, x_2, \dots, x_n$ .

Отсюда непосредственно следует единственность представления симметрического полинома в виде полинома от основных, ибо если бы были два различных представления, разность представлений была бы отличным от нуля полиномом от основных симметрических полиномов, равным нулю как полином от  $x_1, x_2, \dots, x_n$ , что невозможно.

**4. Примеры.** Рассмотрим несколько примеров.

$$1. \quad F(x_1, x_2, \dots, x_n) = x_1^2 + x_2^2 + \dots + x_n^2.$$

Первым членом представления через основные симметрические является  $f_1^2$ . Ясно, что  $F - f_1^2 = -2f_2$ , так что  $F = f_1^2 - 2f_2$ .

$$2. \quad F(x_1, x_2, \dots, x_n) = x_1^3 + x_2^3 + \dots + x_n^3.$$

Первым членом представления является  $f_1^3$ . Во избежание громоздких вычислений применим следующий прием. Прежде всего выясним, какие показатели могут быть у высших членов симметрического однородного полинома третьей степени. Задача эта сводится к разбиению числа 3 на невозрастающие слагаемые. Таких разбиений три:  $3 = 3$ ;  $3 = 2 + 1$ ;  $3 = 1 + 1 + 1$ . Поэтому представление однородного симметрического полинома третьей степени имеет вид  $Af_1^3 + Bf_1f_2 + Cf_3$ . Нужно найти коэффициенты. Очевидно, что  $A = 1$ , ибо таков коэффициент при  $x_1^3$ . Таким образом,

$$x_1^3 + x_2^3 + \dots + x_n^3 = f_1^3 + Bf_1f_2 + Cf_3.$$

Это равенство должно быть тождественным, т. е. сохраняться при всех значениях букв  $x_1, x_2, \dots, x_n$ . Положим  $x_1 = x_2 = 1, x_3 = \dots = x_n = 0$ . Левая часть равна 2, правая равна  $2^3 + 2B$ , откуда  $B = -3$ . Положим теперь  $x_1 = x_2 = x_3 = 1, x_4 = \dots = x_n = 0$ . В левой части будет 3, в правой  $3^3 - 3 \cdot 3 \cdot 3 + C$ , откуда  $C = 3$ . Итак:

$$x_1^3 + x_2^3 + \dots + x_n^3 = f_1^3 - 3f_1f_2 + 3f_3.$$

$$3. \quad F = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

Этот пример нам понадобится в § 3.

Ясно, что  $F$  — симметрический полином и его высший член равен  $x_1^4x_2^2$ . Нам следует установить показатели высших членов, которые встретятся при представлении  $F$  в виде полинома от основных. Эти показатели должны составлять разбиения числа 6 на три или меньше невозрастающих слагаемых, причем эти разбиения должны быть лексикографически не выше разбиения  $6 = 4 + 2$ . Такими разбиениями являются  $4 + 2, 4 + 1 + 1, 3 + 3, 3 + 2 + 1, 2 + 2 + 2$ . Поэтому представление  $F$  через основные имеет вид

$$F = f_1^2f_2^2 + Af_1^3f_3 + Bf_2^3 + Cf_1f_2f_3 + Df_3^2.$$

Зададим такими значениями для  $x_1, x_2, x_3$ , чтобы в правой части были нули, но аннулировались бы не все слагаемые. Например, рассмотрим следующую таблицу значений:

$x_1$	$x_2$	$x_3$	$f_1$	$f_2$	$f_3$	$F$
1	-1	0	0	-1	0	4
1	1	-2	0	-3	-2	0
2	2	-1	3	0	-4	0
1	1	1	3	3	1	0

Подставляя значения из этой таблицы, получим:

$$4 = -B,$$

$$0 = -27B + 4D,$$

$$0 = -108A + 16D,$$

$$0 = 81 + 27A + 27B + 9C + D,$$

откуда  $B = -4, D = -27, A = -4, C = 18$ .

Итак,  $F = f_1^2f_2^2 - 4f_1^3f_3 - 4f_2^3 + 18f_1f_2f_3 - 27f_3^2$ .

## § 2. Значения симметрических полиномов от корней полинома

1. Выражения значений симметрических полиномов от корней полинома через его коэффициенты. Пусть полином  $f(x) \equiv a_0x^n + a_1x^{n-1} + \dots + a_n \in K[x]$  имеет корни  $c_1, c_2, \dots, c_n$  в некото-

ром расширения поля  $K$ . Тогда

$$f(x) = a_0(x - c_1)(x - c_2) \dots (x - c_n).$$

Раскрыв скобки и сравнив коэффициенты при степенях буквы  $x$ , получим:

$$\begin{aligned} a_1 &= -a_0(c_1 + c_2 + \dots + c_n), \\ a_2 &= a_0(c_1c_2 + c_1c_3 + \dots + c_{n-1}c_n), \\ &\dots \dots \dots \\ a_{n-1} &= (-1)^{n-1}a_0(c_1c_2 \dots c_{n-1} + \dots + c_2c_3 \dots c_n), \\ a_n &= (-1)^n a_0 c_1 c_2 \dots c_n. \end{aligned}$$

Мы видим, что значения основных симметрических полиномов от  $c_1, c_2, \dots, c_n$  просто выражаются через коэффициенты:

$$\begin{aligned} f_1(c_1, c_2, \dots, c_n) &= -\frac{a_1}{a_0}, \\ f_2(c_1, c_2, \dots, c_n) &= \frac{a_2}{a_0}, \\ &\dots \dots \dots \\ f_{n-1}(c_1, c_2, \dots, c_n) &= (-1)^{n-1} \frac{a_{n-1}}{a_0}, \\ f_n(c_1, c_2, \dots, c_n) &= (-1)^n \frac{a_n}{a_0}. \end{aligned}$$

Пусть теперь  $F(x_1, x_2, \dots, x_n) = Ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} + \dots$  — симметрический полином с высшим членом  $Ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ . Тогда

$$F(x_1, x_2, \dots, x_n) = Af_1^{\alpha_1 - \alpha_2} f_2^{\alpha_2 - \alpha_3} \dots f_n^{\alpha_n} + Bf_1^{\beta_1 - \beta_2} f_2^{\beta_2 - \beta_3} \dots f_n^{\beta_n} + \dots$$

Следовательно,

$$\begin{aligned} F(c_1, c_2, \dots, c_n) &= A \left(-\frac{a_1}{a_0}\right)^{\alpha_1 - \alpha_2} \left(\frac{a_2}{a_0}\right)^{\alpha_2 - \alpha_3} \dots \\ &\dots \left((-1)^{n-1} \frac{a_{n-1}}{a_0}\right)^{\alpha_{n-1} - \alpha_n} \left((-1)^n \frac{a_n}{a_0}\right)^{\alpha_n} + B \left(-\frac{a_1}{a_0}\right)^{\beta_1 - \beta_2} \left(\frac{a_2}{a_0}\right)^{\beta_2 - \beta_3} \dots \\ &\dots \left((-1)^{n-1} \frac{a_{n-1}}{a_0}\right)^{\beta_{n-1} - \beta_n} \left((-1)^n \frac{a_n}{a_0}\right)^{\beta_n} + \dots \end{aligned}$$

В первое слагаемое множитель  $-1$  войдет с показателем  $\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \dots \equiv \alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_n \pmod{2}$ . Но  $\alpha_1 + \alpha_2 + \dots + \alpha_n = m$  — степень одночлена  $Ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ . Если полином  $F$  однородный степени  $m$ , то во все слагаемые войдет множитель  $(-1)^m$ . В знаменатель первого слагаемого правой части войдет  $a_0^{\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \dots + \alpha_n} = a_0^{\alpha_1}$ , соответственно в знаменатель второго слагаемого войдет  $a_0^{\beta_1}$ , причем  $\beta_1 \leq \alpha_1$  и т. д. Поэтому

для однородного симметрического полинома степени  $m$  будет

$$(-1)^m a_0^{a_1} F(c_1, c_2, \dots, c_n) = \\ = A a_1^{a_1 - a_2} a_2^{a_2 - a_3} \dots a_n^{a_n} + B a_0^{a_1 - \beta_1} a_1^{\beta_1 - \beta_2} a_2^{\beta_2 - \beta_3} \dots a_n^{\beta_n} + \dots,$$

т. е.  $a_0^{a_1} F(c_1, c_2, \dots, c_n)$  является полиномом от коэффициентов полинома  $f(x)$ .

Пример. Доказать, что корни полинома

$$x^{100} + x^{98} + a_3 x^{97} + \dots + a_n$$

не могут быть все вещественными при любых вещественных коэффициентах  $a_3, \dots, a_n$ .

Действительно, сумма квадратов корней равна  $a_1^2 - 2a_2 = -2$ . Если бы все корни были вещественные, сумма их квадратов была бы положительным числом.

**2. Степенные суммы.** Пусть  $f(x) = (x - x_1)(x - x_2) \dots (x - x_n) = x^n - f_1 x^{n-1} + f_2 x^{n-2} + \dots + (-1)^n f_n$ . Вспомним, что

$$f'(x) = (x - x_2)(x - x_3) \dots (x - x_n) + (x - x_1)(x - x_3) \dots$$

$$\dots (x - x_n) + \dots + (x - x_1)(x - x_2) \dots (x - x_{n-1}) = \sum_{i=1}^n \frac{f(x)}{x - x_i}.$$

Вычислим  $\frac{f(x)}{x - x_i}$ , воспользовавшись схемой Хорнера. В результате последовательно получим коэффициенты частного:

$$1, x_i - f_1, x_i^2 - f_1 x_i + f_2, \dots, x_i^{n-1} - f_1 x_i^{n-2} + \dots + (-1)^{n-1} f_{n-1}.$$

Таким образом, коэффициент при  $x^{n-1-k}$  равен

$$x_i^k - f_1 x_i^{k-1} + f_2 x_i^{k-2} - \dots + (-1)^k f_k.$$

Выполнив сложение по  $i$ , получим в качестве коэффициента при  $x^{n-1-k}$  выражение

$$s_k - f_1 s_{k-1} + f_2 s_{k-2} - \dots + (-1)^{k-1} f_{k-1} s_1 + (-1)^k n f_k,$$

где  $s_1, s_2, \dots$  обозначают суммы соответствующих степеней  $x_1, x_2, \dots, x_n$ . Приравнявая это выражение к коэффициенту при  $x^{n-1-k}$  в  $f'(x)$ , получим:

$$s_k - f_1 s_{k-1} + f_2 s_{k-2} - \dots + (-1)^{k-1} f_{k-1} s_1 + (-1)^k n f_k = \\ = (-1)^k (n - k) f_k,$$

откуда

$$s_k - f_1 s_{k-1} + f_2 s_{k-2} - \dots + (-1)^{k-1} f_{k-1} s_1 + (-1)^k k f_k = 0, \\ k = 1, \dots, n - 1,$$

Эти формулы Ньютона позволяют последовательно выражать степенные суммы  $s_k$  через основные симметрические полиномы для  $k$  от 1 до  $n-1$ .

Для  $k \geq n$  аналогичные формулы выводятся еще проще. Умножив равенство  $x_i^n - f_1 x_i^{n-1} + \dots + (-1)^n f_n = 0$  на  $x_i^{k-n}$ , получим

$$x_i^k - f_1 x_i^{k-1} + \dots + (-1)^n f_n x_i^{k-n} = 0.$$

Просуммировав по  $i$ , получим:

$$s_k - f_1 s_{k-1} + \dots + (-1)^n f_n s_{k-n} = 0.$$

**3. Дискриминант полинома.** Дискриминант полинома, говоря неформально, есть полином от его коэффициентов, обращение в нуль которого является необходимым и достаточным условием существования кратного корня. В качестве полинома от корней, обращающегося в нуль при наличии кратного корня, естественно взять произведение всевозможных разностей корней или, что то же самое, определитель Вандермонда от корней. Но этот полином не симметрический, он меняет знак при нечетных подстановках корней. Его квадрат  $(x_1 - x_2)^2 (x_1 - x_3)^2 \dots (x_{n-1} - x_n)^2$  будет уже симметрическим полиномом. Буква  $x_1$  входит в высший член этого полинома с показателем  $2n-2$ . Поэтому  $a_0^{2n-2} (x_1 - x_2)^2 \dots (x_{n-1} - x_n)^2$  является полиномом от коэффициентов полинома  $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ , если вместо букв  $x_1, x_2, \dots, x_n$  подставить корни полинома. Этот полином и называется *дискриминантом*  $D(f)$  полинома  $f(x)$ .

Подсчитаем дискриминант для  $n=2$  и  $n=3$ . При  $n=2$  будет  $D(f) = a_0^2 (x_1 - x_2)^2 = a_0^2 (f_1^2 - 4f_2) = a_0^2 \left( \frac{a_1^2}{a_0^2} - \frac{4a_2}{a_0} \right) = a_1^2 - 4a_0 a_2$ , так что мы получили хорошо известный дискриминант квадратного трехчлена.

При  $n=3$  имеем  $D(f) = a_0^4 (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ . Этот симметрический полином мы выразили через основные в качестве последнего примера в п. 4 § 1. Было получено:

$$(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = f_1^2 f_2^2 - 4f_1^3 f_3 - 4f_2^3 + 18f_1 f_2 f_3 - 27f_3^2.$$

Подставив вместо  $x_1, x_2, x_3$  корни полинома  $f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3$ , получим

$$(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = \frac{a_1^2 a_2^2}{a_0^4} - \frac{4a_1^3 a_3}{a_0^4} - \frac{4a_2^3}{a_0^3} + 18 \frac{a_1 a_2 a_3}{a_0^3} - 27 \frac{a_3^2}{a_0^2},$$

откуда

$$D(f) = a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 a_0 + 18a_0 a_1 a_2 a_3 - 27a_0^2 a_3^2.$$

Для полинома  $f(x) = x^3 + px + q$  будет

$$D(f) = -4p^3 - 27q^2 = -108 \left( \frac{q^2}{4} + \frac{p^3}{27} \right),$$

так что дискриминант в этом случае лишь множителем — 108 отличается от выражения, находящегося под знаком квадратного корня в формуле Кардано.

Дискриминанты полиномов более высокой степени имеют, при явном выражении через коэффициенты, очень сложный вид. Однако существуют представления дискриминанта в виде определителя. Одно, самое простое в теоретическом плане, представление получается так:

$$D(f) = a_0^{2n-2} \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}^2 =$$

$$= a_0^{2n-2} \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

Воспользовавшись тем, что произведение определителей равно определителю произведения их матриц, получим:

$$D(f) = a_0^{2n-2} \begin{vmatrix} n & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix},$$

где  $s_i$  — сумма степеней корней.

Существуют более удобные для вычислений представления дискриминанта в виде определителя, но мы не будем на этом останавливаться.

**4. Алгебраическое решение уравнений третьей и четвертой степени в свете теории симметрических полиномов.** Пусть  $F(x_1, x_2, \dots, x_n)$  — некоторый полином от  $x_1, x_2, \dots, x_n$ . Под действием некоторых подстановок букв  $x_1, x_2, \dots, x_n$  он может не изменяться. Ясно, что множество подстановок, не меняющих данный полином, образует группу. Эта группа  $H$  является подгруппой всей симметрической группы  $S_n$ , и ее индекс  $k$  равен числу различных полиномов  $F = F_1, F_2, \dots, F_k$ , которые можно получить из полинома  $F$  посредством подстановок  $x_1, x_2, \dots, x_n$ . Под действием этих подстановок полиномы  $F_1, F_2, \dots, F_k$  перемещаются так же, как левые классы смежности группы  $S_n$  по подгруппе  $H$  при умножении на элементы из  $S_n$  справа. Поэтому любой симметрический полином от  $F_1, F_2, \dots, F_k$  есть вместе с тем симметрический полином от  $x_1, x_2, \dots, x_n$ , так что если вместо  $x_1, x_2, \dots, x_n$  подставить корни данного полинома  $\hat{f}(x) = x^n + a_1 x^{n-1} + \dots + a_n$ , то соответствующие значения полиномов  $F_1, F_2, \dots, F_k$  будут кор-

нями полинома степени  $k$  с коэффициентами, выражающимися в виде полиномов от коэффициентов  $a_1, a_2, \dots, a_n$  полинома  $f$ .

Рассмотрим в качестве примера применения этих идей вопрос об алгебраическом решении алгебраических уравнений  $f(x) = 0$  при  $n = 3$  и  $n = 4$  в поле комплексных чисел.

Пусть  $n = 3$ . Рассмотрим полином  $\theta_1 = x_1 + x_2\rho + x_3\rho^2$ , где  $\rho = e^{2\pi i/3}$  — первообразный корень степени 3 из единицы. При круговых подстановках  $x_1, x_2, x_3$  полином  $\theta_1$  приобретает множители  $\rho$  и  $\rho^2$  и, следовательно,  $\theta_1^3$  при этом не меняется. Круговые подстановки образуют подгруппу индекса 2 в симметрической группе  $S_3$ , и представителями классов смежности можно считать 1 и транспозицию  $(x_2, x_3)$ . Она переводит  $\theta_1$  в  $\theta_2 = x_1 + x_2\rho^2 + x_3\rho$  и, соответственно,  $\theta_1^3$  в  $\theta_2^3$ . Поэтому  $\theta_1^3 + \theta_2^3$  и  $\theta_1^3\theta_2^3$  являются симметрическими полиномами от  $x_1, x_2, x_3$ .

Именно,  $\theta_1^3 + \theta_2^3 = 2x_1^3 + 2x_2^3 + 2x_3^3 - 3(x_1^2x_2 + \dots) + 12x_1x_2x_3 = = 2f_1^3 - 9f_1f_2 + 27f_3$ . Симметрическим оказывается не только  $\theta_1^3\theta_2^3$ , но и  $\theta_1\theta_2 = x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3 = f_1^2 - 3f_3$ .

Таким образом,  $\theta_1^3$  и  $\theta_2^3$  определяются как корни квадратного уравнения с известными коэффициентами. Затем  $\theta_1$  и  $\theta_2$  находятся посредством извлечения кубического корня, причем значения корней нужно согласовать так, чтобы произведение  $\theta_1\theta_2$  равнялось  $f_1^2 - 3f_3$ . Далее,  $x_1, x_2, x_3$  находятся посредством решения линейной системы

$$\begin{aligned} x_1 + x_2 + x_3 &= f_1, \\ x_1 + x_2\rho + x_3\rho^2 &= \theta_1, \\ x_1 + x_2\rho^2 + x_3\rho &= \theta_2, \end{aligned}$$

которая дает  $x_1 = \frac{1}{3}(f_1 + \theta_1 + \theta_2)$ ,  $x_2 = \frac{1}{3}(f_1 + \theta_1\rho + \theta_2\rho)$ ,  $x_3 = = \frac{1}{3}(f_1 + \theta_1\rho^2 + \theta_2\rho^2)$ .

Легко видеть, что это решение ничем не отличается от решения по формуле Кардано.

Пусть теперь  $n = 4$ . В качестве  $F_1$  возьмем  $x_1x_2 + x_3x_4$ . Полином  $F_1$  не меняется при восьми подстановках, составляющих подгруппу индекса 3 в симметрической группе  $S_4$ . Другие подстановки переводят  $F_1$  в  $F_2 = x_1x_3 + x_2x_4$  и  $F_3 = x_1x_4 + x_2x_3$ . Симметрические полиномы от  $F_1, F_2, F_3$  будут симметрическими и от  $x_1, x_2, x_3, x_4$ . Именно, основные симметрические полиномы будут:

$$\begin{aligned} F_1 + F_2 + F_3 &= f_2, \\ F_1F_2 + F_1F_3 + F_2F_3 &= f_1f_3 - 4f_4, \\ F_1F_2F_3 &= f_1^2f_4 + f_3^2 - 4f_2f_4. \end{aligned}$$

Считая, что  $x_1, x_2, x_3, x_4$  — корни полинома  $x^4 + a_1x^3 + a_2x^2 + + a_3x + a_4$ , мы можем составить кубическое уравнение для  $F_1$ ,

$F_2, F_3$ . Найдя один из корней  $F_1 = x_1x_2 + x_3x_4$ , мы в состоянии найти  $x_1, x_2, x_3, x_4$ , решая цепочку квадратных уравнений. Получается способ, совпадающий со способом Феррари.

Известный под названием метода Эйлера способ получим, если возьмем  $F_1 = (x_1 + x_2 - x_3 - x_4)^2 = f_1^2 - 4f_2 + 4(x_1x_2 + x_3x_4)$ . Полином  $F_1$  не меняется при той же группе из восьми подстановок, что и  $x_1x_2 + x_3x_4$ . Подстановки из классов смежности группы  $S_4$  этой подгруппе переводят  $F_1$  в  $F_2 = (x_1 - x_2 + x_3 - x_4)^2$  и  $F_3 = (x_1 - x_2 - x_3 + x_4)^2$ . Выражения основных симметрических полиномов от  $F_1, F_2, F_3$  дают:

$$F_1 + F_2 + F_3 = 3f_1^2 - 8f_2,$$

$$F_1F_2 + F_1F_3 + F_2F_3 = 3f_1^4 - 16f_1^2f_2 + 16f_2^2 + 16f_1f_3 - 64f_4,$$

$$F_1F_2F_3 = (f_1^3 - 4f_1f_2 + 8f_3)^2,$$

причем симметрическим оказывается и

$$(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4) = f_1^3 - 4f_1f_2 + 8f_3.$$

Таким образом, значения полиномов  $F_1, F_2, F_3$  от корней полинома  $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$  оказываются корнями кубического уравнения с известными коэффициентами. Найдя  $F_1, F_2, F_3$ , нужно извлечь из них квадратные корни, распорядившись знаками корней так, чтобы их произведение равнялось  $f_1^3 - 4f_1f_2 + 8f_3$ .

Корни  $x_1, x_2, x_3, x_4$  найдем из системы линейных уравнений. Получим

$$x_1 = \frac{1}{4}(f_1 + \sqrt{F_1} + \sqrt{F_2} + \sqrt{F_3}),$$

$$x_2 = \frac{1}{4}(f_1 + \sqrt{F_1} - \sqrt{F_2} - \sqrt{F_3}),$$

$$x_3 = \frac{1}{4}(f_1 - \sqrt{F_1} + \sqrt{F_2} - \sqrt{F_3}),$$

$$x_4 = \frac{1}{4}(f_1 - \sqrt{F_1} - \sqrt{F_2} + \sqrt{F_3}).$$

Тонкий анализ близких идей привел Руффини и Абеля к доказательству неразрешимости в радикалах общих уравнений пятой и выше степени. Мы не будем касаться этого трудного вопроса.

### § 3. Результат

**1. Определение результата при помощи симметрических полиномов.** Для двух полиномов  $f(x) \equiv a_0x^n + a_1x^{n-1} + \dots + a_n$  и  $g(x) \equiv b_0x^m + b_1x^{m-1} + \dots + b_m$ ,  $a_0 \neq 0$ ,  $b_0 \neq 0$ , можно построить полином от их коэффициентов так, что обращение его в нуль происходит в том и только в том случае, когда  $f$  и  $g$  не взаимно просты, т. е. если они имеют общий корень в надлежащем расширении основного поля.

Пусть  $x_1, x_2, \dots, x_n$  — корни полинома  $f$ . Симметрический полином  $g(x_1)g(x_2) \dots g(x_n)$  от  $x_1, x_2, \dots, x_n$  обращается в нуль в том и только в том случае, когда один из корней полинома  $f$  является корнем полинома  $g$ . В высший член этого полинома  $x_1$  входит с показателем  $m$ , поэтому  $a_0^m g(x_1)g(x_2) \dots g(x_n)$  является полиномом от коэффициентов  $f$  и, очевидно, полиномом от коэффициентов  $g$ . Этот полином называется *результантом* полиномов  $f$  и  $g$  и обозначается  $R(f, g)$ .

Определение результата кажется не симметричным по отношению к полиномам  $f$  и  $g$ . В действительности это определение «почти симметрично», именно,  $R(g, f) = (-1)^{mn} R(f, g)$ . Для доказательства этой формулы введем в рассмотрение корни  $y_1, y_2, \dots, y_m$  полинома  $g$ , так что  $g(x) = b_0(x - y_1)(x - y_2) \dots (x - y_m)$ . Тогда  $g(x_1)g(x_2) \dots g(x_n) = b_0^n \prod_{i,j} (x_i - y_j)$  и  $R(f, g) = a_0^m b_0^n \prod_{i,j} (x_i - y_j) = (-1)^{mn} a_0^m b_0^n \prod_{i,j} (y_j - x_i)$ .

Далее,  $a_0 \prod_i (y_j - x_i) = f(y_j)$ , так что  $R(f, g) = (-1)^{mn} b_0^n \prod_j f(y_j) = (-1)^{mn} R(g, f)$ .

Отметим еще некоторые свойства результата. Прежде всего ясно, что результат является однородным полиномом степени  $n$  от коэффициентов полинома  $g$  и, в силу соотношения  $R(g, f) = (-1)^{mn} R(f, g)$ , однородным полиномом степени  $m$  от коэффициентов полинома  $f$ .

Далее, назовем весом одночлена  $a_0^{\alpha_0} a_1^{\alpha_1} \dots a_n^{\alpha_n} b_0^{\beta_0} b_1^{\beta_1} \dots b_m^{\beta_m}$  число  $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n + \beta_1 + 2\beta_2 + \dots + m\beta_m$ . Ясно, что веса коэффициентов  $a_1, \dots, a_n$  равны степеням соответствующих основных симметрических полиномов от  $x_1, x_2, \dots, x_n$  и веса  $b_1, \dots, b_m$  равны степеням соответствующих основных симметрических полиномов от  $y_1, y_2, \dots, y_m$ , веса же  $a_0$  и  $b_0$  считаются равными нулю. Поэтому вес одночлена  $a_0^{\alpha_0} a_1^{\alpha_1} \dots a_n^{\alpha_n} b_0^{\beta_0} b_1^{\beta_1} \dots b_m^{\beta_m}$  равен полной степени этого одночлена, рассматриваемого как полином от  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ . Но результат  $a_0^m b_0^n \prod_{i,j} (x_i - y_j)$  есть однородный полином степени  $mn$  относительно  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ . Поэтому веса всех одночленов, составляющих результат, одинаковы и равны  $mn$ .

В качестве примера приведем результат полиномов  $f = a_0 x^2 + a_1 x + a_2$  и  $g = b_0 x^2 + b_1 x + b_2$ . Вычисления здесь не представляют труда, и мы выпишем результат этих вычислений:

$$R(f, g) = a_0^2 b_2^2 - a_0 a_1 b_1 b_2 + a_0 a_2 b_1^2 - 2a_0 a_2 b_0 b_2 + a_1^2 b_0 b_2 - a_1 a_2 b_0 b_1 + a_2^2 b_0^2.$$

**2. Другой способ построения результата.** Для взаимной простоты полиномов

$$f = a_0 x^n + a_1 x^{n-1} + \dots + a_n \text{ и } g = b_0 x^m + b_1 x^{m-1} + \dots + b_m$$



Сперва предположим, что  $x_i$  попарно различны. Умножим матрицу  $M$  слева на матрицу:

$$L = \left( \begin{array}{ccc|ccc} x_1^{m+n-1} & \dots & & x_1^{n-1} & \dots & x_1 & 1 \\ x_2^{m+n-1} & \dots & & x_2^{n-1} & \dots & x_2 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ x_n^{m+n-1} & \dots & & x_n^{n-1} & \dots & x_n & 1 \\ \hline & & E_m & & & 0 & \end{array} \right).$$

Определитель этой матрицы равен

$$(-1)^{mn} \begin{vmatrix} x_1^{n-1} & \dots & x_1 & 1 \\ x_2^{n-1} & \dots & x_2 & 1 \\ \dots & \dots & \dots & \dots \\ x_n^{n-1} & \dots & x_n & 1 \end{vmatrix} \neq 0.$$

При выполнении умножения  $L$  на  $M$  примем во внимание, что  $a_0 x_i^m + a_1 x_i^{m-1} + \dots + a_n = 0$  и  $b_0 x_i^m + b_1 x_i^{m-1} + \dots + b_n = g(x_i)$ .

Получим:

$$LM = \left( \begin{array}{ccc|cccc} & & & x_1^{n-1} g(x_1) & x_1^{n-2} g(x_1) & \dots & g(x_1) \\ & & 0 & x_2^{n-1} g(x_2) & x_2^{n-2} g(x_2) & \dots & g(x_2) \\ & & & \dots & \dots & \dots & \dots \\ & & & x_n^{n-1} g(x_n) & x_n^{n-2} g(x_n) & \dots & g(x_n) \\ \hline a_0 & & & b_0 & & & \\ a_1 & a_0 & & b_1 & & b_0 & \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ a_{m-1} & a_{m-2} & \dots & a_0 & b_{m-1} & b_{m-2} & \dots & b_0 \end{array} \right).$$

В нижних клетках выше  $a_0$  и выше  $b_0$  находятся нули. Поэтому

$$\det LM = (-1)^{mn} a_0^m g(x_1) g(x_2) \dots g(x_n) \begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \dots & 1 \\ x_2^{n-1} & x_2^{n-2} & \dots & 1 \\ \dots & \dots & \dots & \dots \\ x_n^{n-1} & x_n^{n-2} & \dots & 1 \end{vmatrix}.$$

Поделив обе части равенства на  $\det L \neq 0$ , получим

$$\det M = a_0^m g(x_1) g(x_2) \dots g(x_n) = R(f, g).$$

Равенство  $\det M = R(f, g)$  установлено в предположении, что  $x_1, x_2, \dots, x_n$  попарно различны, а это равносильно тому, что дискриминант  $D(f)$  полинома  $f$  отличен от нуля.

Итак,  $\det M$  и  $R(f, g)$  оба являются полиномами от коэффициентов  $f$  и  $g$  и они принимают одинаковые значения при условии, что полином  $D(f)$  отличен от нуля. По предложению о несущественности алгебраических неравенств (стр. 71)  $\det M$  и  $R(f, g)$  равны тождественно.

**3. Линейное представление результата.** Пусть полиномы  $f$  и  $g$  взаимно просты, так что их результат отличен от нуля. Тогда существуют такие полиномы  $p$  и  $q$ , что  $pf + qg = 1$ . Если потребовать, чтобы степени  $q$  и  $p$  были меньше, соответственно, степеней  $f$  и  $g$ , то такие  $q$  и  $p$  определены однозначно. Положив, как в предыдущем пункте,  $p = c_0x^{m-1} + \dots + c_{m-1}$  и  $q = d_0x^{n-1} + \dots + d_{n-1}$ , мы получим для определения коэффициентов систему линейных уравнений с матрицей  $M$  и со столбцом в правой части, состоящим из нулей, кроме последней компоненты, равной 1. По формулам Крамера коэффициенты  $c_0, \dots, c_{m-1}$  являются частными от деления первых  $m$  алгебраических дополнений последней строки определителя матрицы  $M$  на  $\det M = R(f, g)$ , а коэффициенты  $d_0, \dots, d_{n-1}$  суть частные от деления на  $\det M$  алгебраических дополнений с номерами от  $m+1$  до  $n$  элементов последней строки. Положив  $(\det M)p = P$ ,  $(\det M)q = Q$ , получим, что коэффициенты  $P$  и  $Q$  будут полиномами от коэффициентов  $f$  и  $g$ , и имеет место равенство

$$Pf + Qg = R(f, g).$$

Ясно, что полином  $P$  равен определителю матрицы, получающейся из матрицы  $M$  заменой первых  $m$  элементов последней строки на  $x^{m-1}, x^{m-2}, \dots, 1$ , а остальных — на нули. Соответственно, полином  $Q$  равен определителю матрицы, получающейся из  $M$  заменой первых  $m$  элементов последней строки на нули, а последующих — на  $x^{n-1}, x^{n-2}, \dots, 1$ .

**4. Применение результата к исключению неизвестного из системы двух алгебраических уравнений с двумя неизвестными.** Пусть дана система уравнений

$$\begin{aligned} f(x, y) &= 0, \\ g(x, y) &= 0, \end{aligned}$$

где  $f$  и  $g$  — полиномы степеней  $n$  и  $m$  соответственно. Будем предполагать, что коэффициенты полиномов принадлежат алгебраически замкнутому полю и решения разыскиваются в этом поле. (Заметим, что алгебраически замкнутое поле даже в случае ненулевой характеристики содержит бесконечно много элементов. Действительно, к любой конечной системе элементов  $\alpha_1, \alpha_2, \dots, \alpha_n$  можно присоединить новый элемент, например, корень полинома  $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) + 1$ .)

Пусть  $c_0x^n + c_1x^{n-1}y + \dots + c_ny^n$  — однородная часть степени  $n$  полинома  $f(x, y)$ . Возможно, что  $c_0 = 0$ . Сделаем «перекося осей абсцисс» посредством замены неизвестной  $y$  на  $y' = y - \alpha x$  (новая ось абсцисс  $y' = 0$  имеет в исходных координатах  $x, y$  уравнение  $y - \alpha x = 0$ ). Коэффициент при  $x^n$  станет равным  $c_0 + c_1\alpha + \dots + c_n\alpha^n$ , и  $\alpha$  можно выбрать так, что  $a_0 = c_0 + c_1\alpha + \dots + c_n\alpha^n \neq 0$  (это требование налагает конечное число запретов

на выбор  $\alpha$ ). Одновременно можно добиться того, что коэффициент при  $x^m$  в  $g(x, y)$  станет отличным от нуля. В дальнейшем мы еще наложим некоторые запреты на выбор «коэффициента перекося»  $\alpha$ .

Ясно, что решение системы

$$\begin{aligned} f(x, y) &= 0, \\ g(x, y) &= 0 \end{aligned}$$

и решение системы после замены  $y$  на  $y' + \alpha x$  тривиально сводятся одно к другому, так что можно с самого начала считать, что коэффициенты  $a_0$  и  $b_0$  при  $x^n$  в полиноме  $f(x, y)$  и при  $x^m$  в полиноме  $g(x, y)$  отличны от нуля.

Итак, пусть  $f(x, y) = a_0 x^n + a_1(y) x^{n-1} + \dots + a_n(y)$  и  $g(x, y) = b_0 x^m + b_1(y) x^{m-1} + \dots + b_m(y)$ ,  $a_0 \neq 0$ ,  $b_0 \neq 0$ . Так как степень  $f(x, y)$  равна  $n$ , степени полиномов  $a_i(y)$  не превосходят  $i$ . Соответственно, степени  $b_j(y)$  не превосходят  $j$ . Составим результат  $R_x(f, g)$ , рассматривая  $f$  и  $g$  как полиномы от  $x$  с коэффициентами, зависящими от  $y$ . Этот результат является полиномом  $F(y)$  от  $y$ , степень которого не превосходит  $mn$ , что следует из того, что вес каждого члена результата равен  $mn$ . Допустим сначала, что результат не равен нулю тождественно. Тогда он имеет конечное число корней, не более чем  $mn$ . Подставив любой корень результата в полиномы  $f(x, y)$  и  $g(x, y)$ , мы получим полиномы от одного неизвестного  $x$ , результат которых равен нулю. Значит, они имеют общие корни, каждый из которых, вместе со значением для  $y$ , дает решение системы. Легко видеть, что все решения находятся на этом пути. Действительно, если  $x_1, y_1$  — решение системы, то зависящие только от  $x$  полиномы  $f(x, y_1)$  и  $g(x, y_1)$  имеют общий корень  $x_1$ , и, следовательно, их результат равен нулю, т. е.  $y_1$  является корнем результата  $F(y) = R_x(f, g)$ .

Таким образом, система  $f(x, y) = 0$ ,  $g(x, y) = 0$  имеет конечное число решений  $(x_i, y_i)$ . Для оценки их числа наложим дополнительные ограничения на коэффициент перекося  $\alpha$ . Именно, потребуем, чтобы в новых неизвестных все решения имели различные ординаты.

Это приводит снова к конечному числу запретов для  $\alpha$ , именно, запрещены равенства  $y_i - \alpha x_i = y_j - \alpha x_j$ . При таком выборе  $\alpha$  для каждого  $y'$  найдется только одно значение для  $x$ . Так как число корней результата не превосходит  $mn$ , то и число решений системы не превосходит  $mn$ .

Если же результат  $R_x(f, g)$  равен нулю тождественно, то для любого  $y$  найдется соответствующее значение для  $x$ , так что система будет иметь бесконечно много решений.

Причиной этого является наличие в этом случае нетривиального общего делителя  $\phi(x, y)$  у полиномов  $f(x, y)$  и  $g(x, y)$ , и любое решение уравнения  $\phi(x, y) = 0$  дает и решение системы.

**5. Связь дискриминанта полинома с результатом полинома и его производной.** Наличие кратного корня у полинома  $f(x) =$

$= a_0 x^n + a_1 x^{n-1} + \dots + a_n$  равносильно наличию общего корня  $f(x)$  и его производной. Поэтому обращение в нуль  $R(f, f')$  равносильно обращению в нуль дискриминанта. Следовательно,  $R(f, f')$  и  $D(f)$  должны быть тесно связаны. Найдем эту связь.

Пусть  $f(x) = a_0(x - x_1)(x - x_2) \dots (x - x_n)$ . Тогда

$$f'(x_1) = a_0(x_1 - x_2) \dots (x_1 - x_n),$$

$$f'(x_2) = a_0(x_2 - x_1)(x_2 - x_3) \dots (x_2 - x_n),$$

$$\dots \dots \dots$$

$$f'(x_n) = a_0(x_n - x_1)(x_n - x_2) \dots (x_n - x_{n-1}).$$

Следовательно,

$$R(f, f') = a_0^{n-1} f'(x_1) f'(x_2) \dots f'(x_n) = a_0^{2n-1} (x_1 - x_2) \dots$$

$$\dots (x_1 - x_n)(x_2 - x_1) \dots (x_2 - x_n) \dots (x_n - x_1) \dots (x_n - x_{n-1}).$$

Каждая разность  $x_i - x_j$  входит в полученное произведение два раза с противоположными знаками. Поэтому

$$R(f, f') = a_0^{2n-1} (-1)^{\frac{n(n-1)}{2}} \prod_{i>j} (x_i - x_j)^2 = a_0 (-1)^{\frac{n(n-1)}{2}} D(f).$$

Тем самым предполагаемая связь установлена.

## ВЕКТОРНЫЕ ПРОСТРАНСТВА

### § 1. Определения и простейшие свойства

**1. Определение и примеры.** Напомним (стр. 75), что *векторным пространством*  $S$  над полем  $K$  называется аддитивно записанная абелева группа, для элементов которой определено действие умножения на элементы поля  $K$ , удовлетворяющее требованиям:

$$c(u_1 + u_2) = cu_1 + cu_2,$$

$$(c_1 + c_2)u = c_1u + c_2u,$$

$$c_1(c_2u) = (c_1c_2)u,$$

$$1 \cdot u = u,$$

где  $c, c_1, c_2, 1$  — элементы поля  $K$ ,  $u, u_1, u_2$  — элементы векторного пространства. Элементы векторного пространства будем называть *векторами*, элементы поля  $K$  для краткости будем называть числами (хотя они могут иметь другую природу).

Примерами векторных пространств над полем  $\mathbb{R}$  вещественных чисел могут служить множества векторов на плоскости или в пространстве. Другие (уже над любым полем  $K$ ) примеры — матрицы фиксированного строения, в частности, строки и столбцы с элементами из поля  $K$ , полиномы от одной (или нескольких) букв с коэффициентами из поля  $K$ , полиномы ограниченной степени с коэффициентами из поля  $K$ .

Исследование векторных пространств составляет содержание линейной алгебры.

В приложениях линейной алгебры к другим математическим дисциплинам рассматриваются преимущественно векторные пространства над полями  $\mathbb{C}$  и  $\mathbb{R}$ . В теории информации полезными оказываются векторные пространства над конечными полями, особенно над полем  $\text{GF}(2)$  из двух элементов.

Отметим еще свойства нуля векторного пространства.

1.  $0 \cdot u = 0$ . Действительно,  $0 \cdot u + 0 \cdot u = (0 + 0)u = 0 \cdot u$ . Добавив к обеим частям этого равенства элемент, противоположный к  $0 \cdot u$ , получим  $0 \cdot u = 0$ .

2.  $c \cdot 0 = 0$ . Действительно,  $c \cdot 0 + c \cdot 0 = c(0 + 0) = c \cdot 0$ , откуда  $c \cdot 0 = 0$ .

3. Если  $cu = 0$ , то либо  $c = 0$ , либо  $u = 0$ . Действительно, если  $c \neq 0$ , то существует  $c^{-1}$  и  $c^{-1}cu = c^{-1}0 = 0$ , т. е.  $u = 0$ .

**2. Линейные комбинации, линейная зависимость и линейная независимость.** *Линейной комбинацией* векторов  $u_1, u_2, \dots, u_m$  из  $S$  называется вектор  $c_1u_1 + c_2u_2 + \dots + c_mu_m$  при  $c_i \in K$ . Ясно, что линейной комбинацией линейных комбинаций векторов  $u_1, \dots, u_m$  является снова линейная комбинация этих векторов.

Совокупность векторов  $u_1, \dots, u_m$  называется *линейно независимой*, если равенство  $c_1u_1 + \dots + c_mu_m = 0$  возможно только при  $c_1 = \dots = c_m = 0$ . Если же существуют не равные одновременно нулю  $c_1, \dots, c_m$  такие, что  $c_1u_1 + \dots + c_mu_m = 0$ , то совокупность векторов  $u_1, \dots, u_m$  называется *линейно зависимой*. Определения эти совпадают с определениями, данными на стр. 108 в применении к строкам.

Предложение 1. *Совокупность векторов  $u_1, \dots, u_m$  линейно зависима в том и только в том случае, когда один из векторов является линейной комбинацией остальных.*

Предложение 2. *Если совокупность векторов  $u_1, \dots, u_m$  линейно независима, а совокупность  $u_1, \dots, u_m, u_{m+1}$  линейно зависима, то вектор  $u_{m+1}$  есть линейная комбинация векторов  $u_1, \dots, u_m$ .*

Предложение 3. *Если векторы  $v_1, \dots, v_k$  являются линейными комбинациями векторов  $u_1, \dots, u_m$  и  $k > m$ , то совокупность  $v_1, \dots, v_k$  линейно зависима.*

Доказательства этих предложений ничем не отличаются от доказательств аналогичных предложений для строк (стр. 108—110).

Совокупность векторов называется *порождающей*, если все векторы пространства являются их линейными комбинациями. Если для пространства  $S$  существует конечная порождающая система, то пространство называется *конечномерным*, в противном случае — *бесконечномерным*. В конечномерном пространстве не могут существовать сколь угодно большие (по числу векторов) линейно независимые совокупности векторов, ибо, согласно предложению 3, любая совокупность векторов, превосходящая по числу векторов порождающую совокупность, линейно зависима.

Пространство матриц фиксированных размеров и, в частности, пространство строк фиксированной длины конечномерны, в качестве порождающей системы можно взять матрицы с единицей на одной позиции и с нулями на остальных.

Пространство всех полиномов от  $x$  уже бесконечномерно, ибо совокупность полиномов  $1, x, x^2, \dots, x^n$  линейно независима при любом  $n$ .

В дальнейшем будем рассматривать конечномерные пространства.

Предложение 4. *Любая минимальная (по числу векторов) порождающая совокупность векторов линейно независима.*

Действительно, пусть  $u_1, \dots, u_n$  — минимальная порождающая совокупность векторов. Если она линейно зависима, то один из векторов, скажем  $u_n$ , есть линейная комбинация остальных  $u_1, \dots$

$\dots, u_{n-1}$  и всякая линейная комбинация  $u_1, \dots, u_{n-1}, u_n$  есть линейная комбинация меньшей совокупности векторов  $u_1, \dots, u_{n-1}$ , которая тем самым оказывается порождающей.

*Предложение 5. Любая максимальная (по числу векторов) линейно независимая совокупность векторов является порождающей.*

Действительно, пусть  $u_1, \dots, u_n$  — максимальная линейно независимая совокупность и  $u$  — любой вектор пространства. Тогда совокупность  $u_1, \dots, u_n, u$  не будет линейно независимой, и, в силу предложения 2, вектор  $u$  есть линейная комбинация  $u_1, \dots, u_n$ .

*Предложение 6. Любая линейно независимая порождающая совокупность является минимальной среди порождающих и максимальной среди линейно независимых.*

Действительно, пусть  $u_1, \dots, u_n$  — линейно независимая порождающая совокупность векторов. Если  $v_1, \dots, v_k$  — какая-то другая порождающая совокупность, то  $u_1, \dots, u_n$  являются линейными комбинациями  $v_1, \dots, v_k$ , и отсюда заключаем, что  $n \leq k$ , ибо если было бы  $n > k$ , то, в силу предложения 3,  $u_1, \dots, u_n$  была бы линейно зависимой совокупностью. Пусть теперь  $w_1, \dots, w_m$  — какая-либо линейно независимая совокупность. Векторы  $w_1, \dots, w_m$  являются линейными комбинациями векторов  $u_1, \dots, u_n$  и, следовательно,  $m \leq n$ , ибо при  $m > n$ , в силу того же предложения 3,  $w_1, \dots, w_m$  составляли бы линейно зависимую совокупность.

Таким образом, в предложениях 4, 5, 6 устанавливается тождественность трех понятий — минимальная порождающая совокупность векторов, максимальная линейно независимая совокупность векторов и линейно независимая порождающая совокупность.

Совокупность векторов, удовлетворяющая этим условиям, называется *базисом* пространства, а число векторов, составляющих базис, называется *размерностью* пространства. Размерность пространства  $S$  обозначается  $\dim S$ . Таким образом, размерность равна максимальному числу линейно независимых векторов (мы часто в дальнейшем будем говорить слова «линейно независимые» и «линейно зависимые векторы» вместо того, чтобы сказать «векторы, составляющие линейно зависимую совокупность» и — соответственно — для линейно независимой совокупности) и минимальному числу порождающих векторов.

*Предложение 7. Пусть  $u_1, \dots, u_m$  — линейно независимая совокупность векторов, причем их число меньше размерности пространства. Тогда к ним можно присоединить вектор  $u_{m+1}$  так, что совокупность  $u_1, \dots, u_m, u_{m+1}$  останется линейно независимой.*

*Доказательство.* Рассмотрим множество линейных комбинаций  $c_1 u_1 + \dots + c_m u_m$ . Оно не исчерпывает всего пространства, ибо  $u_1, \dots, u_m$  не составляют порождающую совокупность векторов. Возьмем вектор, не являющийся линейной комбинацией  $u_1, \dots, u_m$ . Тогда  $u_1, \dots, u_m, u_{m+1}$  — линейно независимая сово-

купность, так как иначе  $u_{m+1}$  был бы линейной комбинацией векторов  $u_1, \dots, u_m$ , в силу предложения 2.

Из предложения 7 следует, что любую линейно независимую совокупность векторов можно дополнить до базиса.

Это же предложение и его доказательство указывают на характер произвола в выборе базиса. Действительно, если взять произвольной ненулевой вектор, то его можно достраивать до базиса, взяв второй вектор как угодно, только не линейную комбинацию первого, третий как угодно, только не линейную комбинацию первых двух, и т. д.

К базису можно «спуститься», исходя из произвольной порождающей совокупности.

**Предложение 8.** *Любая порождающая совокупность векторов содержит базис.*

Действительно, пусть  $u_1, u_2, \dots, u_m$  — порождающая совокупность векторов. Если она линейно зависима, то один из ее векторов есть линейная комбинация остальных, и его можно исключить из порождающей совокупности. Если оставшиеся векторы линейно зависимы, то можно исключить еще один вектор, и т. д., до тех пор пока не останется линейно независимая порождающая совокупность, т. е. базис.

**3. Координаты вектора.** Пусть  $e_1, \dots, e_n$  — базис  $n$ -мерного пространства  $S$  над полем  $K$  и  $x$  — произвольный вектор этого пространства. Тогда  $x$  есть линейная комбинация  $e_1, \dots, e_n$ :

$$x = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$$

при  $x_i \in K$ .

Такое представление единственно. Действительно, если  $x = x'_1 e_1 + x'_2 e_2 + \dots + x'_n e_n$ , то

$$(x'_1 - x_1) e_1 + (x'_2 - x_2) e_2 + \dots + (x'_n - x_n) e_n = 0,$$

и, в силу линейной независимости базиса,  $x'_1 - x_1 = x'_2 - x_2 = \dots = x'_n - x_n = 0$ , т. е.

$$x'_1 = x_1, \quad x'_2 = x_2, \quad \dots, \quad x'_n = x_n.$$

Коэффициенты  $x_1, x_2, \dots, x_n$  называются координатами вектора  $x$ . Координаты вектора будем представлять себе в виде столбца.

Два векторных пространства над одним и тем же полем называются *изоморфными*, если между их элементами имеется взаимно однозначное соответствие (изоморфизм), сохраняющее линейные комбинации. Из определения ясно, что образ при изоморфизме линейно зависимой совокупности векторов будет линейно зависимой совокупностью, образ линейно независимой совокупности будет линейно независимой совокупностью, образ порождающей совокупности будет порождающей совокупностью, и, следовательно,





рядке. Действительно,

$$((A_1 A_2 \dots A_k)^T)^{-1} = (A_k^T \dots A_2^T A_1^T)^{-1} = (A_1^T)^{-1} (A_2^T)^{-1} \dots (A_k^T)^{-1}.$$

Таким образом, переход к контраградиентным есть автоморфизм в группе всех невырожденных матриц.

## § 2. Подпространства

**1. Определение и размерность.** Подпространством  $P$   $n$ -мерного пространства  $S$  называется множество векторов, образующих векторное пространство по отношению к действиям, которые определены в  $S$ . Иными словами, подпространство есть множество векторов, содержащее вместе с любым конечным множеством векторов все их линейные комбинации. Подпространство  $n$ -мерного пространства конечномерно и его размерность не превосходит  $n$ . Действительно, любая линейно независимая совокупность векторов из  $P$  будет линейно независимой и по отношению к  $S$ , так что максимальное число линейно независимых векторов из  $P$  не превосходит  $n$ , т. е.  $\dim P \leq \dim S$ .

Если  $\dim P = \dim S = n$ , то  $P = S$ . Действительно, в этой ситуации базис  $P$  есть линейно независимая совокупность векторов, содержащая  $n$  элементов, т. е. она максимальна, базис  $P$  есть вместе с тем базис  $S$ , и следовательно, подпространство  $P$  совпадает с  $S$ .

В любом пространстве  $S$  существуют два тривиальных подпространства — само  $S$  и подпространство, состоящее только из нулевого вектора. При  $n > 1$  имеются и нетривиальные подпространства. Строить их можно так. Взять любую конечную совокупность векторов  $u_1, \dots, u_m$  и ввести в рассмотрение множество всех их линейных комбинаций  $c_1 u_1 + \dots + c_m u_m$ . Это множество, очевидно, есть подпространство. Его размерность равна  $m$ , если  $u_1, \dots, u_m$  линейно независимы, и меньше  $m$ , если они линейно зависимы. Поэтому в  $n$ -мерном пространстве существуют нетривиальные подпространства всех возможных размерностей, от 1 до  $n - 1$ .

В силу предложения 7 предыдущего параграфа базис любого подпространства может быть дополнен до базиса всего пространства.

**2. Сумма и пересечение подпространств.** Пусть  $P$  и  $Q$  — два подпространства пространства  $S$ . Их суммой  $P + Q$  называется множество векторов  $x + y$  при  $x \in P$  и  $y \in Q$ . Ясно, что любая линейная комбинация векторов из  $P + Q$  принадлежит  $P + Q$ , так что  $P + Q$  есть подпространство пространства  $S$  (быть может, совпадающее со всем  $S$ ). Далее, пересечение  $P \cap Q$  подпространств  $P$  и  $Q$ , т. е. множество векторов, принадлежащих одновременно  $P$  и  $Q$ , есть, очевидно, подпространство (быть может, состоящее только из нулевого вектора).

Ясно, что подпространства  $P$  и  $Q$  содержатся в  $P + Q$  и  $P + Q$  содержится в любом подпространстве, содержащем  $P$  и  $Q$ . Иными словами,  $P + Q$  есть наименьшее подпространство, содержащее  $P$  и  $Q$ . Пересечение  $P \cap Q$  содержится в  $P$  и  $Q$ , и любое подпространство, содержащееся в  $P$  и  $Q$ , содержится и в  $P \cap Q$ . Это значит, что  $P \cap Q$  есть наибольшее среди подпространств, содержащихся в  $P$  и  $Q$ .

Теорема 1.  $\dim(P + Q) + \dim(P \cap Q) = \dim P + \dim Q$ .

Доказательство. Обозначим  $P + Q = R$  и  $P \cap Q = T$ . Размерности подпространств будем обозначать соответствующими малыми буквами.

Выберем прежде всего базис  $T$ . Пусть это  $e_1, e_2, \dots, e_t$ . Имеем  $T \subset P$  и  $T \subset Q$ . Поэтому базис  $T$  можно дополнить до базиса  $P$  и до базиса  $Q$ . Пусть  $e_1, e_2, \dots, e_t, e_{t+1}, \dots, e_p$  — базис  $P$  и пусть  $e_1, \dots, e_t, e'_{t+1}, \dots, e'_q$  — базис  $Q$ .

Покажем, что векторы  $e_1, \dots, e_t, e_{t+1}, \dots, e_p, e'_{t+1}, \dots, e'_q$  составляют базис  $R = P + Q$ . Любой вектор  $z \in R$  равен  $x + y$  при  $x \in P, y \in Q$ . Следовательно,  $z = x_1 e_1 + \dots + x_t e_t + x_{t+1} e_{t+1} + \dots + x_p e_p + y_1 e_1 + \dots + y_t e_t + y_{t+1} e'_{t+1} + \dots + y_q e'_q$ , так что векторы  $e_1, \dots, e_t, e_{t+1}, \dots, e_p, e'_{t+1}, \dots, e'_q$  порождают  $R$ .

Докажем их линейную независимость. Пусть

$$c_1 e_1 + \dots + c_t e_t + c_{t+1} e_{t+1} + \dots + c_p e_p + c'_{t+1} e'_{t+1} + \dots + c'_q e'_q = 0,$$

откуда

$$\begin{aligned} u = c_1 e_1 + \dots + c_t e_t + c_{t+1} e_{t+1} + \dots + c_p e_p = \\ = -c'_{t+1} e'_{t+1} - \dots - c'_q e'_q. \end{aligned}$$

Вектор  $u$  принадлежит  $P$ , ибо он есть линейная комбинация векторов базиса  $P$ , но вместе с тем  $u \in Q$ , ибо он есть линейная комбинация части базисных векторов  $Q$ . Следовательно,  $u \in P \cap Q$  и является линейной комбинацией векторов базиса этого подпространства:  $u = a_1 e_1 + \dots + a_t e_t$ . Приравнявая это представление  $u$  к его представлению через базис  $Q$ , получим:

$$a_1 e_1 + \dots + a_t e_t = -c'_{t+1} e'_{t+1} - \dots - c'_q e'_q$$

или, что то же самое,

$$a_1 e_1 + \dots + a_t e_t + c'_{t+1} e'_{t+1} + \dots + c'_q e'_q = 0.$$

Но векторы  $e_1, \dots, e_t, e'_{t+1}, \dots, e'_q$  линейно независимы, ибо они составляют базис  $Q$ . Следовательно,  $c'_{t+1} = \dots = c'_q = 0, a_1 = \dots = a_t = 0$  и

$$c_1 e_1 + \dots + c_t e_t + c_{t+1} e_{t+1} + \dots + c_p e_p = 0.$$

В силу линейной независимости базиса подпространства  $P$  получаем

$$c_1 = \dots = c_t = c_{t+1} = \dots = c_p = 0.$$

Итак, все коэффициенты линейной комбинации векторов  $e_1, \dots, \dots, e_t, e_{t+1}, \dots, e_p, e'_{t+1}, \dots, e'_q$  оказались равными нулю. Следовательно, эти векторы линейно независимы. Так как они порождают  $P+Q$ , они составляют базис  $P+Q$ . Их число, т. е.  $\dim(P+Q)$ , равно

$$p+q-t = \dim P + \dim Q - \dim(P \cap Q).$$

Тем самым теорема доказана.

Доказанная теорема служит основой интуиции в вопросе о расположении подпространств в многомерных пространствах. Так, в четырехмерном пространстве  $S$  два двумерных подпространства  $P$  и  $Q$  (т. е. две плоскости, проходящие через начало координат) могут иметь три возможности взаимного расположения. Возможно, что их сумма дает все  $S$ . Тогда  $\dim(P \cap Q) = 0$ , т. е. плоскости пересекаются в одной точке. Возможно, что  $\dim(P+Q) = 3$ , т. е. обе плоскости лежат в трехмерном пространстве и не совпадают. В этом случае  $\dim(P \cap Q) = 1$ , т. е. плоскости пересекаются по прямой. Наконец, если  $\dim(P+Q) = 2$ , то  $P+Q$  совпадает с  $P$ , с  $Q$  и с их пересечением, т. е. это тот случай, когда плоскости  $P$  и  $Q$  совпадают.

**3. Прямая сумма подпространств.** Сумма двух подпространств  $P$  и  $Q$  называется *прямой суммой*, если представление любого вектора из  $P+Q$  в виде суммы вектора из  $P$  и вектора из  $Q$  однозначно, или, что то же самое, из равенства  $u+v=0$  при  $u \in P$ ,  $v \in Q$  следует  $u=0$ ,  $v=0$ . Прямая сумма обозначается  $P \oplus Q$ . Говорят, что если  $S = P \oplus Q$ , то  $S$  *разлагается в прямую сумму* своих подпространств  $P$  и  $Q$ .

*Предложение 2. Для того чтобы сумма  $P+Q$  была прямой, необходимо и достаточно, чтобы  $P \cap Q = 0$ .*

Действительно, если сумма прямая и  $z \in P \cap Q$ , то  $0 = z + (-z)$  при  $z \in P$  и  $-z \in Q$  и, следовательно,  $z = 0$ . Обратно, если  $P \cap Q = 0$  и  $z = u_1 + v_1 = u_2 + v_2$  при  $u_1, u_2 \in P$  и  $v_1, v_2 \in Q$ , то  $u_1 - u_2 = v_2 - v_1$ . В левой части — вектор из  $P$ , в правой — вектор из  $Q$ , следовательно, это — нулевой вектор и  $u_1 = u_2$ ,  $v_1 = v_2$ . Сумма  $P+Q$  прямая.

*Предложение 3. Для того чтобы сумма  $P+Q$  была прямой, необходимо и достаточно, чтобы объединение базисов  $P$  и  $Q$  составляло базис  $P+Q$ .*

Ясно, что объединение базисов  $P$  и  $Q$  порождает  $P+Q$ . Далее, выражая через базисы  $P$  и  $Q$  векторы  $u \in P$  и  $v \in Q$  в равенстве  $u+v=0$ , мы получим равную нулю линейную комбинацию векторов объединения базисов  $P$  и  $Q$ , и она может быть только три-

виальной в том и только в том случае, когда объединение базисов  $P$  и  $Q$  образует линейно независимую совокупность векторов.

Понятие суммы подпространств естественно распространяется на любое конечное число слагаемых подпространств. Именно, суммой  $P_1 + P_2 + \dots + P_k$  называется множество сумм  $u_1 + u_2 + \dots + u_k$  при  $u_i \in P_i$ . Ясно, что, сумма подпространств есть подпространство. Оно порождается объединением базисов слагаемых подпространств. Сумма подпространств называется прямой суммой, если представление ее векторов в виде  $u_1 + u_2 + \dots + u_k$ ,  $u_i \in P_i$ , однозначно или, что то же самое, из равенства  $u_1 + u_2 + \dots + u_k = 0$  при  $u_i \in P_i$  следует, что  $u_i = 0$ ,  $i = 1, \dots, k$ .

Заметим, что можно определить сумму бесконечного множества подпространств  $P_i$ ,  $i \in I$ , как множество конечных сумм векторов из пространств  $P_i$ . Понятие прямой суммы естественно распространяется на случай бесконечного множества подпространств, но оно имеет смысл только для бесконечномерных подпространств.

**Предложение 4.** *Для того чтобы сумма  $P_1 + P_2 + \dots + P_k$  была прямой, необходимо и достаточно, чтобы пересечение каждого из подпространств  $P_i$  с суммой остальных состояло только из нулевого вектора.*

Действительно, если сумма прямая и вектор  $z$  принадлежит  $P_i$  и сумме остальных слагаемых подпространств, то  $z = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_k = 0$  и  $z = 0$ . Обратно, если при всех  $i$  пересечение  $P_i$  с суммой остальных подпространств есть нулевой вектор, то из равенства  $u_1 + \dots + u_{i-1} + u_i + u_{i+1} + \dots + u_k = 0$  следует  $u_i = -u_1 - \dots - u_{i-1} - u_{i+1} - \dots - u_k$ ; откуда  $u_i = 0$ .

**Предложение 5.** *Для того чтобы сумма  $P_1 + P_2 + \dots + P_k$  была прямой, необходимо и достаточно, чтобы объединение базисов  $P_1, P_2, \dots, P_k$  составляло базис суммы.*

Доказательство аналогично доказательству предложения 3.

**Предложение 6.** *Для того чтобы сумма  $P_1 + P_2 + \dots + P_k$  была прямой, необходимо и достаточно, чтобы  $P_1 \cap P_2 = 0$ ,  $(P_1 + P_2) \cap P_3 = 0$ , и т. д., т. е. пересечение каждого подпространства  $P_i$  с суммой предшествующих состояло только из нулевого вектора.*

Необходимость следует из предложения 4. Доказательство достаточности проведем индукцией по числу слагаемых подпространств. Из  $(P_1 + \dots + P_{k-1}) \cap P_k = 0$  следует, что если  $u_1 + \dots + u_{k-1} + u_k = 0$ , то  $u_k = 0$  и  $u_1 + \dots + u_{k-1} = 0$ . В силу индуктивного предположения  $u_1 = \dots = u_{k-1} = 0$ . Базу для индукции дает случай  $k = 2$  (предложение 2).

**4. Относительная линейная независимость и относительный базис.** Пусть  $S$  — векторное пространство и  $P$  — его подпространство. Скажем, что векторы  $u_1, \dots, u_k$  линейно независимы относительно  $P$ , если из включения  $c_1 u_1 + \dots + c_k u_k \in P$  следует, что  $c_1 = \dots = c_k = 0$ .

**Предложение 7.** Для того чтобы совокупность  $u_1, \dots, u_k$  векторов была линейно независима относительно подпространства  $P$ , необходимо и достаточно, чтобы совокупность  $u_1, \dots, u_k, e_1, \dots, e_m$ , где  $e_1, \dots, e_m$  — базис  $P$ , была линейно независимой.

Действительно, если  $u_1, \dots, u_k$  линейно независимы относительно  $P$ , то из  $c_1u_1 + \dots + c_ku_k + b_1e_1 + \dots + b_me_m = 0$  следует, что  $c_1u_1 + \dots + c_ku_k \in P$ , поэтому  $c_1 = \dots = c_k = 0$  и также  $b_1 = \dots = b_m = 0$ , в силу линейной независимости  $e_1, \dots, e_m$ . Обратно, если  $u_1, \dots, u_k, e_1, \dots, e_m$  линейно независимы, то из  $c_1u_1 + \dots + c_ku_k \in P$  следует  $c_1u_1 + \dots + c_ku_k = b_1e_1 + \dots + b_me_m$ , откуда  $c_1 = \dots = c_k = 0$ .

Векторы  $u_1, \dots, u_k$  образуют базис  $S$  относительно  $P$ , если они линейно независимы относительно  $P$  и любой вектор  $x \in S$  представляется в виде их линейной комбинации, с точностью до векторов из  $P$ . Точнее — если  $x = c_1u_1 + \dots + c_ku_k + y$ , при  $y \in P$ .

**Предложение 8.** Для того чтобы векторы  $u_1, \dots, u_k$  составляли базис  $S$  относительно  $P$ , необходимо и достаточно, чтобы векторы  $u_1, \dots, u_k, e_1, \dots, e_m$ , где  $e_1, \dots, e_m$  — базис  $P$ , составляли базис  $S$ .

Действительно, линейная независимость  $u_1, \dots, u_k, e_1, \dots, e_m$  необходима и достаточна для линейной независимости  $u_1, \dots, u_k$  относительно  $P$ . Для того чтобы  $u_1, \dots, u_k$  порождали  $S$  с точностью до векторов из  $P$ , необходимо и достаточно, чтобы  $u_1, \dots, u_k, e_1, \dots, e_m$  порождали  $S$ .

Из предложений 7 и 8 следует, что любая совокупность векторов, дополняющая базис  $P$  до базиса  $S$ , есть базис  $S$  относительно  $P$ . Любая линейно независимая относительно  $P$  совокупность векторов может быть дополнена до базиса  $S$  относительно  $P$ . Число векторов, составляющих базис  $S$  относительно  $P$ , равно разности размерностей  $S$  и  $P$ .

**5. Факторпространство.** Пусть  $S$  — векторное пространство и  $P$  — его подпространство. Скажем, что векторы  $x, y \in S$  сравнимы по подпространству  $P$  (и запишем  $x \equiv y(P)$ ), если  $x - y \in P$ . Ясно, что  $S$  «расслаивается» на классы сравнимых по  $P$  векторов. Далее, если  $x \equiv y(P)$  и  $u \equiv z(P)$ , то  $c_1x + c_2u \equiv c_1y + c_2z(P)$ . Это обстоятельство делает корректным определение операции взятия линейных комбинаций на классах сравнений по  $P$ . Ясно, что классы образуют векторное пространство по отношению к этой операции. Оно называется *факторпространством* и обозначается  $S/P$ . Если отвлечься от операции умножения элементов факторпространства на элемент основного поля,  $S/P$  есть факторгруппа аддитивной группы (т. е. группы относительно сложения) пространства  $S$  по аддитивной группе подпространства  $P$ .

**Предложение 9.** Классы по  $P$ , содержащие базис  $S$  относительно  $P$ , образуют базис  $S/P$ . Обратно, элементы, взятые по одному из классов базиса  $S/P$ , составляют базис  $S$  относительно  $P$ .

Действительно, включение  $c_1u_1 + \dots + c_ku_k \in P$  равносильно сравнению  $c_1u_1 + \dots + c_ku_k \equiv 0 (P)$  и равенству  $c_1\bar{u} + \dots + c_k\bar{u}_k = 0$  (черточка обозначает переход к классам сравнений по  $P$ ), так что линейная независимость  $u_1, \dots, u_k$  относительно  $P$  равносильна линейной независимости элементов  $\bar{u}_1, \dots, \bar{u}_k$  факторпространства. Равенство  $x = c_1u_1 + \dots + c_ku_k + y$  при  $y \in P$  равносильно сравнению  $x \equiv c_1u_1 + \dots + c_ku_k (P)$  и равенству  $\bar{x} = c_1\bar{u}_1 + \dots + c_k\bar{u}_k$  в факторпространстве.

Отсюда следует, в частности, что размерность факторпространства  $S/P$  равна разности размерностей  $S$  и  $P$ .

### § 3. Линейные функции

**1. Сопряженное пространство.** *Линейными функциями* на векторном пространстве  $S$  называются функции, определенные на векторах этого пространства со значениями в основном поле  $K$ , удовлетворяющие условию линейности:  $l(c_1x + c_2y) = c_1l(x) + c_2l(y)$ . Пусть в  $S$  выбран базис  $e_1, e_2, \dots, e_n$ . В силу линейности значение функции  $l$  на любом векторе определяется значениями на базисе; действительно, если  $(x_1, \dots, x_n)^T$  — столбец из координат вектора  $x$ , так что  $x = x_1e_1 + \dots + x_ne_n$ , то  $l(x) = x_1l(e_1) + \dots + x_nl(e_n)$ . Ясно, что любая функция, выражаемая через координаты по формуле  $l(x) = a_1x_1 + \dots + a_nx_n$ , будет линейной функцией. Таким образом, между линейными функциями на  $S$  и строками  $(a_1, \dots, a_n)$  в формуле  $l(x) = a_1x_1 + \dots + a_nx_n$  имеется взаимно однозначное соответствие. Значение функции  $l(x)$  на векторе  $x$  равно произведению строки из коэффициентов линейной функции на столбец из координат вектора  $x$ .

Для линейных функций естественным образом определяются действия сложения и умножения на элементы основного поля, именно, по определению,  $(l_1 + l_2)x = l_1(x) + l_2(x)$  и  $(cl)x = cl(x)$ . По отношению к этим действиям линейные функции образуют векторное пространство, называемое *сopряженным* с пространством  $S$  и обозначаемое  $S^*$ . Оно, очевидно, изоморфно пространству строк коэффициентов линейных функций и, следовательно,  $n$ -мерно, так же как  $S$ . Однако естественного изоморфизма между  $S$  и  $S^*$ , который бы не зависел от выбора базиса, не существует.

Элементы  $x \in S$  естественно порождают линейные функции на пространстве  $S^*$ , если считать  $x(l) = l(x)$ . Поэтому  $S$  изоморфно погружается в  $(S^*)^*$ . Образ при этом погружении совпадает с пространством  $(S^*)^*$ , ибо размерности пространств  $S$  и  $(S^*)^*$  равны. Это позволяет рассматривать пространство  $S$  как сопряженное с пространством  $S^*$ .

Линейные функции на пространстве  $S$  называют также *ковекторами*. В этой терминологии значение линейной функции на векторе называется *скалярным произведением* ковектора на вектор или вектора на ковектор.





где через  $X$  и  $Y$  обозначены столбцы из координат векторов  $x$  и  $y$ . Матрица  $A$  называется *матрицей отображения*  $\mathcal{A}$ .

*Ядром*  $\ker \mathcal{A}$  отображения  $\mathcal{A}$  называется множество всех векторов из  $S$ , отображаемых в  $0$  пространства  $T$ .

*Образом*  $\text{im } \mathcal{A}$  или  $\mathcal{A}S$  отображения  $\mathcal{A}$  называется множество векторов  $\mathcal{A}x$  при  $x \in S$ . Ясно, что ядро и образ  $\mathcal{A}$  являются подпространствами, соответственно, пространств  $S$  и  $T$ .

Векторы из  $S$ , сравнимые по  $\ker \mathcal{A}$ , т. е. отличающиеся слагаемым из  $\ker \mathcal{A}$ , имеют, очевидно, одинаковые образы в  $T$ . Обратно, если  $\mathcal{A}x = \mathcal{A}z$ , то  $\mathcal{A}(x - z) = 0$ , т. е.  $x$  и  $z$  сравнимы по  $\ker \mathcal{A}$ . Следовательно, между векторами образа  $\mathcal{A}S$  оператора  $\mathcal{A}$  и элементами факторпространства  $S/\ker \mathcal{A}$  имеется взаимно однозначное соответствие. Это соответствие, очевидно, сохраняет линейные комбинации, так что пространство  $\mathcal{A}S$  изоморфно факторпространству  $S/\ker \mathcal{A}$ . Следовательно,

$$\dim \mathcal{A}S = \dim S - \dim \ker \mathcal{A}.$$

**2. Изменение матрицы оператора при преобразовании координат в пространствах  $S$  и  $T$ .** Пусть в пространствах  $S$  и  $T$  базисы  $e_1, \dots, e_n$  и  $f_1, \dots, f_m$  заменены на базисы  $e'_1, \dots, e'_n$  и  $f'_1, \dots, f'_m$ . Соответствующие этим заменам матрицы преобразования координат обозначим через  $C$  и  $B$ , столбцы из координат векторов  $x$  и  $y = \mathcal{A}x$  в исходных базисах обозначим через  $X$  и  $Y$ , в преобразованных — соответственно,  $X'$  и  $Y'$ . Матрицу оператора  $\mathcal{A}$  обозначим  $A$ . Тогда  $Y = AX$ ,  $X = CX'$ ,  $Y = BY'$ , так что  $Y' = B^{-1}Y$ . Следовательно,  $Y' = B^{-1}Y = B^{-1}AX = B^{-1}ACX'$ . Поэтому матрицей оператора  $\mathcal{A}$  по отношению к новым базисам является матрица  $A' = B^{-1}AC$ .

**3. Каноническая форма матрицы линейного отображения.** Прежде всего заметим, что размерность образа  $\mathcal{A}S$  равна максимальному числу линейно независимых векторов в порождающей это пространство совокупности векторов  $\mathcal{A}e_1, \dots, \mathcal{A}e_n$ , т. е. равна максимальному числу линейно независимых столбцов матрицы  $A$  оператора  $\mathcal{A}$ . Таким образом,  $\dim \mathcal{A}S = r$ , где  $r$  — ранг матрицы  $A$ .

В силу соотношения между размерностями ядра и образа, отсюда следует, что  $\dim \ker \mathcal{A} = n - r$ .

Пусть  $e_1, \dots, e_r$  — какой-либо базис  $S$  относительно  $\ker \mathcal{A}$ . Тогда векторы  $\mathcal{A}e_1, \dots, \mathcal{A}e_r$  образуют базис  $\mathcal{A}S$ . Действительно, эта совокупность векторов порождает  $\mathcal{A}S$ , ибо любой вектор из  $S$  есть линейная комбинация  $e_1, \dots, e_r$  с точностью до слагаемого из  $\ker \mathcal{A}$ , и поэтому любой вектор из  $\mathcal{A}S$  есть линейная комбинация  $\mathcal{A}e_1, \dots, \mathcal{A}e_r$ . Вместе с тем векторы  $\mathcal{A}e_1, \dots, \mathcal{A}e_r$  линейно независимы, ибо из  $c_1\mathcal{A}e_1 + \dots + c_r\mathcal{A}e_r = 0$  следует  $\mathcal{A}(c_1e_1 + \dots + c_re_r) = 0$ , откуда  $c_1e_1 + \dots + c_re_r \in \ker \mathcal{A}$  и  $c_1 = \dots = c_r = 0$  в силу определения относительного базиса. Пусть  $e_{r+1}, \dots$

$\dots, e_n$  — какой-либо базис  $\ker \mathcal{A}$ . Тогда  $e_1, \dots, e_r, e_{r+1}, \dots, e_n$  можно принять за базис пространства  $S$ . В пространстве  $T$  линейно независимую совокупность  $\mathcal{A}e_1, \dots, \mathcal{A}e_r$  дополним каким-либо образом до базиса  $T$ . Обозначим  $g_1 = \mathcal{A}e_1, \dots, g_r = \mathcal{A}e_r$  и через  $g_{r+1}, \dots, g_m$  — какие-либо векторы, дополняющие  $g_1, \dots, g_r$  до базиса  $T$ .

В выбранных базисах матрица оператора  $A$  есть:

$$\begin{pmatrix} E_r & 0_{r, n-r} \\ 0_{m-r, r} & 0_{m-r, n-r} \end{pmatrix}.$$

Здесь  $E_r$  — единичная  $r \times r$ -матрица,  $0_{r, n-r}$ ,  $0_{m-r, r}$  и  $0_{m-r, n-r}$  — нулевые матрицы указанных размеров.

Полученному результату можно придать следующую форму на языке теории матриц. Ввиду того, что любую  $m \times n$ -матрицу  $A$  можно принять за матрицу линейного оператора из  $n$ -мерного пространства  $S$  в  $m$ -мерное пространство  $T$ , для любой  $m \times n$ -матрицы можно найти такие невырожденные  $m \times m$ -матрицу  $B$  и  $n \times n$ -матрицу  $C$ , что

$$B^{-1}AC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

где  $r$  — ранг матрицы  $A$ . Это равенство можно переписать и так:

$$A = B \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} C_0, \quad \text{где } C_0 = C^{-1}.$$

Пусть  $B = (B_1, B_2)$ , где  $B_1$  — матрица, состоящая из первых  $r$  столбцов матрицы  $B$ , матрица  $B_2$  составлена из остальных  $m-r$  столбцов  $B$ . Соответственно, пусть  $C_0 = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$ , где  $C_1$  составлена из первых  $r$  строк матрицы  $C_0$ , а  $C_2$  составлена из остальных  $n-r$  строк. По правилу умножения матриц, разбитых на клетки, получим

$$A = (B_1, B_2) \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = (B_1, 0) \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = B_1 C_1.$$

Итак, мы получили, что любая  $m \times n$ -матрица ранга  $r$  может быть представлена в виде произведения  $m \times r$ -матрицы  $B_1$  на  $r \times n$ -матрицу  $C_1$ . Обе эти матрицы имеют ранг  $r$ , ибо у матрицы  $B_1$  столбцы линейно независимы, а у матрицы  $C_1$  — строки.

**4. Линейные действия над операторами.** Пусть  $\mathcal{A}$  и  $\mathcal{B}$  — линейные операторы, действующие из  $n$ -мерного пространства  $S$  в  $m$ -мерное пространство  $T$ . Определим линейную комбинацию операторов формулой

$$(c_1 \mathcal{A} + c_2 \mathcal{B})x = c_1 \mathcal{A}x + c_2 \mathcal{B}x.$$

Ясно, что по отношению к этому действию операторы образуют векторное пространство. Выбор базисов в  $S$  и  $T$  задает изоморфизм пространства операторов и пространства  $m \times n$ -матриц. Поэтому размерность пространства операторов равна  $mn$ .

**5. Умножение линейных отображений.** Пусть даны три пространства  $S_1, S_2, S_3$  и даны линейные отображения:  $\mathcal{B}$ , отображающее  $S_1$  в  $S_2$ , и  $\mathcal{A}$ , отображающее  $S_2$  в  $S_3$ . «Сквозное» отображение  $S_1$  в  $S_3$ , т. е. отображение, действующее на векторы из  $S_1$  по формуле  $\mathcal{A}(\mathcal{B}x)$ , называется произведением  $\mathcal{A}\mathcal{B}$  отображений  $\mathcal{A}$  и  $\mathcal{B}$ . Обращаю внимание на то, что первым действующим на  $x$  оказывается правый множитель, и затем на результат действует левый множитель. Такой порядок обусловлен левой записью: оператор расположен слева от объекта, к которому он применяется.

Пусть в  $S_1, S_2, S_3$  выбраны базисы. Пусть по отношению к этим базисам операторы  $\mathcal{A}$  и  $\mathcal{B}$  имеют матрицы  $A$  и  $B$ , и пусть  $X$  — столбец из координат вектора  $x \in S_1$ . Тогда столбцом из координат вектора  $\mathcal{B}x$  будет  $BX$  и столбцом из координат вектора  $\mathcal{A}\mathcal{B}x$  будет  $ABX$ . Таким образом, произведению операторов соответствует, по отношению к выбранным базисам, произведение матриц.

Ясно, что для умножения операторов и взятия их линейных комбинаций верны соотношения билинейности:

$$(c_1\mathcal{A}_1 + c_2\mathcal{A}_2)\mathcal{B} = c_1\mathcal{A}_1\mathcal{B} + c_2\mathcal{A}_2\mathcal{B},$$

$$\mathcal{A}(c_1\mathcal{B}_1 + c_2\mathcal{B}_2) = c_1\mathcal{A}\mathcal{B}_1 + c_2\mathcal{A}\mathcal{B}_2.$$

**6. Обращение невырожденных линейных отображений.** Линейное отображение пространства  $S$  в пространство  $T$  называется *невырожденным*, если образом  $\mathcal{A}$  является все пространство  $T$  и ядро  $\mathcal{A}$  состоит только из нуля, так что из равенства  $\mathcal{A}x = 0$  следует  $x = 0$ . Невырожденное отображение взаимно однозначно, так что существует обратное отображение  $\mathcal{A}^{-1}$ . Из линейности  $\mathcal{A}$  следует линейность  $\mathcal{A}^{-1}$ . Действительно,  $\mathcal{A}^{-1}(c_1x + c_2y)$  есть такой вектор  $z \in S$ , что  $\mathcal{A}z = c_1x + c_2y$ . Пусть  $u = \mathcal{A}^{-1}x$  и  $v = \mathcal{A}^{-1}y$ , т. е.  $\mathcal{A}u = x$ ,  $\mathcal{A}v = y$ . Тогда  $\mathcal{A}z = c_1\mathcal{A}u + c_2\mathcal{A}v = \mathcal{A}(c_1u + c_2v)$  и, следовательно,  $z - c_1u - c_2v = 0$ , ибо ядро  $\mathcal{A}$  состоит только из нуля. Итак,  $\mathcal{A}^{-1}(c_1x + c_2y) = c_1u + c_2v = c_1\mathcal{A}^{-1}x + c_2\mathcal{A}^{-1}y$ . Линейность  $\mathcal{A}^{-1}$  доказана.

Из определения  $\mathcal{A}^{-1}$  ясно, что  $\mathcal{A}^{-1}\mathcal{A}$  является единичным оператором на  $S$  и  $\mathcal{A}\mathcal{A}^{-1}$  есть единичный оператор на  $T$ .

## § 5. Линейные операторы в векторном пространстве

**1. Матрица линейного оператора.** В настоящем и следующих параграфах будут рассматриваться линейные операторы, действующие из векторного пространства  $S$  в себя. Пусть  $e_1, \dots, e_n$  — базис  $S$ . Тогда оператору  $\mathcal{A}$  соответствует матрица, составленная из столбцов координат векторов  $\mathcal{A}e_1, \mathcal{A}e_2, \dots, \mathcal{A}e_n$  относительно базиса  $e_1, e_2, \dots, e_n$ , так что эта матрица квадратная. В отличие от ситуации, когда мы рассматривали линейные операторы действующие из пространства  $S$  в пространство  $T$ , и мы имели возможность выбирать базисы в каждом из этих пространств, здесь сво-

бода в выборе базиса меньше, мы можем выбирать базис лишь в самом пространстве  $S$ . Матрицы преобразования координат  $B$  и  $C$ , независимо выбиравшиеся в ситуации § 4, здесь совпадают, так что формула для изменения матрицы при преобразовании координат принимает вид  $A' = C^{-1}AC$ . Здесь  $A$  — матрица оператора  $\mathcal{A}$ , отнесенная к исходному базису,  $C$  — матрица преобразования координат и  $A'$  — матрица оператора  $\mathcal{A}$  в преобразованном базисе.

Таким образом, при преобразовании координат матрица линейного оператора претерпевает преобразование подобия.

Выше мы видели, что характеристический полином  $\det(tE - A)$  матрицы  $A$  не изменяется при преобразовании подобия. Следовательно, характеристический полином матрицы оператора зависит лишь от самого оператора и не зависит от выбора базиса пространства. Поэтому будем его называть характеристическим полиномом оператора.

**2. Действия над операторами.** Векторное пространство над полем  $K$ , для элементов которого определено действие умножения, сопоставляющее упорядоченной паре векторов третий вектор, называемый их произведением, называется *алгеброй* над  $K$ , если выполнены соотношения билинейности произведения:

$$\begin{aligned}(c_1x_1 + c_2x_2)y &= c_1x_1y + c_2x_2y, \\ x(c_1y_1 + c_2y_2) &= c_1xy_1 + c_2xy_2.\end{aligned}$$

Таким образом, в алгебре соединяются структуры векторного пространства и кольца, согласованные свойствами билинейности. Алгебра называется *ассоциативной*, если действие умножения ассоциативно. Примером ассоциативной алгебры служит алгебра квадратных матриц с элементами из поля  $K$ .

Операторы, действующие из  $S$  в  $S$ , образуют, очевидно, алгебру, ибо они образуют векторное пространство и для них определено действие умножения, удовлетворяющее соотношениям билинейности. Алгебра операторов ассоциативна. Роль единицы в ней играет единичный оператор  $\mathcal{E}$ , сопоставляющий каждому вектору самого себя.

Оператор называется *невыврожденным*, если его ядро состоит только из нуля или, что то же самое (в силу зависимости между размерностями ядра и образа), если  $S$  отображается на все  $S$ . Для невырожденного оператора существует обратный.

Алгебра операторов из  $S$  в  $S$  изоморфна алгебре квадратных  $n \times n$ -матриц, где  $n = \dim S$ . Изоморфизм задается сопоставлением каждому оператору  $\mathcal{A}$  его матрицы относительно некоторого фиксированного базиса. Единичному оператору при этом соответствует единичная матрица, невырожденным операторам — невырожденные матрицы и взаимно обратным операторам — взаимно обратные матрицы.

Для дальнейшего нам будут нужны значения полиномов от оператора. Именно, если  $f(t) = a_0t^n + \dots + a_{n-1}t + a_n \in K[t]$ , то



Доказательство.

$$\det(tE_n - A) = \det \begin{pmatrix} tE_k - A_1 & B \\ 0 & tE_{n-k} - A_2 \end{pmatrix}.$$

По теореме об определителе ступенчатой матрицы

$$\det(tE_n - A) = \det(tE_k - A_1) \det(tE_{n-k} - A_2),$$

что и доказывает предложение.

Матрица оператора еще больше упрощается, если  $S$  разлагается в прямую сумму двух или нескольких инвариантных подпространств. В этой ситуации за базис  $S$  можно взять объединение базисов прямых слагаемых, и оператор  $\mathcal{A}$  будет преобразовывать базис каждого из подпространств  $P_i$  посредством матрицы ограничения оператора  $\mathcal{A}$  на  $P_i$ , так что в целом матрица окажется блочно-диагональной:

$$A = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_m \end{bmatrix}.$$

Здесь  $A_1, A_2, \dots, A_m$  — матрицы оператора  $\mathcal{A}$  на инвариантных прямых слагаемых  $P_1, P_2, \dots, P_m$ , а нулями обозначены нулевые матрицы надлежащих размеров.

Из сказанного следует, что для упрощения матрицы оператора нужно стремиться, насколько это возможно, разложить пространство  $S$  в прямую сумму инвариантных подпространств.

**Предложение 2.** *Ядро и образ любого полинома от оператора  $\mathcal{A}$  (в частности, самого оператора) являются инвариантными подпространствами.*

Доказательство. Пусть вектор  $x$  принадлежит ядру оператора  $f(\mathcal{A})$ . Это значит, что  $f(\mathcal{A})x = 0$ . Но тогда  $\mathcal{A}f(\mathcal{A})x = 0$  и, в силу перестановочности значений полиномов,  $f(\mathcal{A})\mathcal{A}x = 0$ , так что  $\mathcal{A}x$  принадлежит ядру оператора  $f(\mathcal{A})$ . Это значит, что ядро  $f(\mathcal{A})$  инвариантно.

Пусть теперь  $x$  принадлежит образу  $f(\mathcal{A})$ , т. е.  $x = f(\mathcal{A})y$ . Тогда  $\mathcal{A}x = \mathcal{A}f(\mathcal{A})y = f(\mathcal{A})(\mathcal{A}y)$ , так что  $\mathcal{A}x$  тоже принадлежит образу  $f(\mathcal{A})$ , что и означает, что образ  $f(\mathcal{A})$  есть инвариантное подпространство.

**4. Циклическое подпространство и минимальный аннулятор вектора.** Пусть в пространстве  $S$  действует оператор  $\mathcal{A}$ . Для некоторого вектора  $x$  из  $S$  построим наименьшее инвариантное подпространство, содержащее вектор  $x$ . С этой целью введем в рассмотрение совокупность  $x, \mathcal{A}x, \dots, \mathcal{A}^{k-1}x$ , продолжая ее до тех пор, пока в первый раз не возникнет линейная зависимость, так что  $x, \mathcal{A}x, \dots, \mathcal{A}^{k-1}x$  — линейно независимая совокупность векторов, а  $x, \mathcal{A}x, \dots, \mathcal{A}^{k-1}x, \mathcal{A}^k x$  — уже линейно зависимая. Тогда

вектор  $\mathcal{A}^k x$  есть линейная комбинация предшествующих:

$$\mathcal{A}^k x = -a_1 \mathcal{A}^{k-1} x - \dots - a_{k-1} \mathcal{A} x - a_k x.$$

(Мы сознательно взяли коэффициенты линейной комбинации со знаком минус.)

Пространство  $P$ , натянутое на векторы  $x, \mathcal{A}x, \dots, \mathcal{A}^{k-1}x$ , инвариантно. Действительно, если  $y \in P$ , то  $y = c_1 x + c_2 \mathcal{A}x + \dots + c_k \mathcal{A}^{k-1}x$  и  $\mathcal{A}y = c_1 \mathcal{A}x + c_2 \mathcal{A}^2 x + \dots + c_{k-1} \mathcal{A}^k x + c_k \mathcal{A}^{k+1} x = -c_k (a_1 \mathcal{A}^{k-1} x + \dots + a_{k-1} \mathcal{A} x + a_k x) + c_1 \mathcal{A}x + c_2 \mathcal{A}^2 x + \dots + c_{k-1} \mathcal{A}^k x \in P$ , ибо все слагаемые принадлежат  $P$ .

Далее, если  $Q$  — какое-либо инвариантное подпространство, содержащее вектор  $x$ , то оно содержит и векторы  $\mathcal{A}x, \mathcal{A}^2 x, \dots, \mathcal{A}^{k-1}x$ , и, следовательно,  $Q \supset P$ . Таким образом,  $P$  есть минимальное инвариантное подпространство, содержащее вектор  $x$ ; оно называется *циклическим подпространством*, порожденным вектором  $x$ .

Равенство

$$\mathcal{A}^k x = -a_1 \mathcal{A}^{k-1} x - \dots - a_{k-1} \mathcal{A} x - a_k x$$

можно записать в виде

$$f(\mathcal{A})x = 0,$$

где  $f(t) = t^k + a_1 t^{k-1} + \dots + a_{k-1} t + a_k$ .

Полиномы  $F(t)$ , обладающие свойством  $F(\mathcal{A})x = 0$ , называются *аннуляторами* вектора  $x$ . Покажем, что  $f(t)$  является аннулятором наименьшей степени среди ненулевых аннуляторов. Действительно, если  $b_0 t^{k-1} + b_1 t^{k-2} + \dots + b_{k-2} t + b_{k-1}$  есть аннулятор для вектора  $x$ , то  $b_0 \mathcal{A}^{k-1} x + b_1 \mathcal{A}^{k-2} x + \dots + b_{k-2} \mathcal{A} x + b_{k-1} x = 0$ , что возможно только при  $b_0 = b_1 = \dots = b_{k-2} = b_{k-1} = 0$ , в силу линейной независимости  $x, \mathcal{A}x, \dots, \mathcal{A}^{k-1}x$ . Поэтому полином  $f(t)$  называется *минимальным аннулятором* вектора  $x$ .

Предложение 3. *Любой аннулятор вектора  $x$  делится на минимальный аннулятор.*

Действительно, пусть  $F(t)$  — некоторый аннулятор вектора  $x$  и  $f(t)$  — минимальный аннулятор  $x$ . Поделим  $F(t)$  на  $f(t)$  с остатком:  $F(t) = q(t)f(t) + r(t)$ , причем степень  $r(t)$  меньше степени  $f(t)$ . Тогда

$$F(\mathcal{A}) = q(\mathcal{A})f(\mathcal{A}) + r(\mathcal{A}) \quad \text{и} \quad F(\mathcal{A})x = q(\mathcal{A})f(\mathcal{A})x + r(\mathcal{A})x,$$

откуда  $r(\mathcal{A})x = 0$ , ибо  $F(\mathcal{A})x = 0$  и  $f(\mathcal{A})x = 0$ . Следовательно,  $r(t) = 0$ , ибо  $f(t)$  — аннулятор наименьшей степени.

**5. Матрица оператора на циклическом подпространстве и ее характеристический полином.** Пусть в векторном пространстве  $S$  действует оператор  $\mathcal{A}$ . Обозначим через  $P$  циклическое подпространство, порожденное вектором  $x \in S$ , и пусть  $f(t) = t^k + a_1 t^{k-1} + \dots + a_{k+1} t + a_k$  — минимальный аннулятор вектора  $x$ . За базис  $P$  можно принять векторы  $x, \mathcal{A}x, \mathcal{A}^2 x, \dots, \mathcal{A}^{k-1}x$ . Под действием оператора  $\mathcal{A}$  они превращаются, соответственно, в

$\mathcal{A}x, \mathcal{A}^2x, \dots, \mathcal{A}^{k-1}x, \mathcal{A}^kx$ , причем  $\mathcal{A}^kx = -a_kx - a_{k-1}\mathcal{A}x - \dots - a_1\mathcal{A}^{k-1}x$ . Следовательно, матрица оператора  $\mathcal{A}$  в этом базисе равна

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_k \\ 1 & 0 & \dots & 0 & -a_{k-1} \\ 0 & 1 & \dots & 0 & -a_{k-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

Матрица этого вида носит название *сопровождающей* для полинома  $f(t)$ .

**Предложение 4.** *Характеристический полином оператора  $\mathcal{A}$  на циклическом подпространстве, порожденном вектором  $x$ , равен минимальному аннулятору вектора  $x$ .*

Иными словами, нужно доказать, что характеристический полином матрицы, сопровождающей для полинома  $f(t)$ , равен этому полиному. Это — нетрудная задача на вычисление определителей.

Характеристический полином матрицы, сопровождающей для полинома  $f(t)$ , равен

$$\Delta = \begin{vmatrix} t & 0 & \dots & 0 & a_k \\ -1 & t & \dots & 0 & a_{k-1} \\ 0 & -1 & \dots & 0 & a_{k-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & t + a_1 \end{vmatrix}.$$

Для вычисления этого определителя прибавим к его первой строке вторую, умноженную на  $t$ , третью, умноженную на  $t^2$ , ..., последнюю, умноженную на  $t^{k-1}$ . Получим:

$$\begin{aligned} \Delta &= \begin{vmatrix} 0 & 0 & \dots & 0 & f(t) \\ -1 & t & \dots & 0 & a_{k-1} \\ 0 & -1 & \dots & 0 & a_{k-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & t + a_1 \end{vmatrix} = (-1)^{k+1} f(t) \begin{vmatrix} -1 & t & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 \end{vmatrix} \\ &= (-1)^{k+1} (-1)^{k-1} f(t) = f(t). \end{aligned}$$

Предложение доказано.

Сопоставим это предложение с предложением 1, получим, что характеристический полином оператора  $\mathcal{A}$  (на всем пространстве) делится на минимальный аннулятор любого вектора и, следовательно, характеристический полином от оператора аннулирует все векторы пространства, т. е. является нулевым оператором. Тем самым мы снова доказали в терминах операторов теорему Гамильтона — Кэли, доказанную ранее в терминах матриц.

**6. Минимальный полином оператора.** *Минимальным полиномом* оператора  $\mathcal{A}$ , действующего в пространстве  $S$ , называется полиномом наименьшей степени, аннулирующий все векторы простран-

ства  $S$ , т. е. такой полином  $g(t)$  наименьшей степени, что  $g(\mathcal{A}) = 0$ . Обычным приемом деления с остатком легко убедиться в том, что если  $F(\mathcal{A}) = 0$ , то  $F(t)$  делится на минимальный полином. Поэтому минимальный полином является делителем характеристического.

Минимальный полином есть наименьшее общее кратное минимальных аннуляторов векторов базиса. Действительно, минимальный полином является кратным для всех таких аннуляторов и любое кратное аннуляторов векторов базиса аннулирует базисные векторы, а с ними и все векторы пространства.

Более общо, если пространство  $S$  есть сумма (не обязательно прямая сумма) инвариантных подпространств  $P_1, \dots, P_k$ , то минимальный полином оператора  $\mathcal{A}$  на  $S$  равен наименьшему общему кратному минимальных полиномов оператора  $\mathcal{A}$  на подпространствах  $P_1, \dots, P_k$ . Действительно, минимальный полином  $\mathcal{A}$  на  $S$  делится на минимальный полином  $\mathcal{A}$  на  $P_i$ , т. е. является кратным для всех минимальных полиномов подпространств  $P_1, \dots, P_k$ . Вместе с тем любое кратное этих полиномов, в частности, наименьшее общее кратное аннулирует все подпространства  $P_1, \dots, P_k$  и их сумму  $S$ .

**7. Разложение пространства с оператором в прямую сумму примарных подпространств.** Пространство, в котором действует оператор, называется *примарным*, если минимальный полином оператора является степенью неприводимого полинома над основным полем. Цель настоящего пункта — доказать, что пространство можно разложить в прямую сумму инвариантных примарных подпространств. С этой целью докажем несколько вспомогательных предложений. В их формулировках будет всюду предполагаться, что векторы принадлежат пространству, в котором действует оператор  $\mathcal{A}$ .

**Предложение 5.** *Если вектор аннулируется двумя взаимно простыми полиномами, то он равен нулю.*

Действительно, минимальный аннулятор такого вектора делит пару взаимно простых полиномов и, следовательно, равен 1, так что 1 аннулирует вектор, и сам вектор равен нулю.

**Предложение 6.** *Если вектор  $z$  аннулируется полиномом  $g(t) = g_1(t)g_2(t)$ , разлагающимся в произведение двух взаимно простых полиномов  $g_1(t)$  и  $g_2(t)$ , то вектор можно представить в виде суммы двух векторов, один из которых аннулируется полиномом  $g_1(t)$ , другой — полиномом  $g_2(t)$ .*

**Доказательство.** В силу взаимной простоты  $g_1$  и  $g_2$  найдутся такие полиномы  $u$  и  $v$ , что  $ug_2 + vg_1 = 1$ . Тогда  $u(\mathcal{A})g_2(\mathcal{A}) + v(\mathcal{A})g_1(\mathcal{A}) = \mathcal{E}$ , и  $z = \mathcal{E}z = u(\mathcal{A})g_2(\mathcal{A})z + v(\mathcal{A})g_1(\mathcal{A})z = z_1 + z_2$ . Вектор  $z_1 = u(\mathcal{A})g_2(\mathcal{A})z$  аннулируется полиномом  $g_1(t)$ , ибо  $g_1(\mathcal{A})z_1 = g_1(\mathcal{A})u(\mathcal{A})g_2(\mathcal{A})z = u(\mathcal{A})g_1(\mathcal{A})g_2(\mathcal{A})z = 0$ . Аналогично, вектор  $z_2 = v(\mathcal{A})g_1(\mathcal{A})z$  аннулируется полиномом  $g_2(t)$ .

**Предложение 7.** Если вектор  $z$  аннулируется полиномом  $g(t) = g_1(t) \dots g_k(t)$  при попарно взаимно простых сомножителях  $g_1, \dots, g_k$ , то  $z$  представляется в виде суммы  $k$  векторов, аннулирующих, соответственно, полиномами  $g_1, \dots, g_k$ .

Доказывается тривиальным применением метода математической индукции, на основании предложения 6.

**Предложение 8.** Пусть минимальный полином оператора  $\mathcal{A}$  (на всем пространстве) разлагается в произведение  $g(t) = g_1(t) \dots g_k(t)$  попарно взаимно простых полиномов. Тогда пространство однозначно разлагается в прямую сумму инвариантных подпространств  $P_1, \dots, P_k$ , на которых оператор  $\mathcal{A}$  имеет минимальные полиномы  $g_1, \dots, g_k$ .

**Доказательство.** Обозначим через  $P_i$  множество всех векторов, аннулируемых полиномом  $g_i$ , иными словами,  $P_i = \ker g_i(\mathcal{A})$ . Тогда  $P_1 + \dots + P_k = S$ , ибо любой вектор из  $S$  аннулируется полиномом  $g(t)$  и, в силу предложения 7, представляется в виде суммы векторов из  $P_1, \dots, P_k$ . Сумма  $P_1 + \dots + P_k$  прямая, ибо если вектор  $z$  принадлежит  $P_i$  и сумме  $P_1 + \dots + P_{i-1} + P_{i+1} + \dots + P_k$  остальных слагаемых подпространств, то  $z$  аннулируется парой взаимно простых полиномов  $g_i(t)$  и  $g_1(t) \dots g_{i-1}(t) g_{i+1}(t) \dots g_k(t)$  и, следовательно, равен 0. Минимальный полином оператора  $\mathcal{A}$  на  $P_i$  есть  $g_i(t)$  или его делитель, но собственным делителем не может быть, ибо  $g = g_1 \dots g_k$  есть наименьшее общее кратное минимальных полиномов оператора  $\mathcal{A}$  на  $P_i$ .

Однозначность разложения следует из того, что  $P_i$  есть множество всех векторов, аннулируемых полиномом  $g_i$ .

Предложение доказано полностью.

Из предложения 8 сразу вытекает справедливость следующей теоремы:

**Теорема 9.** Пространство, в котором действует оператор, разлагается в прямую сумму примарных подпространств.

Достаточно применить предложение 8 к каноническому разложению  $g = \varphi_1^{m_1} \dots \varphi_k^{m_k}$  минимального полинома  $g$  на неприводимые множители.

Подпространство, состоящее из всех векторов, аннулируемых полиномом  $\varphi_i^{m_i}$ , назовем *полным* примарным подпространством, соответствующим примарному делителю  $\varphi_i^{m_i}$  полинома  $g$ .

**8. Разложение примарного пространства в прямую сумму циклических примарных подпространств.**

**Теорема 10.** Примарное пространство может быть представлено в виде прямой суммы циклических примарных подпространств.

**Доказательство.** Применим метод математической индукции по размерности пространства. За базу для индукции можно принять примарные циклические пространства. Сделаем индуктивное предположение о том, что для примарных пространств, раз-

мерность которых меньше размерности рассматриваемого пространства  $S$ , теорема верна.

Пусть минимальный полином равен  $\varphi^m$ . Тогда все элементы пространства аннулируются делителями этого полинома, т. е. степенями  $\varphi$  с показателями, не превосходящими  $m$ . При этом найдется элемент, аннулируемый полиномом  $\varphi^m$  и не аннулируемый полиномом  $\varphi^{m-1}$ , иначе все векторы аннулировались бы полиномом  $\varphi^{m-1}$ , что противоречит минимальности полинома  $\varphi^m$ . Пусть  $u_1$  — такой вектор и  $P_1$  — циклическое подпространство, порожденное вектором  $u_1$ . Если  $P_1 = S$ , то теорема для пространства  $S$  доказана. Пусть  $P_1 \neq S$ . Рассмотрим факторпространство  $S/P_1$ . Его векторы, очевидно, аннулируются полиномом  $\varphi^m$ , так что  $S/P_1$  примарно и имеет размерность, меньшую чем  $S$ . Поэтому к  $S/P_1$  можно применить индуктивное предположение. Пусть

$$S/P_1 = \bar{P}_2 \oplus \dots \oplus \bar{P}_k$$

(черточки сверху букв обозначают, как обычно, что рассматриваются объекты, составляющие факторпространство),  $\bar{u}_2, \dots, \bar{u}_k$  — векторы из  $S/P_1$ , порождающие  $\bar{P}_2, \dots, \bar{P}_k$ , и  $\varphi^{m_2}, \dots, \varphi^{m_k}$  — аннуляторы векторов  $\bar{u}_2, \dots, \bar{u}_k$ . Ясно, что  $m_i \leq m$  при всех  $i$ . Покажем, что в классах  $\bar{u}_2, \dots, \bar{u}_k$  можно найти элементы  $u_2, \dots, u_k$ , минимальными аннуляторами которых будут те же  $\varphi^{m_2}, \dots, \varphi^{m_k}$ .

Действительно, пусть  $u'_2$  — какой-либо вектор из  $\bar{u}_2$ . Тогда  $\varphi^{m_2} u'_2 \in P_1$ , так что  $\varphi^{m_2} u'_2 = F(\mathcal{A}) u_1$ , где  $F$  — некоторый полином. Но  $\varphi^m$  аннулирует все векторы в  $S$ , так что  $\varphi^{m_2} u'_2 = \varphi^{m-m_2} \varphi^{m_2} u'_2 = = \varphi^{m-m_2}(\mathcal{A}) F(\mathcal{A}) u_1 = 0$ . Следовательно, полином  $\varphi^{m-m_2} F$  делится на  $\varphi^m$ , и поэтому  $F$  делится на  $\varphi^{m_2}$ . Пусть  $F = \varphi^{m_2} F_1$ , так что  $\varphi^{m_2}(\mathcal{A}) u'_2 = \varphi^{m_2}(\mathcal{A}) F_1(\mathcal{A}) u_1$ , откуда  $\varphi^{m_2}(\mathcal{A}) u_2 = 0$  при  $u_2 = u'_2 - F_1(\mathcal{A}) u_1$ . Ясно, что  $u_2 \equiv u'_2$ , так что  $u_2 \in \bar{u}_2$ . Заметим, что полиномы аннулируют векторы  $u_2$  и  $\bar{u}_2$  одновременно, так как их минимальные аннуляторы совпадают. Аналогичным образом выбираются  $u_3, \dots, u_k$ . Пусть  $P_2, \dots, P_k$  — циклические подпространства, порожденные векторами  $u_2, \dots, u_k$ . Так как  $F(\mathcal{A}) u_2 \in \in F(\mathcal{A}) \bar{u}_2$  и если  $F_1(\mathcal{A}) u_2 = F_2(\mathcal{A}) u_2$ , то  $F_1(\mathcal{A}) \bar{u}_2 = F_2(\mathcal{A}) \bar{u}_2$  и обратно (здесь  $F, F_1, F_2$  — любые полиномы), векторы пространства  $P_2$  входят по одному во все классы, составляющие  $\bar{P}_2$ , и нулевой класс представляет нулевой вектор. Аналогичным образом обстоит дело с пространствами  $P_3, \dots, P_k$ .

Сумма пространств  $P_1 + P_2 + \dots + P_k$  равна пространству  $S$ , ибо любой вектор из  $S$  сравним по  $P_1$  с вектором из  $P_2 + \dots + P_k$ . Сумма эта прямая, ибо если  $z_1 + z_2 + \dots + z_k = 0$  при  $z_i \in P_i$ , то  $\bar{z}_2 + \dots + \bar{z}_k = 0$ , откуда  $\bar{z}_2, \dots, \bar{z}_k$  равны нулю, ибо  $S/P_1$  есть прямая сумма  $\bar{P}_2, \dots, \bar{P}_k$ . Но тогда  $z_2 = \dots = z_k = 0$  и, наконец,  $z_1 = 0$ . Теорема доказана.

9. Модули над кольцом главных идеалов. Читатель, вероятно, обратил внимание на сходство формулировок теорем 9 и 10 и их

доказательств с теоремами теории конечных абелевых групп — теоремой о разложении конечной абелевой группы в прямую сумму примарных и теоремой о разложении примарной абелевой группы в прямую сумму примарных циклических подгрупп. Обе эти теории можно рассматривать как частные случаи более общей теории конечно порожденных  $\Lambda$ -периодических модулей над кольцом главных идеалов  $\Lambda$ .

Дадим некоторые относящиеся сюда определения. Пусть  $\Lambda$  — ассоциативное коммутативное кольцо с единицей. Модулем  $M$  над кольцом  $\Lambda$  называется абелева группа, для элементов которой определено умножение на элементы  $\Lambda$ , удовлетворяющее естественным требованиям:

$$(\alpha_1 + \alpha_2)x = \alpha_1x + \alpha_2x,$$

$$\alpha(x_1 + x_2) = \alpha x_1 + \alpha x_2,$$

$$\alpha_1(\alpha_2x) = (\alpha_1\alpha_2)x,$$

$$1 \cdot x = x.$$

Здесь  $\alpha, \alpha_1, \alpha_2 \in \Lambda$  и  $x_1, x_2, x \in M$ .

Модуль называется конечно порожденным, если существует конечное множество  $x_1, \dots, x_k \in M$  такое, что все элементы из  $M$  представляются в виде  $\alpha_1x_1 + \dots + \alpha_kx_k$  при  $\alpha_1, \dots, \alpha_k \in \Lambda$ . Модуль называется  $\Lambda$ -периодическим, если для каждого  $x \in M$  существует такое  $\alpha \in \Lambda$ , что  $\alpha x = 0$ . Каждый элемент  $\alpha$ , обладающий этим свойством, называется аннулятором элемента  $x$ . Множество аннуляторов образует идеал кольца  $\Lambda$  и, если  $\Lambda$  есть кольцо главных идеалов, идеал аннуляторов оказывается главным и порождающий его элемент играет роль минимального аннулятора — всякий другой аннулятор на него делится. Далее, существует аннулятор всего модуля, например произведение аннуляторов элементов  $x_1, \dots, x_k$ , порождающих  $M$ . Аннуляторы всего  $M$  снова образуют главный идеал, так что найдется минимальный в смысле делимости аннулятор, играющий роль минимального полинома. Модуль называется примарным, если он аннулируется степенью простого элемента кольца  $\Lambda$ . Ввиду того, что в кольце главных идеалов существует линейное представление наибольшего общего делителя, доказываются аналоги предложений 6, 7, 8 и теорема 9.

Модуль называется циклическим, если он порождается одним элементом. Аналог теоремы 10 о разложении примарного модуля в прямую сумму примарных циклических доказывается так же, как сама теорема 10, может только представить некоторое затруднение выбор объектов, по которым проводится индукция.

Конечные абелевы группы представляют собой конечно порожденные периодические модули для кольца  $\mathbb{Z}$  целых чисел. Пространство с оператором  $\mathcal{A}$  можно рассматривать, как конечно порожденный периодический модуль над кольцом полиномов  $K[t]$ ,

с «умножением» вектора на  $F(t)$  по правилу  $(F(t))x = F(\mathcal{A})x$ . Как кольцо  $\mathbb{Z}$ , так и кольцо  $K[t]$  являются кольцами главных идеалов.

#### 10. Некоторые следствия.

**Предложение 11.** *Характеристический полином оператора на примарном пространстве равен степени соответствующего неприводимого полинома с показателем, равным сумме показателей в минимальных полиномах для циклических слагаемых.*

Действительно, характеристический полином на прямой сумме инвариантных подпространств равен произведению характеристических полиномов на этих подпространствах. Примарное пространство разлагается в прямую сумму циклических подпространств, и на каждом циклическом подпространстве характеристический полином равен минимальному. Минимальный полином оператора на каждом примарном циклическом слагаемом есть степень неприводимого полинома, именно того, степенью которого является минимальный полином примарного пространства.

**Предложение 12.** *Пусть  $S$  — пространство с оператором  $\mathcal{A}$  и  $\varphi_1^{m_1}\varphi_2^{m_2}\dots\varphi_k^{m_k}$  — каноническое разложение характеристического полинома  $\mathcal{A}$ . Тогда примарные сомножители  $\varphi_1^{m_1}, \varphi_2^{m_2}, \dots, \varphi_k^{m_k}$  равны характеристическим полиномам оператора  $\mathcal{A}$  на полных примарных прямых слагаемых.*

Действительно, характеристический полином оператора  $S$  на всем пространстве равен произведению характеристических полиномов на полных примарных прямых слагаемых. Эти полиномы равны степеням неприводимых полиномов, различных для различных прямых слагаемых. Следовательно, произведение этих характеристических полиномов есть каноническое разложение характеристического полинома на всем пространстве.

**Предложение 13.** *Инвариантные подпространства примарного циклического пространства  $S$  с характеристическим полиномом  $\varphi^m$  суть  $\varphi S, \varphi^2 S, \dots, \varphi^{m-1} S$ , составляющие убывающую цепочку*

$$S \supset \varphi S \supset \varphi^2 S \supset \dots \supset \varphi^{m-1} S \supset \varphi^m S = 0.$$

**Доказательство.** Пусть  $u$  — вектор, порождающий  $S$ . Тогда все векторы из  $S$  имеют вид  $F(\mathcal{A})u$ , где  $F(t)$  — полиномы из  $K[t]$ . Пусть  $P$  — инвариантное подпространство пространства  $S$  и  $v = F_1(\mathcal{A})u$  — такой вектор из  $P$ , для которого полином  $F_1(t)$  делится на возможно меньшую степень полинома  $\varphi$ . Пусть эта степень равна  $\varphi^{m_1}$ , так что  $F_1(t) = \varphi^{m_1}F_2(t)$ , причем  $F_2(t)$  не делится на  $\varphi$ . Полином  $F_2(t)$  взаимно прост с  $\varphi^m$ , так что существуют такие полиномы  $p(t)$  и  $q(t)$ , что  $F_2 p + \varphi^m q = 1$ . Тогда  $p(\mathcal{A})v = p(\mathcal{A})F_1(\mathcal{A})u = p(\mathcal{A})\varphi^{m_1}(\mathcal{A})F_2(\mathcal{A})u = \varphi^{m_1}(\mathcal{A})(\mathcal{E} - q(\mathcal{A})\varphi^m(\mathcal{A}))u = \varphi^{m_1}(\mathcal{A})u$ , ибо  $\varphi^m(\mathcal{A})u = 0$ .

Следовательно,  $\varphi^{m_1}(\mathcal{A})u$  принадлежит пространству  $P$  и порождает его, ибо полиномы  $F(t)$  для элементов из  $P$  делятся на

$\varphi^{m_1}$ . Таким образом,  $P = \varphi^{m_1}(A)S$  при некотором  $m_1$ . Включения  $S \supset \varphi S \supset \varphi^2 S \supset \dots \supset \varphi^{m-1} S \supset \varphi^m S = 0$  тривиальны в силу инвариантности всех  $\varphi^{m_1}(A)S$ .

**Предложение 14.** *Примарное циклическое пространство неразложимо в сумму правильных инвариантных подпространств.*

Действительно, если  $P_1$  и  $P_2$  — два инвариантных подпространства, то одно из них содержится в другом, пусть  $P_2 \subset P_1$  и  $P_2 + P_1 = P_1 \neq S$ .

Таким образом, разложение пространства в прямую сумму примарных циклических подпространств окончательное, полученные прямые слагаемые уже не разлагаются в прямую сумму инвариантных подпространств.

**11. Каноническая форма матрицы оператора.** Как мы видели выше, для упрощения матрицы оператора целесообразно разложить пространство в прямую сумму инвариантных подпространств и взять в качестве базиса объединение базисов прямых слагаемых. Тогда матрица примет блочно-диагональный вид с блоками, равными матрицам ограничений оператора на прямые слагаемые.

В качестве прямых слагаемых следует взять примарные циклические подпространства. Если в примарном циклическом пространстве с минимальным полиномом  $\varphi^m$ , где  $\varphi$  — неприводимый полином степени  $k$ , взять в качестве базиса  $u, \mathcal{A}u, \mathcal{A}^2u, \dots, \mathcal{A}^{m-k-1}u$ , где  $u$  — порождающий пространство вектор, мы получим в качестве матрицы оператора матрицу, сопровождающую полином  $\varphi^m$ . Если это сделать в каждом примарном циклическом слагаемом, матрица оператора станет блочно-диагональной, состоящей из полиномов, сопровождающих минимальные полиномы примарных циклических слагаемых. Эту форму матрицы оператора назовем грубой канонической формой.

Более полно отражает строение примарного циклического пространства форма матрицы в базисе:

$$e_1 = u, e_2 = \mathcal{A}u, \dots, e_k = \mathcal{A}^{k-1}u,$$

$$e_{k+1} = \varphi(\mathcal{A})u, e_{k+2} = \mathcal{A}\varphi(\mathcal{A})u, \dots, e_{2k} = \mathcal{A}^{k-1}\varphi(\mathcal{A})u,$$

$$e_{2k+1} = \varphi^2(\mathcal{A})u, \dots, e_{mk} = \mathcal{A}^{m-1}\varphi^{k-1}(\mathcal{A})u.$$

Если  $\varphi(t) = t^k + a_1 t^{k-1} + \dots + a_k$ , то

$$\mathcal{A}e_k = e_{k+1} - a_1 e_k - a_2 e_{k-1} - \dots - a_k e_1,$$

$$\mathcal{A}e_{2k} = e_{2k+1} - a_1 e_{2k} - a_2 e_{2k-1} - \dots - a_k e_{k+1},$$

$$\dots \dots \dots$$

$$\mathcal{A}e_{mk} = \dots - a_1 e_{mk} - a_2 e_{mk-1} - \dots - a_k e_{(m-1)k+1}$$

и  $\mathcal{A}e_i = e_{i+1}$  при  $i$ , не делящемся на  $k$ .

В этом базисе матрица оператора  $\mathcal{A}$  состоит из диагональных блоков, каждый из которых равен сопровождающей полином  $\varphi$  матрице, «связанных» единичками, примыкающими снизу и слева

к соседним блокам. (Эти единички возникают из первых слагаемых в выражениях  $\mathcal{A}e_k, \mathcal{A}e_{2k}, \dots, \mathcal{A}e_{(m-1)k}$  через базис.)

Если осуществить такой выбор базиса во всех примарных циклических пространствах, мы получим форму матрицы, которую назовем общей канонической формой. Она лучше грубой формы тем, что в ней участвуют сопровождающие матрицы для самих неприводимых полиномов, а не для их степеней.

Общая каноническая форма принимает особо простой вид в случае, если характеристический полином разлагается на линейные множители, так что минимальные полиномы примарных циклических слагаемых имеют вид  $(t - \lambda)^m$ .

В этом случае сопровождающая матрица для полинома  $t - \lambda$  есть матрица первого порядка  $\lambda$ , и каноническая матрица на примарном циклическом пространстве имеет вид

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{pmatrix}.$$

Такая матрица называется *каноническим блоком Жордана*. Матрица оператора на всем пространстве примет вид блочно-диагональной матрицы, составленной из блоков Жордана. Такая матрица называется *канонической матрицей Жордана*.

Диагональные элементы канонических блоков являются корнями характеристического полинома, и каждый корень может входить в несколько блоков. Ясно, что кратность корня характеристического полинома равна сумме порядков блоков Жордана с этим корнем на диагонали.

В частности, если характеристический полином не имеет кратных корней, то порядки всех блоков Жордана равны 1 и каноническая матрица оператора принимает особо простой вид  $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ , где  $\lambda_1, \lambda_2, \dots, \lambda_n$  — корни характеристического полинома.

Вместо общей канонической формы матрицы оператора на примарном циклическом пространстве иногда оказывается удобной так называемая блочно-жорданова форма. В этой форме по диагонали расположены блоки из сопровождающей матрицы неприводимого полинома, но блоки «связаны» не единичками, как в общей форме, а единичными матрицами, например, матрица имеет вид:

$$\begin{pmatrix} A & & \\ E & A & \\ & E & A \end{pmatrix}.$$

Можно доказать, что если неприводимый полином  $\phi$  *сепарабелен*, т. е. не имеет кратных корней ни в каком расширении основного поля, то матрица оператора на примарном циклическом про-

пространстве с минимальным полиномом  $\varphi^m$  может быть приведена к блочно-жордановой форме. Мы не будем это доказывать в столь общей ситуации. Но сепарабельность  $\varphi$  здесь существенна. Чтобы это продемонстрировать, рассмотрим пример. Пусть  $K_0 = \text{GF}(2)$  и  $K = K_0(y)$ . Полином  $\varphi(t) = t^2 - y \in K[t]$ , очевидно, неприводим в поле  $K$ , так как если бы он был приводим, то раскладывался бы и в кольце полиномов  $K_0[y, t]$ , что не имеет места. Он не сепарабелен, ибо его производная равна нулю. Его сопровождающая матрица есть  $\begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix}$ . В циклическом пространстве с минимальным полиномом  $\varphi^2$  общая каноническая форма есть

$$A = \begin{pmatrix} 0 & y & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

а блочно-жорданова

$$B = \begin{pmatrix} 0 & y & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & y \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Нетрудно проверить, что над полем  $K$  не существует преобразования подобия, переводящего  $A$  в  $B$ . С этой целью следует рассмотреть систему шестнадцати линейных однородных уравнений с шестнадцатью неизвестными, именно, элементами матрицы  $C$ , такой что

$$AC = CB.$$

Из рассмотрения этой системы нетрудно получить (учитывая, что характеристика поля  $K$  равна 2), что первые две строки матрицы  $C$  состоят из нулей, так что невырожденной матрицы, удовлетворяющей уравнению  $AC = CB$ , не существует.

Конечно, неприводимые несепарабельные полиномы могут существовать только над полями с ненулевой характеристикой. Для полей характеристики 0, в частности для числовых полей, неприводимых несепарабельных полиномов не существует.

**12. Оператор проектирования.** Пусть  $S = P \oplus Q$ . Тогда любой вектор  $z \in S$  однозначно представляется в виде  $z = x + y$  при  $x \in P$  и  $y \in Q$ . Вектор  $x$  называется *проекцией* вектора  $z$  на  $P$  параллельно  $Q$ , вектор  $y$ , соответственно, — проекцией вектора  $z$  на  $Q$  параллельно  $P$ . Если  $z = c_1 z_1 + c_2 z_2$ ,  $z = x + y$ ,  $z_1 = x_1 + y_1$ ,  $z_2 = x_2 + y_2$ , то  $z = (c_1 x_1 + c_2 x_2) + (c_1 y_1 + c_2 y_2)$ , так что  $x = c_1 x_1 + c_2 x_2$ . Переход от вектора  $z$  к вектору  $x$  называется *оператором проектирования* или *проектором*. Если  $z = c_1 z_1 + c_2 z_2$ , то  $x = c_1 x_1 + c_2 x_2$ . Поэтому оператор проектирования линеен. Далее, если  $x \in P$ , то его разложение на векторы из  $P$  и  $Q$  есть  $x = x + 0$ . Следовательно, оператор проектирования действует на векторы из  $P$  как единичный оператор, а на векторы из  $Q$  — как нулевой.

Пусть  $\mathcal{A}$  — оператор проектирования  $S$  на  $P$  параллельно  $Q$ . Тогда при любом  $z \in S$  вектор  $\mathcal{A}z$  принадлежит  $P$ , так что  $\mathcal{A}(\mathcal{A}z) = \mathcal{A}z$ . Таким образом, оператор  $\mathcal{A}^2 - \mathcal{A}$  аннулирует все векторы из  $S$ , и тем самым  $\mathcal{A}^2 - \mathcal{A} = 0$ , т. е.  $\mathcal{A}^2 = \mathcal{A}$ .

Оператор  $\mathcal{A}$ , для которого  $\mathcal{A}^2 = \mathcal{A}$ , называется *идемпотентным*. Таким образом, оператор проектирования идемпотентен.

Справедливо и обратное, любой идемпотентный оператор, отличный от 0 и  $\mathcal{E}$ , есть оператор проектирования. Действительно, пусть  $\mathcal{A}^2 = \mathcal{A}$ . Обозначим  $\mathcal{A}S = P$  и  $(\mathcal{E} - \mathcal{A})S = Q$ . Для любого  $z \in S$  верно равенство  $z = \mathcal{A}z + (\mathcal{E} - \mathcal{A})z = x + y$  при  $x \in P$ ,  $y \in Q$ . Следовательно,  $S = P + Q$ . Остается доказать, что эта сумма прямая. Пусть  $v \in P \cap Q$ . Тогда  $v = \mathcal{A}z_1$  и  $v = (\mathcal{E} - \mathcal{A})z_2$  при некоторых  $z_1, z_2 \in S$ . Из первого представления следует, что  $\mathcal{A}v = \mathcal{A}^2z_1 = \mathcal{A}z_1 = v$ , из второго, что  $\mathcal{A}v = (\mathcal{A} - \mathcal{A}^2)z_2 = 0$ . Таким образом,  $v = 0$  и  $S = P \oplus Q$ . Следовательно, из равенства  $z = x + y$  при  $x = \mathcal{A}z \in P$  и  $y = (\mathcal{E} - \mathcal{A})z \in Q$  следует, что  $x = \mathcal{A}z$  есть проекция вектора  $z$  на  $P$  параллельно  $Q$ .

В базисе, составленном из базисов  $P$  и  $Q$ , оператор проектирования имеет диагональную матрицу, ибо все векторы из  $P$  являются собственными векторами для собственного значения 1, а все векторы из  $Q$  — собственными векторами для собственного значения 0. Поэтому матрица имеет вид

$$\begin{pmatrix} E_k & 0 \\ 0 & 0 \end{pmatrix},$$

где  $k = \dim P$ .

**13. Полуобратные линейные отображения.** Пусть  $\mathcal{A}$  — любое отображение пространства  $S$  в пространство  $T$ . Положим  $\ker \mathcal{A} = P$  и обозначим через  $S_0$  какое-либо подпространство, дополняющее  $P$  до  $S$ , т. е. такое, что  $P + S_0 = S$ . Положим  $T_0 = \mathcal{A}S$ , и пусть  $Q$  — какое-либо подпространство, дополняющее  $T_0$  до  $T$ , т. е.  $T_0 + Q = T$ .

Тогда  $\mathcal{A}$  отображает  $S_0$  на  $T_0$ , ибо векторы из  $P$  отображаются на нулевой вектор. Ядро этого отображения состоит только из нулевого вектора, ибо  $S_0$  и  $P$  пересекаются только по 0. Поэтому ограничение  $\mathcal{A}_0$  оператора  $\mathcal{A}$  на  $S_0$  имеет обратный оператор  $\mathcal{A}_0^{-1}$ , определенный на подпространстве  $T_0$  пространства  $T$ .

Пусть  $\mathcal{A}^{(-1)}$  есть продолжение  $\mathcal{A}_0^{-1}$  на все пространство  $T$ , отображающее векторы из  $Q$  в нулевой вектор пространства  $S$ . Ясно, что  $\mathcal{A}^{(-1)}$  есть линейный оператор, действующий из  $T$  в  $S$ . Он называется *полуобратным* для  $\mathcal{A}$ . Разумеется,  $\mathcal{A}^{(-1)}$  зависит от выбора подпространств  $S_0$  и  $Q$ .

Для  $\mathcal{A}^{(-1)}$  подпространство  $Q$  является ядром и  $S_0$  — образом. Подпространство  $T_0$  составляет прямую сумму, равную  $T$ , с ядром  $Q$  оператора  $\mathcal{A}^{(-1)}$ , и подпространство  $P$  дополняет образ  $S_0$  оператора  $\mathcal{A}^{(-1)}$  до пространства  $S$ . Таким образом, поменяв ролями

$S$  и  $T$ ,  $S_0$  и  $T_0$ ,  $P$  и  $Q$ , мы можем построить  $(\mathcal{A}^{(-1)})^{(-1)}$ . Ясно, что  $(\mathcal{A}^{(-1)})^{(-1)} = \mathcal{A}$ .

Оператор  $\mathcal{A}^{(-1)}\mathcal{A}$  отображает  $S$  в  $S$ . Если  $z = x + y \in S$  при  $x \in S_0$ ,  $y \in P$ , то  $\mathcal{A}z = \mathcal{A}x = \mathcal{A}_0x \in T_0$  и  $\mathcal{A}^{(-1)}\mathcal{A}z = \mathcal{A}_0^{-1}\mathcal{A}_0x = x$ . Таким образом,  $\mathcal{A}^{(-1)}\mathcal{A}$  отображает любой вектор  $z$  из  $S$  на его составляющую  $x$  в разложении  $z = x + y$ ,  $x \in S_0$ ,  $y \in P$ . Оператор  $\mathcal{A}^{(-1)}\mathcal{A}$  проектирует векторы из  $S$  на подпространство  $S_0$  параллельно подпространству  $P$ .

Соответственно, оператор  $\mathcal{A}\mathcal{A}^{(-1)}$ , отображающий  $T$  в  $T$ , проектирует векторы из  $T$  на подпространство  $T_0$  параллельно  $Q$ .

Полуобратный оператор  $\mathcal{A}^{(-1)}$  обладает свойством  $\mathcal{A}\mathcal{A}^{(-1)}\mathcal{A} = \mathcal{A}$ . Действительно, если  $z = x + y$ ,  $x \in S_0$ ,  $y \in P$ , то  $\mathcal{A}^{(-1)}\mathcal{A}z = x$  и  $\mathcal{A}\mathcal{A}^{(-1)}\mathcal{A}z = \mathcal{A}x = \mathcal{A}z$ , ибо  $x$  и  $z$  отличаются слагаемым из ядра  $\mathcal{A}$ . Это верно для любого  $z \in S$ , следовательно,  $\mathcal{A}\mathcal{A}^{(-1)}\mathcal{A} = \mathcal{A}$ . Соответственно,  $\mathcal{A}^{(-1)}\mathcal{A}\mathcal{A}^{(-1)} = \mathcal{A}^{(-1)}$ .

**Предложение 15.** Если оператор  $\mathcal{A}$  из  $S$  в  $T$  и оператор  $\mathcal{B}$  из  $T$  в  $S$  связаны соотношениями  $\mathcal{A}\mathcal{B}\mathcal{A} = \mathcal{A}$  и  $\mathcal{B}\mathcal{A}\mathcal{B} = \mathcal{B}$ , то  $\mathcal{B} = \mathcal{A}^{(-1)}$  по отношению к некоторым прямым разложениям пространств  $S$  и  $T$ .

**Доказательство.** Из  $\mathcal{A}\mathcal{B}\mathcal{A} = \mathcal{A}$  следует, что  $\mathcal{B}\mathcal{A}\mathcal{B}\mathcal{A} = \mathcal{B}\mathcal{A}$ , т. е.  $\mathcal{B}\mathcal{A}$  есть идемпотентный оператор из  $S$  в  $S$ . Следовательно, он является оператором проектирования. Обозначим через  $S_0$  подпространство, на которое  $\mathcal{B}\mathcal{A}$  проектирует  $S$ , и через  $P$  — подпространство, параллельно которому происходит проектирование. Проверим, что  $P = \ker \mathcal{A}$ . Действительно, если  $x \in P$ , то  $\mathcal{B}\mathcal{A}x = 0$  и  $\mathcal{A}\mathcal{B}\mathcal{A}x = \mathcal{A}x = 0$ , так что  $P \subseteq \ker \mathcal{A}$ . Обратное включение тривиально. Из того же соотношения  $\mathcal{A}\mathcal{B}\mathcal{A} = \mathcal{A}$  заключаем, что  $\mathcal{A}\mathcal{B}\mathcal{A}\mathcal{B} = \mathcal{A}\mathcal{B}$ , т. е.  $\mathcal{A}\mathcal{B}$  — идемпотентный оператор из  $T$  в  $T$ , т. е. оператор проектирования. Введем обозначения  $T_0$  и  $Q$  для образа и ядра  $\mathcal{A}\mathcal{B}$ . Операторы  $\mathcal{A}$  и  $\mathcal{B}$  осуществляют взаимно обратные отображения подпространств  $S_0$  и  $T_0$ , ибо  $\mathcal{B}\mathcal{A}$  действует на  $S_0$  как единичный оператор,  $\mathcal{A}\mathcal{B}$  действует таким же образом на  $T_0$ . Остается доказать, что  $Q$  аннулируется оператором  $\mathcal{B}$ . Здесь используется соотношение  $\mathcal{B}\mathcal{A}\mathcal{B} = \mathcal{B}$ . Действительно, при  $y \in Q$  будет  $\mathcal{B}y = \mathcal{B}(\mathcal{A}\mathcal{B})y = 0$ , ибо  $\mathcal{A}\mathcal{B}y = 0$ .

Для операторов, действующих из  $S$  в  $S$ , тоже можно определить полуобратные операторы, исходя из двух, вообще говоря, различных разложений  $S$  в прямую сумму подпространств, — одно разложение  $S = P + S_0$ , другое  $S = \mathcal{A}S + Q$ .

Имеется ситуация, когда эти разложения можно взять одинаковыми. Именно, если подпространства  $\mathcal{A}S$  и  $P = \ker \mathcal{A}$  пересекаются только по нулевому вектору. Это значит, что если  $\mathcal{A}z \neq 0$ , то  $\mathcal{A}(\mathcal{A}z) = \mathcal{A}^2z \neq 0$ . Тогда и  $\mathcal{A}^3z$ , и  $\mathcal{A}^4z$ , и т. д. — все отличны от нулевого вектора. Таким образом, поставленному ограничению можно дать такую формулировку: из  $\mathcal{A}^kz = 0$  при  $k \geq 2$  должно следовать, что  $\mathcal{A}z = 0$ . Взяв в этом случае разложение  $S =$



а это и значит, что  $\lambda$  есть корень характеристического полинома  $\det(tE - A)$  оператора  $\mathcal{A}$ .

**Предложение 2.** *Линейная комбинация собственных векторов, принадлежащих одному и тому же собственному значению, есть собственный вектор, принадлежащий тому же собственному значению, или нулевой вектор.*

Действительно, если  $\mathcal{A}x = \lambda x$  и  $\mathcal{A}y = \lambda y$ , то  $\mathcal{A}(c_1x + c_2y) = c_1\mathcal{A}x + c_2\mathcal{A}y = \lambda(c_1x + c_2y)$ , так что если  $c_1x + c_2y \neq 0$ , то  $c_1x + c_2y$  — собственный вектор.

Таким образом, все собственные векторы, принадлежащие собственному значению  $\lambda$ , вместе с нулевым вектором образуют подпространство — подпространство собственных векторов.

**Предложение 3.** *Собственные векторы, принадлежащие попарно различным собственным значениям, линейно независимы.*

Проведем индукцию по числу векторов. Для одного вектора предложение верно, ибо собственный вектор ненулевой. Пусть предложение верно для совокупности собственных векторов, число которых меньше  $k$ , и пусть  $u_1, u_2, \dots, u_k$  — совокупность собственных векторов, принадлежащих попарно различным собственным значениям  $\lambda_1, \lambda_2, \dots, \lambda_k$ . Допустим, что

$$c_1u_1 + c_2u_2 + \dots + c_ku_k = 0.$$

Применив к обеим частям этого равенства оператор, получим

$$c_1\lambda_1u_1 + c_2\lambda_2u_2 + \dots + c_k\lambda_ku_k = 0.$$

Умножим первую зависимость на  $\lambda_k$  и вычтем из второй. Получим

$$c_1(\lambda_1 - \lambda_k)u_1 + c_2(\lambda_2 - \lambda_k)u_2 + \dots + c_{k-1}(\lambda_{k-1} - \lambda_k)u_{k-1} = 0,$$

откуда, в силу индуктивного предположения,

$$c_1(\lambda_1 - \lambda_k) = c_2(\lambda_2 - \lambda_k) = \dots = c_{k-1}(\lambda_{k-1} - \lambda_k) = 0.$$

По условию все разности  $\lambda_1 - \lambda_k, \dots, \lambda_{k-1} - \lambda_k$  отличны от нуля. Следовательно,  $c_1 = c_2 = \dots = c_{k-1} = 0$  и  $c_ku_k = 0$ . Вектор  $u_k$  ненулевой. Значит, и  $c_k = 0$ .

**Предложение 4.** *Если характеристический полином оператора  $\mathcal{A}$  не имеет кратных корней, то существует базис пространства, в котором матрица оператора диагональна.*

Действительно, в этом случае, в силу предложения 3, существует базис  $u_1, u_2, \dots, u_n$  из собственных векторов, и в этом базисе матрица оператора  $\mathcal{A}$  диагональна, в силу равенств  $\mathcal{A}u_1 = \lambda_1u_1, \mathcal{A}u_2 = \lambda_2u_2, \dots, \mathcal{A}u_n = \lambda_nu_n$ .

**Предложение 5.** *Для того чтобы существовал базис, диагонализующий матрицу оператора  $\mathcal{A}$ , необходимо и достаточно, чтобы размерности подпространств собственных векторов были равны кратностям соответствующих собственных значений как корней характеристического полинома.*

**Доказательство.** Пусть размерность подпространства собственных векторов, принадлежащих собственному значению  $\lambda$ , равна  $k$ . Ясно, что это подпространство инвариантно, матрица оператора на нем равна  $\lambda E_k$  и характеристический полином оператора  $\mathcal{A}$  на этом подпространстве равен  $(t - \lambda)^k$ . Ввиду того, что характеристический полином оператора  $\mathcal{A}$  на всем пространстве делится на характеристический полином  $\mathcal{A}$  на любом инвариантном подпространстве,  $k$  не превосходит кратности  $\lambda$  как корня характеристического полинома.

Ясно, что базис, в котором оператор  $\mathcal{A}$  имеет диагональную форму, состоит из собственных векторов и на диагонали находятся соответствующие собственные значения. Кратность корня характеристического полинома диагональной матрицы равна кратности вхождения этого корня на диагонали. Поэтому число базисных собственных векторов, отвечающих собственному значению  $\lambda$ , равно кратности  $\lambda$  как корня характеристического полинома. Следовательно размерность пространства собственных векторов, соответствующих  $\lambda$ , не меньше кратности  $\lambda$  как корня характеристического полинома, но и не больше, как было установлено выше.

**Предложение 6.** Любое собственное значение оператора является корнем его минимального полинома.

**Доказательство.** Пусть  $u$  — собственный вектор оператора  $\mathcal{A}$ , принадлежащий собственному значению  $\lambda$ . Тогда минимальным аннулятором вектора  $u$  является линейный двучлен  $t - \lambda$ . Минимальный полином оператора аннулирует все векторы, так что делится на все минимальные аннуляторы, в частности, на  $t - \lambda$ . Следовательно,  $\lambda$  есть корень минимального полинома, что и требовалось доказать.

Из предложения 6 следует, что характеристический полином оператора и его минимальный полином разлагаются на одинаковые линейные множители, различны могут быть лишь их кратности.

**2. Корневые векторы.** Вектор  $u$  называется *корневым* для оператора  $\mathcal{A}$ , если при некотором  $\lambda$  выполняется равенство  $(\mathcal{A} - \lambda \mathcal{E})^m u = 0$ , т. е. если вектор  $u$  аннулируется полиномом  $(t - \lambda)^m$ . Наименьший показатель  $m$  называется *высотой* корневого вектора. Собственный вектор — это корневой вектор высоты 1. Число  $\lambda$ , участвующее в определении корневого вектора, является собственным значением. Действительно, для корневого вектора  $u$  высоты  $m$  будет  $v = (\mathcal{A} - \lambda \mathcal{E})^{m-1} u \neq 0$ , но  $(\mathcal{A} - \lambda \mathcal{E})v = 0$ , т. е.  $v$  есть собственный вектор, принадлежащий собственному значению  $\lambda$ .

Высота корневого вектора, соответствующего собственному значению  $\lambda$ , не превосходит кратности  $\lambda$  как корня минимального полинома оператора. Эта верхняя грань достигается, т. е. существует корневой вектор, высота которого равна кратности соответствующего собственного значения как корня минимального поли-

нома. Действительно, пусть минимальный полином оператора  $\mathcal{A}$  равен  $(t - \lambda)^m F(t)$ , где  $F(\lambda) \neq 0$ . Полином  $(t - \lambda)^{m-1} F(t)$  аннулирует не все векторы, так что найдется вектор  $v$ , не аннулируемый этим полиномом. Тогда вектор  $u = F(\mathcal{A})v$  не аннулируется полиномом  $(t - \lambda)^{m-1}$ , но аннулируется полиномом  $(t - \lambda)^m$ , т. е. является корневым вектором высоты  $m$ .

**Предложение 7.** *Линейная комбинация корневых векторов, соответствующих одному и тому же собственному значению  $\lambda$ , является корневым вектором, соответствующим тому же собственному значению.*

**Доказательство.** Пусть  $u_1$  и  $u_2$  — два корневых вектора, соответствующих собственному значению  $\lambda$ , и пусть  $m_1$  и  $m_2$  — их высоты,  $m_1 \geq m_2$ . Тогда полином  $(t - \lambda)^{m_1}$  аннулирует оба вектора, а также любую их линейную комбинацию.

Таким образом, корневые векторы, соответствующие данному собственному значению, образуют подпространство, называемое *корневым подпространством*.

**Предложение 8.** *Корневые векторы, соответствующие попарно различным собственным значениям, линейно независимы.*

**Доказательство.** Пусть  $u_1, \dots, u_k$  — корневые векторы для оператора  $\mathcal{A}$ , соответствующие собственным значениям  $\lambda_1, \dots, \lambda_k$ ,  $\lambda_i \neq \lambda_j$ , и пусть  $m_1, \dots, m_k$  — их высоты. Допустим, что

$$c_1 u_1 + \dots + c_i u_i + \dots + c_k u_k = 0.$$

Рассмотрим полином

$$f_i(t) = (t - \lambda_1)^{m_1} \dots (t - \lambda_i)^{m_i - 1} \dots (t - \lambda_k)^{m_k}.$$

Применим оператор  $f_i(\mathcal{A})$  к обеим частям линейной зависимости. Этот оператор аннулирует все корневые векторы, кроме  $u_i$ , ибо полином  $f_i(t)$  делится на аннуляторы этих векторов. Но он не аннулирует  $u_i$ , ибо  $f_i(t)$  не делится на минимальный аннулятор этого вектора. Получим  $c_i f_i(\mathcal{A}) u_i = 0$ , откуда  $c_i = 0$ , ибо  $f_i(\mathcal{A}) u_i \neq 0$ . Это верно для всех  $i = 1, \dots, k$ .

**Теорема 9.** *Векторное пространство  $S$  над  $\mathbb{C}$ , в котором действует оператор  $\mathcal{A}$ , разлагается в прямую сумму корневых подпространств.*

**Доказательство.** То, что сумма корневых подпространств есть прямая сумма, следует из линейной независимости векторов из различных корневых подпространств. То, что эта сумма заполняет все пространство  $S$ , следует из предложения 8 предыдущего параграфа, ибо полиномы  $(t - \lambda_1)^{m_1}, \dots, (t - \lambda_k)^{m_k}$ , произведением которых является минимальный полином, попарно взаимно просты. Теорема доказана.

Теорема 9 есть, конечно, частный случай теоремы 9 предыдущего параграфа.

**3. Нильпотентный оператор.** Оператор  $\mathcal{B}$  называется *нильпотентным*, если некоторая его степень есть нулевой оператор. Наименьший показатель степени, обладающей этим свойством, называется показателем нильпотентности. Таким образом, если  $m$  есть показатель нильпотентности оператора  $\mathcal{B}$ , то  $\mathcal{B}^m = 0$ , но  $\mathcal{B}^{m-1} \neq 0$ . Ясно, что минимальный полином для нильпотентного оператора показателя  $m$  есть  $t^m$ . Нильпотентный оператор имеет единственное собственное значение 0. Все векторы пространства являются корневыми. Высоты их не превосходят показателя нильпотентности, и существуют векторы, высота которых равна показателю нильпотентности.

Для дальнейшего удобно считать, что нулевой вектор имеет высоту, равную нулю.

Введем в рассмотрение цепочку вложенных друг в друга инвариантных подпространств:

$$\{0\} = Q_0 \subseteq Q_1 \subseteq \dots \subseteq Q_l \subseteq \dots \subseteq Q_m = S,$$

где подпространство  $Q_j$ ,  $j = 1, \dots, m$ , состоит из векторов, высоты которых не превосходят  $j$ . По построению,  $Q_j = \ker \mathcal{B}^j$ .

**Предложение 10.** Пусть  $j \geq 2$ . Если векторы  $v_1, \dots, v_k$  принадлежат  $Q_j$  и линейно независимы относительно  $Q_{j-1}$ , то векторы  $\mathcal{B}v_1, \dots, \mathcal{B}v_k$  принадлежат  $Q_{j-1}$  и линейно независимы относительно  $Q_{j-2}$ .

**Доказательство.** Если  $v_i \in Q_j$ , то  $\mathcal{B}^j v_i = 0$ , так что  $\mathcal{B}^{j-1}(\mathcal{B}v_i) = 0$ , т. е.  $\mathcal{B}v_i \in Q_{j-1}$ . Допустим, что  $\mathcal{B}v_1, \dots, \mathcal{B}v_k$  связаны зависимостью

$$c_1 \mathcal{B}v_1 + \dots + c_k \mathcal{B}v_k \in Q_{j-2}.$$

Это значит, что  $\mathcal{B}^{j-2}(c_1 \mathcal{B}v_1 + \dots + c_k \mathcal{B}v_k) = 0$ , так что  $\mathcal{B}^{j-1}(c_1 v_1 + \dots + c_k v_k) = 0$ , т. е.

$$c_1 v_1 + \dots + c_k v_k \in Q_{j-1}.$$

Следовательно,  $c_1 = \dots = c_k = 0$ , в силу линейной независимости векторов  $v_1, \dots, v_k$  относительно  $Q_{j-1}$ . Это и требовалось доказать.

Построим теперь базис  $S$  следующим образом. Пусть  $v_{11}, \dots, v_{1k_1}$  — базис  $Q_m$  относительно  $Q_{m-1}$ . Тогда, в силу предложения 10, векторы  $\mathcal{B}v_{11}, \dots, \mathcal{B}v_{1k_1}$  принадлежат  $Q_{m-1}$  и линейно независимы относительно  $Q_{m-2}$ . Дополним эту совокупность векторов до базиса  $Q_{m-1}$  относительно  $Q_{m-2}$ . Пусть  $v_{21}, \dots, v_{2k_2}$  — дополняющая совокупность векторов. Тогда  $\mathcal{B}^2 v_{11}, \dots, \mathcal{B}^2 v_{1k_1}, \mathcal{B}v_{21}, \dots, \mathcal{B}v_{2k_2}$  принадлежат  $Q_{m-2}$  и линейно независимы относительно  $Q_{m-3}$ . Дополним их совокупность до базиса  $Q_{m-2}$  относительно  $Q_{m-3}$ . Продолжив этот процесс до построения базиса  $Q_1$ , получим следующую совокупность векторов:

$Q_m$	$v_{11}$	...	$v_{1k_1}$			
$Q_{m-1}$	$\mathcal{B}v_{11}$	...	$\mathcal{B}v_{1k_1}$	$v_{21}$	...	$v_{2k_2}$
$Q_{m-2}$	$\mathcal{B}^2v_{11}$	...	$\mathcal{B}^2v_{1k_1}$	$\mathcal{B}v_{21}$	...	$\mathcal{B}v_{2k_2}$
.....						
$Q_2$	$\mathcal{B}^{m-2}v_{11}$	...	$\mathcal{B}^{m-2}v_{1k_1}$	$\mathcal{B}^{m-3}v_{21}$	...	$\mathcal{B}^{m-3}v_{2k_2}$
$Q_1$	$\mathcal{B}^{m-1}v_{11}$	...	$\mathcal{B}^{m-1}v_{1k_1}$	$\mathcal{B}^{m-2}v_{21}$	...	$\mathcal{B}^{m-2}v_{2k_2}$

(Слева мы выписали названия подпространств, для которых каждая строка векторов образует базис относительно подпространства с меньшим на 1 индексом.)

Выписанная совокупность векторов составляет базис пространства  $Q_m = S$ . Действительно, векторы в нижней строке образуют базис  $Q_1$ . Векторы второй строки снизу образуют базис  $Q_2$  относительно  $Q_1$ , так что они вместе с векторами нижней строки составляют базис  $Q_2$ . После присоединения векторов третьей снизу строки получится базис  $Q_3$  и т. д.

Разобьем теперь построенный базис на «башни», рассматривая вместе векторы  $v_{11}, \mathcal{B}v_{11}, \dots, \mathcal{B}^{m-1}v_{11}$  и т. д., расположенные в приведенной схеме на одной вертикали. Общий вид «башни»:  $v, \mathcal{B}v, \dots, \mathcal{B}^{k-1}v$  при некотором  $k$ , причем  $\mathcal{B}^k v = 0$ . Подпространство, натянутое на векторы башни, является циклическим, порожденным вектором, находящимся наверху башни. Все пространство  $S = Q_m$  есть прямая сумма этих циклических подпространств. Тем самым мы вновь доказали теорему 10 из предыдущего параграфа для нильпотентного оператора.

Построенный базис называется *каноническим* для пространства с нильпотентным оператором. Хотя в его выборе имеется некоторый произвол, число башен каждой высоты вполне определяется размерностями подпространств  $Q_1, Q_2, \dots, Q_m$ .

На циклическом пространстве с базисом  $v, \mathcal{B}v, \dots, \mathcal{B}^{k-1}v$  (при  $\mathcal{B}^k v = 0$ ) матрица оператора  $\mathcal{B}$  имеет вид

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Такая матрица называется нильпотентным жордановым блоком. Во всем пространстве матрица нильпотентного оператора по отношению к каноническому базису квазидиагональна с жордановыми блоками вдоль диагонали. Число блоков равно числу нижних этажей башен, т. е. числу линейно независимых собственных векто-

...	$v_{m-1, 1}$	...	$v_{m-1, k_{m-1}}$	
...	$\mathcal{B}v_{m-1, 1}$	...	$\mathcal{B}v_{m-1, k_{m-1}}$	$v_{m1}$ ... $v_{mk_m}$

ров. Заметим, что результаты этого пункта сохраняют силу для векторных пространств над любым полем, а не только над полем  $\mathbb{C}$  комплексных чисел.

**4. Каноническая форма Жордана матрицы оператора.** Пространство  $S$ , в котором действует оператор  $\mathcal{A}$ , однозначно разлагается в прямую сумму корневых подпространств. Взяв в пространстве базис, составленный посредством объединения базисов корневых подпространств, мы придем к квазидиагональной матрице для оператора  $\mathcal{A}$ , диагональные блоки которой суть матрицы оператора  $\mathcal{A}$  на корневых подпространствах.

Рассмотрим корневое подпространство, соответствующее собственному значению  $\lambda$ . Оператор  $(\mathcal{A} - \lambda \mathcal{E})^m$ , где  $m$  — кратность  $\lambda$  как корня минимального полинома, аннулирует все векторы рассматриваемого подпространства, т. е. оператор  $\mathcal{B} = \mathcal{A} - \lambda \mathcal{E}$  нильпотентен на этом подпространстве.

В каноническом базисе для оператора  $\mathcal{B}$  этот оператор имеет квазидиагональную матрицу с нильпотентными жордановыми блоками вдоль диагонали. В том же базисе оператор  $\mathcal{A} = \mathcal{B} + \lambda \mathcal{E}$  будет иметь матрицу, отличающуюся от матрицы оператора  $\mathcal{B}$  тем, что к нулям на главной диагонали прибавится  $\lambda$ , ибо единичному оператору  $\mathcal{E}$  соответствует единичная матрица. Таким образом, матрица оператора на рассматриваемом корневом подпространстве есть квазидиагональная матрица, составленная из жордановых блоков

$$\begin{pmatrix} \lambda & 0 & \dots & 0 & 0 \\ 1 & \lambda & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}$$

с числом  $\lambda$  на главной диагонали. Число блоков с данным  $\lambda$  равно числу линейно независимых собственных векторов для собственного значения  $\lambda$ , ибо каждый собственный вектор оператора  $\mathcal{B}$  есть собственный вектор для оператора  $\mathcal{A}$ , соответствующий собственному значению  $\lambda$ .

Если во всех корневых подпространствах выбрать канонические базисы, то в их объединении оператор будет иметь квазидиаго-

нальную форму, диагональными блоками которой являются канонические блоки Жордана, отвечающие всем собственным значениям, т. е. каноническую форму Жордана общего вида. Тем самым мы вновь пришли к результату, полученному в конце предыдущего параграфа из более общих соображений.

На языке матриц теорема о канонической форме означает, что для квадратной матрицы  $A$  с элементами из поля  $\mathcal{C}$  существует невырожденная матрица  $C$  такая, что  $C^{-1}AC$  есть каноническая матрица Жордана.

Заметим еще, что характеристические полиномы  $(t - \lambda)^k$  жордановых блоков называются элементарными делителями матрицы  $tE - A$ . Этот термин связан с другим подходом к рассматриваемому вопросу, основанным на теории матриц над кольцом полиномов  $\mathcal{C}[t]$ . Именно, если построить наибольшие общие делители миноров порядка  $j$  матрицы  $tE - A$ , мы получим некоторые полиномы  $g_j(t)$ . Почти очевидно, что  $g_j$  делится на  $g_{j-1}$ . Их частные  $f_j = g_j/g_{j-1}$  называются инвариантными делителями матрицы  $tE - A$ . Примарные множители  $(t - \lambda_i)^k$  инвариантных делителей как раз и являются элементарными делителями матрицы  $tE - A$ . Мы не будем на этом останавливаться.

**5. Пример.** Рассмотрим в заключение параграфа один небольшой пример. Пусть  $A$  — квадратная матрица ранга 1. Ее строки пропорциональны, так что ее можно представить в виде произведения столбца  $B = (b_1, b_2, \dots, b_n)^T$  на строку  $C = (c_1, c_2, \dots, c_n)$ . Оба множителя ненулевые. Для определенности положим, что  $b_1 \neq 0$  и  $c \neq 0$ . Матрицу  $A$  будем рассматривать как оператор левого умножения в пространстве столбцов. Пусть  $X = (x_1, x_2, \dots, x_n)^T$ . Тогда  $AX = BCX = (c_1x_1 + c_2x_2 + \dots + c_nx_n)B$ .

Поэтому  $X = B$  является собственным вектором оператора  $\mathcal{A}$ , принадлежащим собственному значению  $c_1b_1 + c_2b_2 + \dots + c_nb_n$ . Далее, любой вектор с компонентами, удовлетворяющими требованию  $c_1x_1 + c_2x_2 + \dots + c_nx_n = 0$ , является собственным вектором при собственном значении, равном 0. Таких линейно независимых векторов существует  $n-1$ . Пусть это будут  $X_1, \dots, X_{n-1}$ . Если  $\lambda = c_1b_1 + c_2b_2 + \dots + c_nb_n \neq 0$ , то векторы  $B, X_1, \dots, X_{n-1}$  составляют базис из собственных векторов, и в этом базисе матрица оператора левого умножения на  $A$  принимает вид

$$\begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Если же  $c_1b_1 + c_2b_2 + \dots + c_nb_n = 0$ , то вектор  $B$  попадает в пространство, натянутое на  $X_1, \dots, X_{n-1}$ . В этом случае  $A^2 = BCBC = 0$ , ибо  $CB = 0$ , т. е.  $A$  нильпотентна показателя 2. В этом случае в канонический базис, кроме собственных векторов, нужно включить один корневой. В качестве корневого можно взять

любой такой вектор  $X$ , что  $AX \neq 0$ , что будет, если  $c_1x_1 + c_2x_2 + \dots + c_nx_n \neq 0$ . Можно взять, в частности,  $X = (1, 0, \dots, 0)^T$ . Тогда  $AX = c_1B$ . Вектор  $c_1B$  нужно дополнить до базиса пространства собственных векторов. Для того чтобы обеспечить линейную независимость этих векторов с вектором  $c_1B = (c_1b_1, \dots, c_1b_n)^T$ , достаточно взять дополняющие векторы  $X_2, \dots, X_{n-1}$  с нулевой первой компонентой и с остальными, удовлетворяющими соотношению  $c_2x_2 + \dots + c_nx_n = 0$ . Таких найдется  $n-2$  линейно независимых и не больше, ибо среди чисел  $c_2, \dots, c_n$  имеется хотя бы одно отличное от нуля, иначе равенство  $c_1b_1 + c_2b_2 + \dots + c_nb_n = 0$  было бы невозможно. В выбранном базисе  $X, c_1B, X_2, \dots, X_{n-1}$  матрица оператора умножения на  $A$  принимает вид

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Итак, в терминах матриц, существует такая невырожденная матрица  $P$ , что

$$P^{-1}AP = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad \text{если } \lambda = b_1c_1 + \dots + b_nc_n \neq 0,$$

или

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad \text{если } b_1c_1 + \dots + b_nc_n = 0.$$

## § 7. Операторы в векторных пространствах над полем $\mathbb{R}$ вещественных чисел

Поле вещественных чисел не алгебраически замкнуто, т. е. не каждый полином с вещественными коэффициентами имеет только вещественные корни. В частности, характеристический полином матрицы может иметь корни с ненулевой мнимой частью, и таким корням не соответствует собственный вектор в исходном пространстве. Поэтому преобразование матрицы оператора к канонической форме Жордана не всегда возможно. Цель настоящего параграфа — вывести достаточно наглядную каноническую форму в этом случае.

**1. Комплексификация вещественного пространства.** Пусть  $S$  — векторное пространство над полем  $\mathbb{R}$ . Погрузим его в векторное пространство  $\mathcal{S}$  над полем  $\mathbb{C}$  следующим образом. Введем в рассмотрение формальные суммы  $x + iy$  при  $x \in S, y \in S$ . Условимся

считать, что  $x + iy = x' + iy'$  в том и только в том случае, если  $x = x'$  и  $y = y'$ . Определим сложение по формуле  $(x + iy) + (x' + iy') = x + x' + i(y + y')$  и умножение на комплексные числа по формуле  $(a + bi)(x + iy) = ax - by + i(bx + ay)$ . Легко проверить, что множество  $S$  всех  $x + yi$ ,  $x \in S$ ,  $y \in S$ , удовлетворяет по отношению к введенным действием всем аксиомам векторного пространства над полем  $\mathbb{C}$ . Пространство  $S$  называется *комплексификацией* пространства  $S$ . Базис  $e_1, \dots, e_n$  пространства  $S$  оказывается базисом и для  $S$  по отношению к полю  $\mathbb{C}$ . Действительно, пусть  $x = b_1 e_1 + \dots + b_n e_n$ ,  $y = c_1 e_1 + \dots + c_n e_n$ , при  $b_i, c_i \in \mathbb{R}$ , тогда  $x + iy = (b_1 + ci)e_1 + \dots + (b_n + cn)e_n$ . Поэтому комплексификация  $S$   $n$ -мерного вещественного пространства  $S$  оказывается тоже  $n$ -мерной по отношению к полю  $\mathbb{C}$ .

Векторы из  $S$ , отождествляемые с векторами из  $S$  с нулевой второй компонентой, будем называть вещественными. Векторы  $z = x + iy$  и  $\bar{z} = x - iy$ ,  $x, y \in S$ , будем называть *комплексно сопряженными*. Легко проверить, что  $\alpha z = \bar{\alpha} \bar{z}$  при  $\alpha \in \mathbb{C}$  и  $\overline{z + z'} = \bar{z} + \bar{z}'$ .

**Предложение 1.** Если векторы  $v_1, \dots, v_k \in S$  линейно независимы над  $\mathbb{C}$ , то сопряженные векторы  $\bar{v}_1, \dots, \bar{v}_k$  тоже линейно независимы.

Действительно, если  $c_1 \bar{v}_1 + \dots + c_k \bar{v}_k = 0$ , то  $\bar{c}_1 v_1 + \dots + \bar{c}_k v_k = 0$ , откуда  $\bar{c}_1 = \dots = \bar{c}_k = 0$  и, следовательно,  $c_1 = \dots = c_k = 0$ .

**2. Продолжение операторов, действующих в вещественном пространстве, на комплексификацию.** Пусть  $\mathcal{A}$  — оператор, действующий в вещественном векторном пространстве  $S$ . Продолжим его на комплексификацию  $S$  по формуле  $\mathcal{A}(x + iy) = \mathcal{A}x + i\mathcal{A}y$ . Покажем, что продолженный оператор останется линейным и над полем  $\mathbb{C}$ . То, что он переводит сумму в сумму, очевидно, нужно только убедиться в том, что комплексный множитель можно вынести за знак оператора. Это легко проверяется. Действительно,

$$\begin{aligned} \mathcal{A}(a + bi)(x + iy) &= \mathcal{A}(ax - by + i(bx + ay)) = \\ &= \mathcal{A}(ax - by) + i\mathcal{A}(bx + ay) = a\mathcal{A}x - b\mathcal{A}y + i(b\mathcal{A}x + a\mathcal{A}y) = \\ &= (a + bi)\mathcal{A}(x + iy). \end{aligned}$$

Заметим еще, что вектор, сопряженный с  $\mathcal{A}z$ , при  $z \in S$  равен  $\mathcal{A}\bar{z}$ .

**Предложение 2.** Пусть  $z$  принадлежит комплексификации  $S$  вещественного пространства  $S$  с оператором  $\mathcal{A}$ . Пусть  $\varphi(t) = t^k + a_1 t^{k-1} + \dots + a_k$  — полином с комплексными коэффициентами, являющийся аннулятором для вектора  $z$ . Тогда полином  $\bar{\varphi}(t) = t^k + \bar{a}_1 t^{k-1} + \dots + \bar{a}_k$  с сопряженными коэффициентами есть аннулятор для вектора  $\bar{z}$ .

Действительно, переход к сопряженным в равенстве  $\mathcal{A}^k z + a_1 \mathcal{A}^{k-1} z + \dots + a_k z = 0$  дает  $\mathcal{A}^k \bar{z} + \bar{a}_1 \mathcal{A}^{k-1} \bar{z} + \dots + \bar{a}_k \bar{z} = 0$ , что и доказывает предложение.

Из доказанного предложения следует, что если  $z$  — корневой вектор, соответствующий комплексному собственному значению  $\lambda$ , то  $\bar{z}$  — корневой вектор, соответствующий сопряженному собственному значению  $\bar{\lambda}$ . Более того, учитывая сохранение линейной независимости при переходе к сопряженным векторам, мы можем заключить, что векторы, сопряженные с каноническим базисом в корневом подпространстве, соответствующем  $\lambda$ , составляют канонический базис в корневом подпространстве, соответствующем  $\bar{\lambda}$ , и каждой «башне» векторов канонического базиса для  $\lambda$  соответствует башня из сопряженных векторов для  $\bar{\lambda}$ .

**3. Каноническая форма оператора в вещественном пространстве.** Разобьем пространство  $S$  в прямую сумму корневых подпространств для оператора  $\mathcal{A}$  и затем корневые подпространства — в прямые суммы циклических, натянутых на «башни» канонического базиса. Ясно, что для каждого из вещественных собственных значений канонический базис может быть взят в самом пространстве  $S$ , и этим базисам соответствуют вещественные блоки Жордана.

Пусть теперь  $\lambda = a + bi$  — комплексное собственное значение при  $b \neq 0$ ,  $\bar{\lambda}$  — сопряженное собственное значение,  $P$  — подпространство, натянутое на башню канонического базиса корневого подпространства для  $\lambda$ ,  $\bar{P}$  — подпространство из сопряженных векторов, входящее прямым слагаемым в корневое подпространство для  $\bar{\lambda}$ . Сумма подпространств  $P + \bar{P}$  есть прямая сумма, ибо корневые подпространства для различных собственных значений  $\lambda$  и  $\bar{\lambda}$  пересекаются только по нулевому вектору. Пусть  $z_1 = x_1 + iy_1$ ,  $z_2 = x_2 + iy_2$ , ...,  $z_k = x_k + iy_k$  — базис подпространства  $P$ . Тогда  $z_1, \dots, z_k$  вместе с  $\bar{z}_1, \dots, \bar{z}_k$  составляют базис подпространства  $P \oplus \bar{P}$ . Базис (относительно поля  $\mathbb{C}$ ) составят также вещественные векторы  $x_1, y_1, \dots, x_k, y_k$ , ибо векторы  $z_1, z_2, \dots, z_k, \bar{z}_1, \bar{z}_2, \dots, \bar{z}_k$  выражаются через них линейно и, наоборот,  $x_1, y_1, \dots, x_k, y_k$  выражаются линейно через  $z_1, \bar{z}_1, \dots, z_k, \bar{z}_k$ . Вещественное подпространство, натянутое на векторы  $x_1, y_1, x_2, y_2, \dots, x_k, y_k$ , есть пересечение  $S$  и  $P \oplus \bar{P}$ . Выясним, как действует оператор  $\mathcal{A}$  на эту совокупность векторов. Вспомним, что  $z_2 = (\mathcal{A} - \lambda \mathcal{E}) z_1$ ,  $z_3 = (\mathcal{A} - \lambda \mathcal{E}) z_2$ , ...,  $z_k = (\mathcal{A} - \lambda \mathcal{E}) z_{k-1}$  и  $(\mathcal{A} - \lambda \mathcal{E}) z_k = 0$ . Перепишем эти соотношения в форме:

$$\mathcal{A}z_1 = \lambda z_1 + z_2, \mathcal{A}z_2 = \lambda z_2 + z_3, \dots$$

$$\dots, \mathcal{A}z_{k-1} = \lambda z_{k-1} + z_k, \mathcal{A}z_k = \lambda z_k.$$

Подставив  $\lambda = a + bi$  и  $z_i = x_i + iy_i$ , получим:

$$\mathcal{A}x_1 + i\mathcal{A}y_1 = ax_1 - by_1 + i(bx_1 + ay_1) + x_2 + iy_2,$$

$$\mathcal{A}x_2 + i\mathcal{A}y_2 = ax_2 - by_2 + i(bx_2 + ay_2) + x_3 + iy_3,$$

$$\dots \dots \dots$$

$$\mathcal{A}x_{k-1} + i\mathcal{A}y_{k-1} = ax_{k-1} - by_{k-1} + i(bx_{k-1} + ay_{k-1}) + x_k + iy_k,$$

$$\mathcal{A}x_k + i\mathcal{A}y_k = ax_k - by_k + i(bx_k + ay_k).$$



# ЕВКЛИДОВО И УНИТАРНОЕ ПРОСТРАНСТВА

## § 1. Определения и простейшие свойства

**1. Скалярное произведение.** В обычной геометрии на плоскости и в пространстве существеннейшую роль играют метрические понятия, связанные с измерением. К ним относятся длина отрезка и угол между прямыми. В векторной терминологии это длина вектора и угол между векторами. Длина вектора не является линейной функцией от вектора и угол между векторами не является линейной функцией от одного из векторов при фиксированном втором. Несмотря на это, из длин двух векторов и угла между ними при помощи действий, далеких от линейности, можно построить так называемое скалярное произведение векторов, являющееся билинейной функцией от векторов, т. е. линейной по каждому из векторов при фиксированном втором. Именно, скалярным произведением двух векторов называется произведение их длин и косинуса угла между ними. Билинейность почти очевидна на основании определения. Действительно, скалярное произведение векторов  $x$  и  $y$  равно длине вектора  $x$ , умноженной на величину ортогональной проекции вектора  $y$  на направление вектора  $x$ , а проекция линейной комбинации векторов на любое направление равна такой же линейной комбинации проекций. Таким образом, скалярное произведение оказывается линейной функцией от  $y$  при фиксированном  $x$  и, в силу симметрии, линейной функцией от  $x$  при фиксированном  $y$ . Тем самым скалярное произведение векторов с точки зрения алгебры проще длины вектора и угла между векторами. В свою очередь, эти величины просто выражаются через скалярное произведение. Именно, квадрат длины вектора равен скалярному произведению вектора на себя. Косинус угла между векторами равен частному от деления скалярного произведения на произведение длин.

Все сказанное дает основания при введении метрических понятий в теорию многомерных вещественных пространств отталкиваться от понятия скалярного произведения.

Дадим определения.

*Скалярным произведением*  $(x, y)$  векторов вещественного векторного пространства называется функция от векторов  $x, y$  с вещественными значениями, удовлетворяющая требованиям:

1) линейности по первому аргументу

$$(c_1x + c_2y, z) = c_1(x, z) + c_2(y, z);$$

## 2) симметрии

$$(x, y) = (y, x);$$

## 3) положительной определенности

$$(x, x) > 0 \quad \text{при } x \neq 0.$$

Из линейности по первому аргументу и симметрии следует и линейность по второму аргументу:

$$(x, c_1y + c_2z) = c_1(x, y) + c_2(x, z).$$

Далее, длиной  $|x|$  вектора  $x$  называется  $\sqrt{(x, x)}$ . В следующем пункте будет доказано неравенство  $(x, y)^2 \leq |x|^2 \cdot |y|^2$ , которое делает осмысленным определение угла  $\varphi$ , образованного векторами  $x$  и  $y$ , посредством формулы

$$\cos \varphi = \frac{(x, y)}{|x| \cdot |y|}.$$

Вещественное конечномерное пространство со скалярным произведением называется *евклидовым* пространством. Бесконечномерное пространство со скалярным произведением называется *предгильбертовым*. (Оно называется *гильбертовым*, если обладает свойством полноты как метрическое пространство, т. е. если любая последовательность вложенных замкнутых сфер с безгранично убывающими радиусами имеет общую точку. В функциональном анализе устанавливается, что предгильбертово пространство всегда может быть пополнено до гильбертова.)

В комплексном пространстве тоже вводится скалярное произведение как функция  $(x, y)$  от двух векторов  $x$  и  $y$  с комплексными значениями и удовлетворяющая следующим требованиям:

## 1) линейности по первому аргументу

$$(c_1x + c_2y, z) = c_1(x, z) + c_2(y, z);$$

## 2) симметрии с переходом к сопряженному

$$(y, x) = \overline{(x, y)};$$

## 3) положительной определенности

$$(x, x) > 0 \quad \text{при } x \neq 0.$$

Заметим, что из первых двух требований следует инволюционная (т. е. с переходом к сопряженным в коэффициентах) линейность по второму аргументу:

$$(x, c_1y + c_2z) = \bar{c}_1(x, y) + \bar{c}_2(x, z)$$

(распространенные в последние годы прилагательные «полулинейная» в смысле «линейная с инволюцией» и тем более «полуторалинейная» в смысле «билинейная с инволюционной линейностью по второму аргументу» мне представляются малоудачными).

Из условия симметрии уже следует, что  $(x, x)$  есть вещественное число, ибо  $(x, x) = \overline{(x, x)}$ , условие положительной определенности добавляет к вещественности числа  $(x, x)$  еще и положительность.

Так же, как в вещественном случае,  $(x, x)$  принимается за квадрат длины вектора  $x$ . Понятие угла между векторами в комплексном пространстве не вводится.

Конечномерное комплексное пространство со скалярным произведением, удовлетворяющим поставленным требованиям, называется *унитарным* пространством. Бесконечномерные пространства имеют название комплексных предгильбертовых и, в случае полноты, — комплексных гильбертовых пространств.

**2. Неравенство Коши.** Известное под этим названием (в более конкретной обстановке) неравенство  $|(x, y)|^2 \leq (x, x)(y, y)$  доказывается для вещественных и для комплексных пространств одним и тем же приемом. Проведем доказательство для комплексного пространства. Если  $x = 0$ , неравенство тривиально. Пусть  $x \neq 0$ . Введем в рассмотрение вектор  $z = y - \frac{(y, x)}{(x, x)} \cdot x$ . Тогда  $(z, x) = (y, x) - \frac{(y, x)}{(x, x)} \cdot (x, x) = 0$  и, следовательно,  $(z, z) = (z, y) - \frac{(y, x)}{(x, x)} (z, x) = (z, y) = (y, y) - \frac{(y, x) \cdot (x, y)}{(x, x)} = \frac{(x, x)(y, y) - |(x, y)|^2}{(x, x)}$ . Но  $(z, z) \geq 0$  и  $(x, x) > 0$ . Следовательно,

$$(x, x)(y, y) - |(x, y)|^2 \geq 0.$$

Неравенство доказано.

**3. Примеры.** Простейшими примерами евклидова и унитарного пространства являются арифметические пространства, т. е. пространства столбцов  $x = (x_1, x_2, \dots, x_n)^T$  с вещественными элементами в евклидовом случае и с комплексными в унитарном, при скалярном произведении  $(x, y) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$  и, соответственно,  $x_1 \bar{y}_1 + x_2 \bar{y}_2 + \dots + x_n \bar{y}_n$ .

Неравенство Коши для арифметического унитарного пространства имеет вид

$$|x_1 \bar{y}_1 + x_2 \bar{y}_2 + \dots + x_n \bar{y}_n|^2 \leq (|x_1|^2 + |x_2|^2 + \dots + |x_n|^2)(|y_1|^2 + |y_2|^2 + \dots + |y_n|^2).$$

Оно было установлено еще в гл. IV в качестве примера на применение теоремы Бине — Коши.

Примером предгильбертова пространства может служить пространство бесконечных последовательностей комплексных чисел, имеющих лишь конечное число ненулевых компонент. Скалярное произведение  $x = (x_1, x_2, \dots)$  и  $y = (y_1, y_2, \dots)$  определяется как  $(x, y) = x_1 \bar{y}_1 + x_2 \bar{y}_2 + \dots$ . Эта сумма имеет лишь конечное число отличных от нуля слагаемых. Для того чтобы пополнить это пространство до гильбертова, нужно присоединить бесконечные последовательности  $x = (x_1, x_2, \dots)$  со сходящимися рядами из квадратов модулей. Если  $x$  и  $y$  — две такие последовательности, то применив неравенство Коши к отрезкам ряда  $x_1 \bar{y}_1 + x_2 \bar{y}_2 + \dots$ , легко получим, что этот ряд абсолютно сходится. Его сумму и нужно принять за скалярное произведение. Так построенное пространство обозначается  $l_2$ .

Еще один важный пример предгильбертова пространства дают комплекснозначные непрерывные на данном промежутке  $[a, b]$

функции со скалярным произведением  $(f, g) = \int_a^b f(t) \overline{g(t)} dt$ . Применение неравенства Коши в этой ситуации дает интегральное неравенство

$$\left| \int_a^b f(t) \overline{g(t)} dt \right|^2 \leq \int_a^b |f(t)|^2 dt \cdot \int_a^b |g(t)|^2 dt.$$

Для пополнения этого пространства до гильбертова нужно присоединить функции с суммируемым (т. е. интегрируемым в смысле Лебега) квадратом модуля.

**4. Евклидово и унитарное пространства в общем случае.** Пусть  $S$  — евклидово пространство и  $e_1, e_2, \dots, e_n$  — некоторый его базис. Пусть  $x = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$  и  $y = y_1 e_1 + y_2 e_2 + \dots + y_n e_n$ . Тогда, в силу билинейности скалярного произведения,  $(x, y) = \sum_{i,j} g_{ij} x_i y_j$ , где  $g_{ij} = (e_i, e_j)$ . В силу симметрии скалярного произведения  $g_{ij} = g_{ji}$ , так что матрица  $(g_{ij})$  (называемая *матрицей Грама* для базиса  $e_1, \dots, e_n$ ) симметрична. Далее,  $(x, x) = \sum_{i,j} g_{ij} x_i x_j$  и, в силу требования  $(x, x) > 0$  при  $x \neq 0$ ,  $(g_{ij})$  — положительно определенная матрица (т. е. является матрицей положительно определенной квадратичной формы). В матричной форме скалярное произведение записывается в виде  $X^T G Y$ , где  $X$  и  $Y$  — столбцы из координат векторов  $x$  и  $y$  и  $G = (g_{ij})$ . При преобразовании координат с матрицей  $C$  скалярное произведение в новых координатах  $X', Y'$  запишется в виде  $X'^T C^T G C Y'$ , так что матрица Грама преобразуется по формуле преобразования квадратичной формы:  $C' = C^T G C$ . В главе V (см. стр. 153 и 163) было установлено, что положительно определенная квадратичная форма может быть приведена к сумме квадратов новых переменных, т. е.

к квадратичной форме с единичной матрицей коэффициентов. Следовательно, в евклидовом пространстве существует такой базис, в котором матрица Грама есть единичная матрица. Это значит, что  $(e_i, e_i) = 1$  и  $(e_i, e_j) = 0$  при  $i \neq j$ . Такой базис называется *ортонормальным*.

Пусть теперь  $S$  — унитарное пространство и  $e_1, \dots, e_n$  — его базис. Тогда  $(x, y) = \sum g_{ij} x_i \bar{y}_j = X^T G \bar{Y}$ , где  $X$  и  $Y$  — столбцы из координат  $x$  и  $y$ ,  $G = (g_{ij})$ , где  $g_{ij} = (e_i, e_j)$ ,  $x_1, \dots, x_n$  и  $y_1, \dots, y_n$  — координаты векторов  $x$  и  $y$  в выбранном базисе. В этой ситуации матрица Грама  $G = (g_{ij})$  эрмитово симметрична, ибо  $(e_j, e_i) = \overline{(e_i, e_j)}$ . Скалярное произведение имеет вид  $(x, x) = \sum g_{ij} x_i \bar{x}_j$ , т. е. представляется в виде эрмитовой формы от  $\bar{x}_1, \dots, \bar{x}_n$  с матрицей  $G$ . Эта форма является положительно определенной. При преобразовании координат с матрицей  $C$  матрица Грама преобразуется в  $C^T G C = C_1^* G C_1$ , где  $C_1 = \bar{C}$ , т. е. изменяется по формуле преобразования матрицы эрмитовой формы. Положительно определенная эрмитова форма может быть преобразована к сумме квадратов модулей новых переменных т. е. к эрмитовой форме с единичной матрицей. Следовательно и в этом случае существует ортонормальный базис со свойствами  $(e_i, e_i) = 1$  и  $(e_i, e_j) = 0$  при  $i \neq j$ .

В п. 6 это обстоятельство будет установлено без ссылки на алгебраическую теорию квадратичных и эрмитовых форм, но при помощи соображений довольно прозрачных при пользовании геометрической терминологией. По существу же эти соображения почти равносильны преобразованию положительно определенных форм к каноническому виду.

**5. Ортогонализация совокупности векторов.** Векторы  $u$  и  $v$  унитарного (или евклидова) пространства называются *ортогональными*, если  $(u, v) = 0$ . Из  $(u, v) = 0$  следует, что  $(v, u) = 0$ , так как  $(v, u) = \overline{(u, v)}$ . Из ортогональности  $u$  и  $v$  следует ортогональность  $c_1 u$  и  $c_2 v$  при любых  $c_1$  и  $c_2$ . Нулевой вектор ортогонален любому другому. Верно и обратное утверждение:

**Предложение 1.** Если вектор  $v$  ортогонален всем векторам унитарного (евклидова) пространства, то он равен нулю.

Действительно, если вектор ортогонален всем векторам пространства, то он ортогонален самому себе, т. е.  $(v, v) = 0$  и  $v = 0$ .

**Предложение 2.** Попарно ортогональные ненулевые векторы линейно независимы.

Действительно, пусть  $v_1, v_2, \dots, v_k$  — попарно ортогональные ненулевые векторы, так что  $(v_i, v_j) = 0$  при  $i \neq j$  и  $(v_i, v_i) > 0$ . Пусть  $c_1 v_1 + \dots + c_i v_i + \dots + c_k v_k = 0$ . Тогда  $(c_1 v_1 + \dots + c_i v_i + \dots + c_k v_k, v_i) = 0$ , откуда  $c_i (v_i, v_i) = 0$  и, наконец,  $c_i = 0$ .

**Теорема 3 (об ортогонализации).** Пусть  $v_1, v_2, \dots, v_k$  — линейно независимая совокупность векторов в унитарном (или евклидовом) пространстве. Исходя из нее, можно построить от-

личные от нуля попарно ортогональные векторы  $v'_1, v'_2, \dots, v'_k$  так, что

$$\begin{aligned} v'_1 &= v_1, \\ v'_2 &= v_2 + c_{21}v_1, \\ v'_3 &= v_3 + c_{31}v_1 + c_{32}v_2, \\ &\dots \\ v'_{k-1} &= v_{k-1} + c_{k-1,1}v_1 + c_{k-1,2}v_2 + \dots + c_{k-1,k-2}v_{k-2}, \\ v'_k &= v_k + c_{k1}v_1 + c_{k2}v_2 + \dots + c_{k,k-1}v_{k-1}, \end{aligned}$$

т. е. каждый вектор  $v'_i$  получается из  $v_i$  посредством прибавления линейной комбинации предыдущих векторов  $v_1, \dots, v_{i-1}$ .

Доказательство. Применим индукцию по  $k$ . База индукции при  $k=1$  тривиальна. Пусть теорема доказана для совокупности из  $k-1$  вектора, и в этом предположении докажем для  $k$ .

Будем искать  $v'_k$  в виде суммы  $v_k$  и линейной комбинации уже ортогональных векторов  $v'_1, v'_2, \dots, v'_{k-1}$ :

$$v'_k = v_k + b_1v'_1 + b_2v'_2 + \dots + b_{k-1}v'_{k-1}.$$

Приравняем нулю  $(v'_k, v'_i)$  при  $i < k$ . Получим:

$$\begin{aligned} 0 &= (v_k, v'_i) + b_1(v'_1, v'_i) + \dots + b_i(v'_i, v'_i) + \dots + b_{k-1}(v'_{k-1}, v'_i) = \\ &= (v_k, v'_i) + b_i(v'_i, v'_i), \end{aligned}$$

откуда  $b_i$  определяется однозначно:  $b_i = -\frac{(v_k, v'_i)}{(v'_i, v'_i)}$ . Выразим

теперь  $v'_k$  через  $v_k, v_1, \dots, v_{k-1}$ . Получим

$$\begin{aligned} v'_k &= v_k + b_1v_1 + \\ &+ b_2(v_2 + c_{21}v_1) + \dots + b_{k-1}(v_{k-1} + c_{k-1,1}v_1 + \dots + c_{k-1,k-2}v_{k-2}) = \\ &= v_k + c_{k1}v_1 + c_{k2}v_2 + \dots + c_{k,k-1}v_{k-1} \end{aligned}$$

при некоторых  $c_{k1}, c_{k2}, \dots, c_{k,k-1}$ . Остается показать, что  $v'_k \neq 0$ . Но если бы  $v'_k = 0$ , то векторы  $v_1, v_2, \dots, v_{k-1}, v_k$  были бы линейно зависимы.

Теорема доказана.

Процесс ортогонализации можно провести несколько иначе. Сначала построить векторы  $u_2, u_3, \dots, u_k$ , добавив к  $v_2, v_3, \dots, v_k$  подходящие кратные  $v_1$  так, чтобы  $u_2, u_3, \dots, u_k$  стали бы ортогональны  $v_1$ . Затем построить векторы  $u'_3, \dots, u'_k$  за счет добавления к  $u_3, \dots, u_k$  подходящего кратного вектора  $u_2$  с тем, чтобы  $u'_3, \dots, u'_k$  стали ортогональны к  $u_2$ . При этом ортогональность  $v_1$  сохранится. Процесс продолжается до конца. В итоге векторы

$v_1, u_2, u'_3, \dots$  — это те же векторы  $v'_1, v'_2, \dots, v'_k$ , что и в первом процессе. Заметим, что так осуществленный процесс ортогонализации точно воспроизводит процесс преобразования положительно определенной эрмитовой (или квадратичной) формы к каноническому виду.

Дадим еще одну интерпретацию процесса ортогонализации. Последовательность  $F$  вложенных подпространств  $0 = P_0 \subset P_1 \subset \dots \subset P_{k-1} \subset P_k$  называется *флагом*, если размерность каждого подпространства на единицу больше размерности предыдущего, так что  $\dim P_i = i$ . Базисом флага называется базис пространства  $P_k$ , включающий базисы всех подпространств, составляющих флаг, так что если  $v_1, v_2, \dots, v_k$  — базис флага, то  $v_1$  — базис  $P_1$ ,  $v_1$  и  $v_2$  — базис  $P_2$  и т. д.

Пусть  $v_1, v_2, \dots, v_k$  — базис флага  $F$ , и пусть

$$\begin{aligned} v'_1 &= c_{11}v_1, \\ v'_2 &= c_{21}v_1 + c_{22}v_2, \\ v'_3 &= c_{31}v_1 + c_{32}v_2 + c_{33}v_3, \\ &\vdots \\ v'_k &= c_{k1}v_1 + c_{k2}v_2 + \dots + c_{kk}v_k, \end{aligned}$$

причем  $c_{11} \neq 0, c_{22} \neq 0, \dots, c_{kk} \neq 0$ .

Тогда  $v'_1$  — ненулевой вектор в  $P_1$ ,  $v'_2$  принадлежит  $P_2$  и не является линейной комбинацией  $v'_1$  и т. д.,  $v'_i$  принадлежит  $P_i$  и не является линейной комбинацией  $v'_1, \dots, v'_{i-1}$  при всех  $i$ . Следовательно,  $v'_1, v'_2, \dots, v'_i$  линейно независимы и образуют базис  $P_i$ , так что  $v'_1, v'_2, \dots, v'_k$  есть базис флага  $F$ . Ясно, что любой базис флага  $F$  связан с базисом  $v_1, v_2, \dots, v_k$  формулами указанного вида.

Вернемся к теореме об ортогонализации. Примем исходную систему векторов  $v_1, v_2, \dots, v_k$  за базис некоторого флага  $F$ . Тогда векторы  $v'_1, v'_2, \dots, v'_k$  после проведения ортогонализации составят базис того же флага, но составленный из попарно ортогональных векторов. Поэтому теорема об ортогонализации может быть сформулирована следующим образом:

*Для любого флага существует ортогональный базис, т. е. базис, состоящий из попарно ортогональных векторов.*

**6. Ортонормальный базис.** Вектор в унитарном (или евклидовом) пространстве называется *нормированным*, если его длина равна 1. Любой отличный от нуля вектор можно умножить на некоторое число так, что в результате получится нормированный вектор. Действительно, пусть  $x \neq 0$ . Тогда  $(ax, ax) = a\bar{a}(x, x) = |a|^2(x, x)$ . Достаточно взять  $a$  таким, что  $|a| = \frac{1}{\sqrt{(x, x)}} = \frac{1}{|x|}$ .

Так выбранное число  $a$  называется *нормирующим множителем* для вектора  $x$ . В унитарном пространстве нормирующий множитель определен с точностью до множителя с модулем, равным 1. В евклидовом пространстве нормирующий множитель определен с точностью до знака.

Ясно, что если векторы ортогональны, то и после их нормирования получатся ортогональные векторы.

Пусть теперь  $v_1, v_2, \dots, v_n$  — какой-либо базис унитарного (или евклидова) пространства. Применив к нему процесс ортогонализации, придем к ортогональному базису. После нормирования всех базисных векторов придем к базису, составленному из попарно ортогональных и нормированных векторов  $e_1, e_2, \dots, e_n$ . Такой базис носит название *ортонормального*. Для ортонормального базиса выполняются соотношения  $(e_i, e_i) = 1$  и  $(e_i, e_j) = 0$  при  $i \neq j$ , так что матрица Грама для ортонормального базиса есть единичная матрица.

Скалярное произведение векторов в координатах в ортонормальном базисе имеет, очевидно, вид  $(x, y) = x_1\bar{y}_1 + x_2\bar{y}_2 + \dots + x_n\bar{y}_n$ , т. е. точно такой же, как в арифметическом пространстве столбцов.

Тем самым установлен изоморфизм, с сохранением скалярных произведений, унитарного (или евклидова) пространства с арифметическим пространством столбцов.

**7. Преобразование координат при замене ортонормального базиса.** Напомним, что матрица преобразования координат, с которой координаты векторов в базисе  $e_1, e_2, \dots, e_n$  выражаются через координаты в базисе  $e'_1, e'_2, \dots, e'_n$ , имеет своими столбцами координаты векторов  $e'_1, e'_2, \dots, e'_n$  относительно базиса  $e_1, e_2, \dots, e_n$ .

Допустим, что  $e_1, e_2, \dots, e_n$  и  $e'_1, e'_2, \dots, e'_n$  — ортонормальные базисы унитарного (или евклидова) пространства. Векторы  $e'_1, e'_2, \dots, e'_n$  нормированы, следовательно, суммы квадратов модулей элементов столбцов матрицы равны 1. Далее,  $(e'_i, e'_j) = 0$  при  $i \neq j$ , так что суммы произведений элементов  $i$ -го столбца на числа, сопряженные с элементами  $j$ -го столбца, равны 0. Следовательно, матрица преобразования координат при замене ортонормальных базисов унитарна (ортогональна для евклидова пространства).

Ясно, что любая унитарная (ортогональная) матрица является матрицей преобразования координат при замене ортонормального базиса на некоторый тоже ортонормальный базис.

## § 2. Подпространства унитарного (или евклидова) пространства

**1. Ортонормальный базис подпространства и его дополнение до ортонормального базиса пространства.** Любое подпространство унитарного (или евклидова) пространства само является унитар-

ным (евклидовым) по отношению к тому же скалярному умножению.

Пусть  $P$  есть  $k$ -мерное подпространство  $n$ -мерного унитарного (евклидова) пространства  $S$ . Пусть  $e_1, \dots, e_k$  — ортонормальный базис  $P$ . Дополним его до базиса  $S$ , присоединив векторы  $v_{k+1}, \dots, v_n$ . Применим к базису  $e_1, \dots, e_k, v_{k+1}, \dots, v_n$  процесс ортогонализации. Первые векторы  $e_1, \dots, e_k$  при этом не изменятся, так как они попарно ортогональны. Получим ортогональный базис  $e_1, \dots, e_k, v'_{k+1}, \dots, v'_n$ . Чтобы получить ортонормальный базис  $S$ , остается только нормировать векторы  $v'_{k+1}, \dots, v'_n$ .

**2. Ортогональное дополнение.** Пусть  $S$  есть  $n$ -мерное унитарное (или евклидово) пространство и  $P$  — его  $k$ -мерное подпространство,  $1 \leq k \leq n-1$ . Ортогональным дополнением  $P^\perp$  к подпространству  $P$  называется множество всех векторов из  $S$ , ортогональных всем векторам из  $P$ . Ясно, что если векторы ортогональны всем векторам из  $P$ , то любая их линейная комбинация обладает тем же свойством. Поэтому  $P^\perp$  есть подпространство  $S$ .

Пусть  $e_1, \dots, e_k$  — ортонормальный базис  $P$  и  $e_1, \dots, e_k, e_{k+1}, \dots, e_n$  — включающий его ортонормальный базис  $S$ . Натянем на векторы  $e_{k+1}, \dots, e_n$  подпространство  $Q$ . Любой вектор из  $Q$ , будучи линейной комбинацией векторов  $e_{k+1}, \dots, e_n$ , ортогонален векторам  $e_1, \dots, e_k$  и, следовательно, любой их линейной комбинации, т. е. любому вектору из  $P$ . Следовательно,  $Q \subseteq P^\perp$ . Пусть теперь вектор  $x = x_1 e_1 + \dots + x_k e_k + x_{k+1} e_{k+1} + \dots + x_n e_n \in P^\perp$ . Тогда  $(x, e_i) = x_i = 0$  при  $i = 1, \dots, k$ , так что  $x = x_{k+1} e_{k+1} + \dots + x_n e_n \in Q$ . Итак, любой вектор из  $Q$  принадлежит  $P^\perp$  и любой вектор из  $P^\perp$  принадлежит  $Q$ . Подпространства  $Q$  и  $P^\perp$  совпадают.

Таким образом, ортогональное дополнение  $P^\perp$  к подпространству  $P$  есть подпространство, натянутое на векторы, дополняющие ортонормальный базис  $P$  до ортонормального базиса  $S$ .

Теперь легко установить следующие свойства ортогональных дополнений.

$$1. \dim P^\perp = \dim S - \dim P.$$

Непосредственно следует из построения базиса  $P^\perp$ .

$$2. (P^\perp)^\perp = P.$$

Действительно, в качестве векторов, дополняющих ортонормальный базис  $e_{k+1}, \dots, e_n$  подпространства  $P^\perp$  до ортонормального базиса  $S$ , можно взять  $e_1, \dots, e_k$ , и натянутое на эти векторы подпространство  $(P^\perp)^\perp$  совпадает с  $P$ .

$$3. \text{Если } P_1 \subset P_2, \text{ то } P_1^\perp \supset P_2^\perp.$$

Ясно из определения ортогонального дополнения.

$$4. (P_1 + P_2)^\perp = P_1^\perp \cap P_2^\perp.$$

Действительно, любой вектор из  $(P_1 + P_2)^\perp$  ортогонален всем векторам из  $P_1$  и всем векторам из  $P_2$ , т. е. принадлежит  $P_1^\perp \cap P_2^\perp$ .

Обратно, любой вектор из  $P_1^\perp \cap P_2^\perp$  ортогонален всем векторам из  $P_1$  и всем векторам из  $P_2$  и любым их суммам, т. е. принадлежит  $(P_1 + P_2)^\perp$ .

Перейдя в свойстве 4 к ортогональным дополнениям, получим  $P_1 + P_2 = (P_1^\perp \cap P_2^\perp)^\perp$ . Заменяя в этом равенстве  $P_1^\perp$  и  $P_2^\perp$  на  $P_1$  и  $P_2$ , получим:

$$5. (P_1 \cap P_2)^\perp = P_1^\perp + P_2^\perp.$$

Таким образом, переход к ортогональным дополнениям обращает отношение включения подпространств и переставляет операции сложения и пересечения подпространств.

$$6. S = P \oplus P^\perp.$$

Действительно, базис  $S$  есть объединение базисов  $P$  и  $P^\perp$ . В этой ситуации говорят, что пространство  $S$  есть *ортогональная сумма* подпространств  $P$  и  $P^\perp$ .

Более общо, скажем, что  $S$  есть ортогональная сумма своих подпространств  $P_1, \dots, P_k$ , если  $S = P_1 + \dots + P_k$ , причем векторы, взятые из различных подпространств, ортогональны. Ортогональная сумма всегда прямая, ибо из равенства  $v_1 + \dots + v_k = 0$  при  $v_i \in P_i$  следует равенство нулю всех слагаемых  $v_i$ , ибо наличие ненулевых слагаемых в левой части противоречило бы линейной независимости ненулевых попарно ортогональных векторов.

### § 3. Пространства, сопряженные с евклидовым и унитарным пространствами

#### 1. Пространство, сопряженное с евклидовым пространством.

Пусть  $S$  — евклидово пространство. Любому вектору  $y \in S$  можно поставить в соответствие линейную функцию  $l_y \in S^*$  со значениями  $l_y(x) = (x, y)$ . Если  $y \neq z$ , то  $l_y \neq l_z$ , ибо равенство  $(x, y) = (x, z)$  при всех  $x \in S$  значит, что  $(x, y - z) = 0$  при всех  $x$ , что возможно только при  $y = z$ . Пусть  $x_1, \dots, x_n$  — координаты вектора  $x$  в ортонормальном базисе. Любая линейная функция от  $x$  представляется в виде  $y_1 x_1 + \dots + y_n x_n$  при некоторых  $y_1, \dots, y_n$ , т. е. в виде  $(x, y)$ , где  $y$  — вектор с координатами  $y_1, \dots, y_n$ . Таким образом, между векторами из  $S$  и ковекторами из  $S^*$  имеется естественное взаимно однозначное соответствие  $y \leftrightarrow l_y$ . Далее, из линейности скалярного произведения по второму аргументу  $(x, c_1 y_1 + c_2 y_2) = c_1 (x, y_1) + c_2 (x, y_2)$  следует, что линейной комбинации векторов соответствует такая же линейная комбинация ковекторов. Таким образом, соответствие  $y \leftrightarrow l_y$  задает изоморфизм пространства  $S$  и сопряженного с ним пространства  $S^*$ .

#### 2. Пространство, сопряженное с унитарным пространством.

Так же, как в евклидовом пространстве, устанавливается взаимно однозначное соответствие между векторами и ковекторами по пра-

в силу  $y \leftrightarrow l_y$ , где  $l_y$  — линейная функция со значениями  $l_y(x) = (x, y)$ . Линейность функции  $l_y$  следует из линейности скалярного произведения относительно первого аргумента.

Однако линейной комбинации векторов соответствует линейная комбинация ковекторов с сопряженными коэффициентами, в силу свойства  $(x, c_1 y_1 + c_2 y_2) = \bar{c}_1(x, y_1) + \bar{c}_2(x, y_2)$ . Таким образом, между унитарным пространством и его сопряженным имеется инволюционный изоморфизм, с заменой коэффициентов на сопряженные при линейном комбинировании.

#### § 4. Операторы в унитарном пространстве

**1. Инвариантный флаг для оператора в комплексном пространстве.** Пусть  $S$  — векторное пространство над полем  $\mathbb{C}$ , и  $\mathcal{A}$  — линейный оператор в  $S$ .

*Предложение 1. Для оператора  $\mathcal{A}$ , действующего в комплексном пространстве  $S$ , существует флаг, составленный из инвариантных подпространств.*

Для доказательства достаточно установить, что для каждого  $k$ -мерного инвариантного подпространства  $P_k$  найдется объемлющее его  $(k+1)$ -мерное инвариантное подпространство  $P_{k+1}$ . Пусть  $\bar{S} = S/P_k$  и  $\bar{\mathcal{A}}$  — оператор, индуцированный оператором  $\mathcal{A}$  на  $\bar{S}$ . Пусть  $\lambda$  — собственное значение оператора  $\bar{\mathcal{A}}$  и  $\bar{u} \in \bar{S}$  — соответствующий собственный вектор. Пусть  $u$  — произвольный вектор из класса  $\bar{u}$ . Тогда  $\mathcal{A}u \equiv \lambda u \pmod{P_k}$ , т. е.  $\mathcal{A}u = \lambda u + z$  при  $z \in P_k$ . Вектор  $u$  не принадлежит  $P_k$ , ибо  $\bar{u} \neq 0$ . Пусть  $P_{k+1}$  — подпространство, натянутое на базис  $P_k$  и на вектор  $u$ . Оно  $(k+1)$ -мерно, ибо  $u \notin P_k$ . Оно инвариантно. Действительно,  $x \in P_{k+1}$  значит, что  $x = cu + y$  при  $y \in P_k$ . Тогда  $\mathcal{A}x = c\mathcal{A}u + \mathcal{A}y = c\lambda u + cz + \mathcal{A}y \in P_{k+1}$ , ибо  $u, z$  и  $\mathcal{A}y$  принадлежат  $P_{k+1}$ . Тем самым предложение 1 доказано.

В любом базисе флага, составленного из инвариантных подпространств, оператор имеет верхнюю треугольную матрицу. Действительно, пусть  $u_1, u_2, \dots, u_n$  — базис флага, состоящего из инвариантных подпространств  $P_1, P_2, \dots, P_n$ . Тогда  $\mathcal{A}u_1 \in P_1$ , т. е.  $\mathcal{A}u_1 = \lambda_1 u_1$ . Далее,  $\mathcal{A}u_2 \in P_2$ , т. е.  $\mathcal{A}u_2 = a_{12}u_1 + \lambda_2 u_2$ ,  $\mathcal{A}u_3 = a_{13}u_1 + a_{23}u_2 + \lambda_3 u_3$  и т. д. Матрица из координатных столбцов векторов  $\mathcal{A}u_1, \mathcal{A}u_2, \dots, \mathcal{A}u_n$  есть

$$A = \begin{pmatrix} \lambda_1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & \lambda_2 & a_{23} & \dots & a_{2n} \\ 0 & 0 & \lambda_3 & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Диагональные элементы матрицы  $A$  суть собственные значения оператора  $\mathcal{A}$ , ибо характеристический полином матрицы  $A$  равен  $(t - \lambda_1)(t - \lambda_2) \dots (t - \lambda_n)$ .

Пусть теперь  $S$  — унитарное пространство. В силу теоремы об ортогонализации для любого флага существует ортонормальный базис. Следовательно, верна следующая теорема Шура:

**Теорема 2.** *Для любого оператора в унитарном пространстве существует ортонормальный базис, в котором оператор имеет верхнюю треугольную матрицу.*

Любую квадратную комплексную матрицу можно принять за матрицу линейного оператора по отношению к некоторому ортонормальному базису. Переход от исходного ортонормального базиса к ортонормальному базису инвариантного флага влечет преобразование координат с унитарной матрицей. Поэтому теорема Шура имеет следующий эквивалент на языке матриц:

*Для любой квадратной комплексной матрицы  $A$  существует такая унитарная матрица  $C$ , что  $C^{-1}AC$  есть верхняя треугольная матрица.*

Рассмотрим один интересный частный случай. Пусть матрица сама унитарна. Тогда верхняя треугольная матрица  $C^{-1}AC$  тоже унитарна и, следовательно, ее строки и столбцы нормированны, т. е. суммы квадратов модулей элементов всех ее строк и столбцов равны 1. Но легко видеть, что верхняя треугольная матрица

$$\begin{pmatrix} \lambda_1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & \lambda_2 & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

с нормированными строками и столбцами диагональна и ее диагональные элементы по модулю равны 1. Действительно, рассматривая сумму квадратов модулей элементов первого столбца, получим  $|\lambda_1|^2 = 1$ . Для первой строки теперь получим  $|\lambda_1|^2 + |a_{12}|^2 + \dots + |a_{1n}|^2 = 1$ , откуда  $|a_{12}|^2 + \dots + |a_{1n}|^2 = 0$  и  $a_{12} = \dots = a_{1n} = 0$ . Теперь обратимся ко второму столбцу и затем второй строке. Получим  $|\lambda_2|^2 = 1$  и  $a_{23} = \dots = a_{2n} = 0$  и т. д. Таким образом, для унитарных матриц верна следующая теорема:

**Теорема 3.** *Для любой унитарной матрицы  $A$  найдется такая унитарная матрица  $C$ , что  $C^{-1}AC$  диагональна. Все собственные значения унитарной матрицы равны по модулю 1.*

Эту теорему мы получим далее в качестве частного случая более общей теоремы.

**2. Сопряженный оператор.** Сопряженным оператором для данного оператора  $\mathcal{A}$ , действующего в унитарном пространстве  $S$ , называется такой оператор  $\mathcal{A}^*$ , что при любых векторах  $x$  и  $y$  имеет место равенство  $(\mathcal{A}x, y) = (x, \mathcal{A}^*y)$ .

Докажем существование сопряженного оператора. С этой целью перейдем к координатной записи. Пусть  $(x_1, x_2, \dots, x_n)^T$  — столбец из координат вектора  $x$  в некотором ортонормальном базисе,  $(y_1, y_2, \dots, y_n)^T$  — координаты вектора  $y$  и  $A = (a_{ij})$  — матрица оператора  $\mathcal{A}$ .



Свойство 1 очевидно из рассмотрения матриц для  $\mathcal{A}$  и  $\mathcal{A}^*$ . Это же легко проверяется и бескоординатно:

$$(\mathcal{A}^*x, y) = (\overline{y}, \overline{\mathcal{A}^*x}) = (\overline{\mathcal{A}y}, \overline{x}) = (x, \mathcal{A}y).$$

Свойства 2 и 3 непосредственно получаются из определения сопряженного оператора. Свойство 4 проверяется, например, так:  $(\mathcal{A}\mathcal{B}x, y) = (\mathcal{B}x, \mathcal{A}^*y) = (x, \mathcal{B}^*\mathcal{A}^*y)$ .

Для дальнейшего важно еще одно, менее очевидное свойство сопряженного оператора.

**Предложение 4.** *Ортогональное дополнение  $P^\perp$  к инвариантному для оператора  $\mathcal{A}$  подпространству  $P$  инвариантно для оператора  $\mathcal{A}^*$ .*

**Доказательство.** Пусть  $y \in P^\perp$ . Это значит, что  $y$  ортогонален всем векторам из  $P$ , в частности, всем векторам  $\mathcal{A}x$  при  $x \in P$ . Это значит, что  $(\mathcal{A}x, y) = 0$  и  $(x, \mathcal{A}^*y) = 0$ . Это равенство верно для всех  $x \in P$ , следовательно,  $\mathcal{A}^*y \in P^\perp$ .

**3. Нормальные операторы.** Оператор, действующий в унитарном пространстве, называется *нормальным*, если он перестановочен со своим сопряженным. К классу нормальных операторов относятся самосопряженные операторы, совпадающие со своими сопряженными, и унитарные операторы, для каждого из которых сопряженный равен обратному.

В ортонормальном базисе самосопряженный оператор имеет эрмитову матрицу, а унитарный — унитарную.

**Предложение 5.** *Если  $\mathcal{A}$  — нормальный оператор,  $\mathcal{E}$  — единичный и  $\alpha$  — любое комплексное число, то оператор  $\mathcal{B} = \mathcal{A} - \alpha\mathcal{E}$  тоже нормальный.*

**Доказательство.** Проверим равенство  $\mathcal{B}\mathcal{B}^* = \mathcal{B}^*\mathcal{B}$ . Имеем

$$\mathcal{B}\mathcal{B}^* = (\mathcal{A} - \alpha\mathcal{E})(\mathcal{A}^* - \bar{\alpha}\mathcal{E}) = \mathcal{A}\mathcal{A}^* - \alpha\mathcal{A}^* - \bar{\alpha}\mathcal{A} + \alpha\bar{\alpha}\mathcal{E};$$

$$\mathcal{B}^*\mathcal{B} = (\mathcal{A}^* - \bar{\alpha}\mathcal{E})(\mathcal{A} - \alpha\mathcal{E}) = \mathcal{A}^*\mathcal{A} - \bar{\alpha}\mathcal{A} - \alpha\mathcal{A}^* + \alpha\bar{\alpha}\mathcal{E}.$$

Поэтому  $\mathcal{B}\mathcal{B}^* = \mathcal{B}^*\mathcal{B}$ , ибо  $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$ .

**Предложение 6.** *Собственный вектор нормального оператора есть собственный вектор и сопряженного оператора, соответствующий сопряженному собственному значению.*

**Доказательство.** Пусть  $u$  — собственный вектор нормального оператора  $\mathcal{A}$ , принадлежащий собственному значению  $\lambda$ . Тогда  $\mathcal{A}u = \lambda u$ , что можно записать как  $\mathcal{B}u = 0$ , где  $\mathcal{B} = \mathcal{A} - \lambda\mathcal{E}$ . Из равенства  $\mathcal{B}u = 0$  следует, что  $(\mathcal{B}u, \mathcal{B}u) = 0$ . Но  $(\mathcal{B}u, \mathcal{B}u) = (u, \mathcal{B}^*\mathcal{B}u) = (u, \mathcal{B}^*\mathcal{B}u) = (\mathcal{B}^*u, \mathcal{B}^*u)$ . Следовательно,  $\mathcal{B}^*u = 0$ , откуда  $(\mathcal{A}^* - \bar{\lambda}\mathcal{E})u = 0$  и  $\mathcal{A}^*u = \bar{\lambda}u$ , что и требовалось доказать.

**Теорема 7.** *Для нормального оператора существует ортонормальный базис, в котором матрицы оператора и его сопряженного диагональны и их соответствующие диагональные элементы сопряжены.*

**Доказательство.** Пусть  $u_1$  — нормированный собственный вектор для нормального оператора  $\mathcal{A}$  и  $P_1$  — одномерное подпро-

пространство, натянутое на вектор  $u_1$ . Так как  $u_1$  является собственным вектором и для  $\mathcal{A}^*$ , подпространство  $P_1$  инвариантно и для  $\mathcal{A}^*$ . Следовательно, ортогональное дополнение  $P_1^\perp$  к  $P_1$  инвариантно как для  $\mathcal{A}$ , так и для  $\mathcal{A}^*$ . Ограничения операторов  $\mathcal{A}$  и  $\mathcal{A}^*$  на  $P_1^\perp$  останутся взаимно сопряженными, ибо раз равенство  $(\mathcal{A}x, y) = (x, \mathcal{A}^*y)$  верно для всех векторов  $x, y$  пространства, оно будет верно и для векторов из  $P_1^\perp$ . Для оператора  $\mathcal{A}$  на  $P_1^\perp$  найдется нормированный собственный вектор  $u_2$ . Он ортогонален вектору  $u_1$ . Вектор  $u_2$  будет собственным и для  $\mathcal{A}^*$ . Поэтому подпространство  $P_2$ , натянутое на векторы  $u_1$  и  $u_2$ , инвариантно как для  $\mathcal{A}$ , так и для  $\mathcal{A}^*$ . Его ортогональное дополнение  $P_2^\perp$  тоже инвариантно для  $\mathcal{A}$  и  $\mathcal{A}^*$ , которые на  $P_2^\perp$  останутся взаимно сопряженными. В  $P_2^\perp$  находится нормированный собственный вектор  $u_3$ , который ортогонален  $u_1$  и  $u_2$ , он будет собственным вектором и для оператора  $\mathcal{A}^*$ . Продолжая этот процесс шаг за шагом, построим ортонормальную совокупность собственных векторов для  $\mathcal{A}$ , которая в конце концов даст базис пространства. В этом базисе матрицы операторов  $\mathcal{A}$  и  $\mathcal{A}^*$  диагональны. Соответствующие диагональные элементы будут сопряжены как собственные значения операторов  $\mathcal{A}$  и  $\mathcal{A}^*$ , соответствующие одному и тому же собственному вектору. Теорема доказана.

По ходу доказательства теоремы мы конструировали ортонормальный базис из собственных векторов. Но некоторые собственные векторы ортогональны автоматически.

*Предложение 8. Собственные векторы нормального оператора, принадлежащие различным собственным значениям, ортогональны.*

Действительно, пусть  $u$  и  $v$  — собственные векторы нормального оператора  $\mathcal{A}$ , соответствующие собственным значениям  $\lambda$  и  $\mu$ ,  $\lambda \neq \mu$ . Тогда  $u$  и  $v$  будут собственными векторами и для сопряженного оператора  $\mathcal{A}^*$ , соответствующие собственным значениям  $\bar{\lambda}$  и  $\bar{\mu}$ . Подсчитаем двумя способами число  $(\mathcal{A}u, v)$ . С одной стороны,  $(\mathcal{A}u, v) = (\lambda u, v) = \lambda(u, v)$ . С другой стороны,  $(\mathcal{A}u, v) = (u, \mathcal{A}^*v) = (u, \bar{\mu}v) = \bar{\mu}(u, v)$ . Сравнив, получим  $(\lambda - \mu)(u, v) = 0$ , откуда  $(u, v) = 0$ , что и требовалось доказать.

Доказанное предложение дает возможность указать другую конструкцию для построения ортонормального базиса из собственных векторов.

В силу диагонализуемости матрицы нормального оператора любой вектор пространства равен сумме собственных векторов, и, следовательно, пространство равно сумме подпространств собственных векторов, принадлежащих попарно различным собственным значениям. В силу предложения 8 эта сумма ортогональная. Поэтому для построения ортонормального базиса всего пространства достаточно объединить ортонормальные базисы всех подпространств собственных векторов.

Нормальность оператора не только достаточна для диагонализуемости матрицы в некотором ортонормальном базисе, но и необходима. Действительно, если матрица оператора  $\mathcal{A}$  равна  $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ , то в том же базисе матрица сопряженного базиса сопряжена с матрицей  $\mathcal{A}$ , т. е. равна  $\text{diag}(\bar{\lambda}_1, \bar{\lambda}_2, \dots, \bar{\lambda}_n)$ , а любые диагональные матрицы коммутируют.

**4. Самосопряженные операторы.** Предложение 9. *Для того чтобы нормальный оператор был самосопряженным, необходимо и достаточно, чтобы все его собственные значения были вещественными.*

Действительно, матрица самосопряженного оператора в любом ортонормальном базисе совпадает с сопряженной, в частности, диагональная матрица, получающаяся в базисе из собственных векторов. Но диагональная матрица совпадает с сопряженной, составленной из комплексно сопряженных чисел, в том и только в том случае, когда она вещественна. Элементы, находящиеся на диагонали, равны собственным значениям.

Предложение о возможности унитарного преобразования матрицы самосопряженного оператора к вещественной форме в терминах матриц означает, что для любой эрмитовой матрицы  $A$  существует унитарная матрица  $C$  такая, что  $C^{-1}AC = C^*AC$  есть вещественная диагональная матрица. Это равносильно тому, что эрмитова форма с матрицей  $A$  может быть приведена к каноническому виду посредством преобразования переменных с унитарной матрицей. Это было сформулировано в конце гл. V.

Если оператор  $\mathcal{A}$  самосопряженный, то  $(\mathcal{A}x, x)$  вещественно при всех значениях вектора  $x$ . Действительно,  $(\mathcal{A}x, x) = (x, \mathcal{A}^*x) = (x, \mathcal{A}x) = (\mathcal{A}x, x)$ .

Если все значения  $(\mathcal{A}x, x)$  при ненулевых векторах  $x$  положительны, то самосопряженный оператор  $\mathcal{A}$  называется положительно определенным. Если  $u_1, \dots, u_n$  — ортонормальный базис из собственных векторов оператора  $\mathcal{A}$  при собственных значениях  $\lambda_1, \dots, \lambda_n$  и  $x_1, x_2, \dots, x_n$  — координаты вектора  $x$  в этом базисе, то

$$\begin{aligned} (\mathcal{A}x, x) &= (\mathcal{A}(x_1u_1 + \dots + x_nu_n), x_1u_1 + \dots + x_nu_n) = \\ &= (x_1\lambda_1u_1 + \dots + x_n\lambda_nu_n, x_1u_1 + \dots + x_nu_n) = \\ &= \lambda_1|x_1|^2 + \dots + \lambda_n|x_n|^2. \end{aligned}$$

Из этого равенства следует, что для положительной определенности оператора необходимо и достаточно, чтобы все его собственные значения были положительны.

**Предложение 10.** *Из положительно определенного самосопряженного оператора можно «извлечь квадратный корень», являющийся самосопряженным положительно определенным оператором. Это значит, что для положительно определенного самосо-*

пряженного оператора  $\mathcal{A}$  существует положительно определенный оператор  $\mathcal{B}$  такой, что  $\mathcal{B}^2 = \mathcal{A}$ .

Доказательство. Пусть  $\lambda_1, \lambda_2, \dots, \lambda_n$  — собственные значения самосопряженного положительно определенного оператора  $\mathcal{A}$  и  $u_1, u_2, \dots, u_n$  — ортонормальный базис из соответствующих собственных векторов. Все числа  $\lambda_1, \lambda_2, \dots, \lambda_n$  положительны, и из них можно извлечь положительные квадратные корни.

Пусть  $\mathcal{B}$  — оператор, имеющий собственные векторы  $u_1, u_2, \dots, u_n$  и собственные значения  $\sqrt{\lambda_1}, \sqrt{\lambda_2}, \dots, \sqrt{\lambda_n}$ . Этот оператор самосопряжен, ибо его матрица в ортонормальном базисе  $u_1, u_2, \dots, u_n$  диагональна и вещественна. Он положительно определен, ибо его собственные значения положительны. Квадрат его матрицы в базисе  $u_1, u_2, \dots, u_n$  равен матрице оператора  $\mathcal{A}$  в том же базисе. Следовательно,  $\mathcal{B}^2 = \mathcal{A}$ .

**Теорема 11.** *Любой невырожденный оператор равен произведению унитарного на положительно определенный.*

Доказательство. Пусть  $\mathcal{A}$  — невырожденный оператор. Тогда оператор  $\mathcal{A}^* \mathcal{A}$  самосопряженный и положительно определенный.

Действительно,  $(\mathcal{A}^* \mathcal{A})^* = \mathcal{A}^* (\mathcal{A}^*)^* = \mathcal{A}^* \mathcal{A}$ . Далее, при  $x \neq 0$  имеем  $(\mathcal{A}^* \mathcal{A}x, x) = (\mathcal{A}x, \mathcal{A}x) > 0$ , ибо  $\mathcal{A}x \neq 0$  при  $x \neq 0$ . Пусть  $\mathcal{B}$  — квадратный корень из оператора  $\mathcal{A}^* \mathcal{A}$ . Тогда  $\mathcal{A}^* \mathcal{A} = \mathcal{B}^2$ . Умножив это равенство справа и слева на  $\mathcal{B}^{-1}$ , получим

$$\mathcal{B}^{-1} \mathcal{A}^* \mathcal{A} \mathcal{B}^{-1} = \mathcal{E}.$$

Но  $\mathcal{B}^{-1} \mathcal{A}^* = (\mathcal{A} \mathcal{B}^{-1})^*$ . Таким образом, оператор  $\mathcal{A} \mathcal{B}^{-1}$  и его сопряженный взаимно обратны, т. е. оператор  $\mathcal{U} = \mathcal{A} \mathcal{B}^{-1}$  унитарный. Следовательно,

$$\mathcal{A} = \mathcal{U} \mathcal{B},$$

что и требовалось доказать.

Это разложение носит название *полярного разложения оператора*.

Существует и другое полярное разложение, в котором положительно определенный множитель находится слева, а унитарный справа. Действительно, применив полярное разложение к сопряженному оператору  $\mathcal{A}^*$ , получим

$$\mathcal{A}^* = \mathcal{U} \mathcal{B},$$

и переход к сопряженным дает

$$\mathcal{A} = \mathcal{B}^* \mathcal{U}^* = \mathcal{B} \mathcal{U}^{-1}.$$

Оператор  $\mathcal{U}^{-1}$  унитарен вместе с  $\mathcal{U}$ .

**5. Оператор ортогонального проектирования.** Пусть  $S = P \oplus \mathcal{Q}$ , где  $\mathcal{Q} = P^\perp$ . В этом случае проектирование называется ортогональным, и соответствующий оператор называется *оператором ортогонального проектирования*. Оператор ортогонального проектирования самосопряжен, ибо он имеет вещественную диагональ-

ную матрицу в ортонормальном базисе, получающемся посредством объединения ортонормальных базисов  $P$  и  $Q$ .

**Предложение 12.** *Любой самосопряженный идемпотентный оператор есть оператор ортогонального проектирования.*

Действительно, любой идемпотентный оператор  $\mathcal{A}$ , как мы видели на стр. 331, является оператором проектирования  $S$  на  $P = \mathcal{A}S$  параллельно  $Q = (\mathcal{E} - \mathcal{A})S$ . Нужно доказать только, что  $P$  и  $Q$  ортогональны. Пусть  $x = \mathcal{A}u \in P$  и  $y = v - \mathcal{A}v \in Q$ . Тогда  $(x, y) = (\mathcal{A}u, v - \mathcal{A}v)$ . В силу самосопряженности  $\mathcal{A}$  имеем  $(\mathcal{A}u, v - \mathcal{A}v) = (u, \mathcal{A}v - \mathcal{A}^2v) = (u, 0) = 0$ , что и требовалось доказать.

## 6. Унитарные операторы.

**Предложение 13.** *Для того чтобы нормальный оператор был унитарен, необходимо и достаточно, чтобы его собственные значения были равны 1 по модулю.*

Действительно, диагональная матрица нормального оператора в ортонормальном базисе из собственных векторов унитарна в том и только в том случае, если все ее диагональные элементы, т. е. собственные значения, равны 1 по модулю.

Предложение о возможности унитарного преобразования подобия матрицы унитарного оператора к диагональной форме мы получили ранее более формальными средствами при помощи теоремы Шура.

## § 5. Операторы в евклидовом пространстве

**1. Комплексификация евклидова пространства.** Пусть  $S$  — евклидово пространство и  $\bar{S}$  — его комплексификация. Введем скалярное произведение в  $\bar{S}$  по формуле:

$$(x + yi, u + vi) = (x, u) + (y, v) + i((y, u) - (x, v)).$$

Нужно проверить корректность этого определения. Аддитивность по первому аргументу при фиксированном втором очевидна. Для проверки линейности по первому аргументу достаточно убедиться в возможности вынесения комплексного множителя из первого аргумента. Соответствующее вычисление не представляет труда, но довольно громоздко. Именно:

$$\begin{aligned} ((a + bi)(x + yi), u + vi) &= (ax - by + (bx + ay)i, u + vi) = \\ &= (ax - by, u) + (bx + ay, v) + i((bx + ay, u) - (ax - by, v)) = \\ &= a(x, u) - b(y, u) + b(x, v) + a(y, v) + b(x, u)i + \\ &\quad + a(y, u)i - a(x, v)i + b(y, v)i = \\ &= (a + bi)((x, u) + (y, v) + i((y, u) - (x, v))) = \\ &= (a + bi)(x + yi, u + vi). \end{aligned}$$

Симметрия с инволюцией очевидна — при перестановке местами  $x + yi$  и  $u + vi$  вещественная часть скалярного произведения не меняется, а мнимая меняет знак на обратный.

Наконец,  $(x + yi, x + yi) = (x, x) + (y, y) + i((y, x) - (x, y)) = (x, x) + (y, y) > 0$ , если  $x + yi \neq 0$ . Таким образом, комплексификация  $S$  евклидова пространства  $S$  становится унитарным пространством.

Заметим еще, что скалярное произведение пары векторов  $x + yi$ ,  $u + vi$  и скалярное произведение пары комплексно сопряженных с ними векторов  $x - yi$ ,  $u - vi$  комплексно сопряженные. Это непосредственно следует из определения скалярного произведения в  $S$ .

**2. Операторы в евклидовом пространстве и их продолжение на комплексификацию.** В евклидовом пространстве для оператора  $A$  определяется сопряженный оператор  $A^*$  той же формулой  $(Ax, y) = (x, A^*y)$  при любых  $x$  и  $y$ , что и в унитарном пространстве. Доказательство существования и единственности сопряженного оператора ничем не отличается от аналогичных доказательств для унитарного пространства. Матрица оператора  $A^*$  в ортонормальном базисе просто транспонирована с матрицей оператора  $A$ . При продолжении взаимно сопряженных операторов  $A$  и  $A^*$  с  $S$  на  $S$  они останутся сопряженными.

Действительно,

$$\begin{aligned} (A(x + iy), u + iv) &= (Ax + iAy, u + iv) = \\ &= (Ax, u) + (Ay, v) - (Ax, v)i + (Ay, u)i = \\ &= (x, A^*u) + (y, A^*v) - (x, A^*v)i + (y, A^*u)i = \\ &= ((x + yi), (A^*u + A^*vi)) = (x + yi, A^*(u + vi)). \end{aligned}$$

**3. Нормальные операторы в евклидовом пространстве.** Нормальный оператор  $A$  в евклидовом пространстве  $S$  остается нормальным и при его продолжении на комплексификацию  $S$  пространства  $S$ . Поэтому в  $S$  существует ортонормальный базис из собственных векторов, диагонализующий матрицу оператора  $A$ .

Для вещественных собственных значений можно взять вещественные собственные векторы, т. е. лежащие в  $S$ . Действительно, координаты собственных векторов относительно базиса  $S$  определяются из линейных однородных уравнений с вещественными коэффициентами в случае вещественности собственного значения.

Комплексные собственные значения появляются парами сопряженных с одинаковой кратностью. Выбрав ортонормальный базис из собственных векторов, принадлежащих некоторому собственному значению  $\lambda = a + bi$  при  $b \neq 0$ , базис из собственных векторов для собственного значения  $\bar{\lambda} = a - bi$  можно взять из векторов, сопряженных с векторами базиса собственных значений для  $\lambda$ . Такой базис будет ортонормальным. Теперь натянем на каждую пару  $u + vi$  и  $u - vi$  сопряженных векторов двумерное комплексное подпространство. Все эти подпространства инвариантны, ортогональны друг другу и вещественным собственным

векторам, соответствующим вещественным собственным значениям.

Комплексное пространство, натянутое на векторы  $u + vi$  и  $u - vi$ , очевидно, совпадает с комплексным подпространством, натянутым на вещественные векторы  $u$  и  $v$ , и, следовательно, является комплексификацией вещественного подпространства, натянутого на  $u$  и  $v$ .

Далее, из ортогональности собственных векторов  $u + vi$  и  $u - vi$ , принадлежащих различным собственным значениям  $\lambda = a + bi$  и  $\bar{\lambda} = a - bi$ , следует:

$$0 = (u + vi, u - vi) = (u, u) - (v, v) + i((v, u) + (u, v)) = \\ = (u, u) - (v, v) + 2i(u, v),$$

ибо в евклидовом пространстве  $S$  скалярное произведение симметрично.

Из этого равенства следует, что  $(u, v) = 0$ , т. е. векторы  $u$  и  $v$  ортогональны, а также  $(u, u) = (v, v)$ . Вспомним теперь, что вектор  $u + vi$  нормированный, т. е., ввиду ортогональности  $u$  и  $v$ ,  $(u, u) + (v, v) = 1$ . Поэтому  $(u, u) = (v, v) = 1/2$ , так что векторы  $u$  и  $v$  не нормированны, но становятся нормированными после умножения на  $\sqrt{2}$ .

Итак, для нормального оператора, действующего в евклидовом пространстве  $S$ , существует ортонормальный базис, составленный из собственных векторов, принадлежащих вещественным собственным значениям, и умноженных на  $\sqrt{2}$  вещественных и мнимых частей собственных векторов, принадлежащих комплексным собственным значениям. Одномерные подпространства, натянутые на вещественные собственные векторы, и двумерные, натянутые на компоненты комплексных собственных векторов, инвариантны, так что матрица оператора в построенном базисе квазидиагональна и составлена из диагональных блоков первого и второго порядка. Блоки первого порядка — это вещественные собственные значения. Найдем блоки второго порядка. Пусть  $u + vi$  — собственный вектор, принадлежащий собственному значению  $a + bi$ . Тогда

$$\mathcal{A}(u + vi) = (a + bi)(u + vi),$$

откуда

$$\mathcal{A}u = au - bv,$$

$$\mathcal{A}v = bu + av.$$

Ровно те же соотношения сохраняются после умножения векторов  $u$  и  $v$  на  $\sqrt{2}$ . Таким образом, блоки второго порядка имеют вид

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Заметим еще, что эти блоки появляются из подпространства, натянутого на сопряженные собственные векторы, принадлежащие сопряженным собственным значениям  $a \pm bi$ , так что наряду с блоком  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , записанным при помощи собственного значения  $a + bi$ , не нужно включать блок  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ , соответствующий собственному значению  $a - bi$ .

**4. Самосопряженные операторы в евклидовом пространстве.** Нормальный оператор в евклидовом пространстве самосопряжен в том и только в том случае, если все его собственные значения вещественны. Действительно, самосопряженный оператор в евклидовом пространстве остается самосопряженным и в комплексификации. Поэтому существует ортонормальный базис в самом евклидовом пространстве, в котором его матрица диагональна. В терминах матриц это значит, что для любой вещественной симметричной матрицы  $A$  существует ортогональная матрица  $C$  такая, что  $C^{-1}AC = C^T AC$  диагональна. Это обстоятельство было выяснено еще в гл. V в связи с ортогональным преобразованием квадратичной формы к каноническому виду. Тесная связь между теорией самосопряженных операторов в евклидовом пространстве с теорией квадратичных форм ясно видна из того, что скалярное произведение  $(Ax, x)$  выражается через координаты вектора  $x$  в ортонормальном базисе в виде квадратичной формы с матрицей, равной матрице оператора  $A$  в том же базисе, и при ортогональном преобразовании координат матрица оператора и матрица квадратичной формы преобразуются одинаково:

$$A \rightarrow C^{-1}AC = C^T AC,$$

ибо для ортогональной матрицы  $C^{-1} = C^T$ .

Для самосопряженных операторов в евклидовом пространстве имеют место те же свойства, которые отмечались для самосопряженных операторов в унитарном пространстве, и их доказательства ничем не отличаются от доказательств в случае унитарного пространства.

Поэтому ограничимся их перечислением.

Самосопряженный оператор положительно определен в том и только в том случае, когда его собственные значения положительны.

Из самосопряженного положительно определенного оператора можно извлечь положительно определенный квадратный корень.

Любой невырожденный оператор можно представить в виде произведения положительно определенного самосопряженного оператора на ортогональный, как в одном, так и в другом порядке.

Оператор ортогонального проектирования есть самосопряженный идемпотентный оператор и обратно, самосопряженный идемпотентный оператор есть оператор ортогонального проектирования.

**5. Ортогональные операторы.** Ортогональный оператор имеет ортогональную матрицу в любом ортонормальном базисе. Так как ортогональный оператор нормален, существует ортонормальный базис, в котором матрица оператора блочно-диагональна и состоит из вещественных чисел  $\lambda_i$  на диагонали и блоков вида  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ . Из ортогональности такой матрицы следует, что  $\lambda_i = \pm 1$ , и в каждом блоке второго порядка  $a^2 + b^2 = 1$ . (Это можно увидеть также из того, что ортогональный оператор становится унитарным при продолжении на комплексификацию, и, следовательно, все его собственные значения равны 1 по модулю.)

Можно положить  $a = \cos \varphi$ ,  $b = \sin \varphi$ . Оператор на плоскости с матрицей  $\begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix}$  есть оператор вращения плоскости на угол  $-\varphi$ .

Ортогональный оператор называется *собственно ортогональным*, если определитель его матрицы равен 1; если же определитель равен  $-1$ , то оператор называется *несобственно ортогональным*. Порядок базисных векторов можно выбрать так, чтобы по диагонали следовали сначала 1, потом  $-1$  и за ними блоки второго порядка. В случае, если оператор собственно ортогонален, число диагональных элементов, равных  $-1$ , четно. Матрицу второго порядка  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$  удобно рассматривать как блок второго порядка  $\begin{pmatrix} \cos \pi & \sin \pi \\ -\sin \pi & \cos \pi \end{pmatrix}$ , геометрически означающий поворот плоскости на  $\pi$ .

Таким образом, действие собственно ортогонального оператора геометрически означает следующее. Пространство разбивается в ортогональную сумму подпространств, одно из которых натянуто на собственные векторы, принадлежащие собственному значению 1, — это подпространство неподвижных векторов, и нескольких двумерных подпространств, каждое из которых вращается на некоторый угол (вообще говоря, разные плоскости на разные углы).

В случае несобственно ортогонального оператора имеется еще один базисный вектор, переходящий в противоположный под действием оператора.

## § 6. Преобразование уравнения гиперповерхности второго порядка к каноническому виду

**1. Пространство точек.** Пусть дано векторное пространство  $S$ . *Пространством точек* для  $S$  называется однородное пространство  $M$  для аддитивной группы пространства  $S$  с нулевыми стабилизаторами для всех точек  $M$  (заметим, что, в силу коммутативности группы, стабилизаторы всех точек совпадают).

Подробнее,  $M$  есть множество объектов, называемых *точками*, для которых определено действие *сдвига* на вектор, переводящее точку в точку.

Записывая эту операцию знаком  $+$ , мы придем к следующим свойствам этой операции:

1.  $(m + x) + y = m + (x + y)$ , где  $m \in M$ ,  $x, y \in S$ .
2.  $m + 0 = m$ , где  $0$  — нулевой вектор.
3. Для любых точек  $m_1$  и  $m_2$  из  $M$  найдется такой вектор  $x$ , что  $m_1 + x = m_2$ .
4. Если  $m + x = m$ , то  $x = 0$ .

Первые два требования означают, что  $M$  есть множество, на котором определено действие «сдвига» на векторы из  $S$ , т. е.  $M$  есть  $S^+$ -множество (здесь  $S^+$  обозначает аддитивную группу пространства  $S$ ). Третье условие означает однородность  $M$  как  $S^+$ -множества. Наконец, четвертое, — что стабилизаторы всех точек состоят только из  $0$ .

Зафиксировав некоторую точку  $m_0$  в  $M$ , мы можем сопоставить каждой точке  $m$  из  $M$  вектор, переводящий  $m_0$  в  $m$ . Этот вектор назовем координатным вектором для  $m$  при выбранном начале координат  $m_0$ . Соответствие между точками и их координатными векторами взаимно однозначно. Началу координат соответствует нулевой вектор.

Если изменить начало координат, перенеся его на вектор  $x_0$  в точку  $m'_0$ , то координатные векторы  $x$  и  $x'$  любой точки  $m \in M$  относительно начал  $m_0$  и  $m'_0$  связаны очевидным соотношением

$$x = x_0 + x'.$$

Выбор начала координат в пространстве точек и выбор базиса в векторном пространстве  $S$  дает возможность сопоставить каждой точке ее координаты, именно, координаты координатного вектора точки относительно выбранного базиса.

Если  $S$  — евклидово пространство, то соответствующее пространство точек называется евклидовым. Координаты точек относительно некоторого начала и ортонормального базиса в  $S$  носят название прямоугольных координат. Преобразование координат при фиксированном начале, но с переходом от одного ортонормального базиса  $S$  к другому, называется преобразованием поворота осей. В дальнейших пунктах этого параграфа пространство точек будет предполагаться евклидовым.

**2. Алгебраические гиперповерхности.** Множество всех точек в пространстве, координаты  $x_1, \dots, x_n$  которых связаны соотношением  $F(x_1, \dots, x_n) = 0$ , где  $F$  — полином с вещественными коэффициентами, называется *алгебраической гиперповерхностью*. Степень полинома  $F$  называется степенью или порядком гиперповерхности.

Гиперповерхности первой степени называются гиперплоскостями. В векторной форме уравнение любой гиперплоскости можно

записать в виде  $(b, x) = p$ , где  $b$  — некоторый ненулевой вектор,  $x$  — координатный вектор точки. Без нарушения общности можно считать вектор  $b$  нормированным. Тогда уравнение  $(b, x) = p$  называется нормальным уравнением гиперплоскости.

Если уравнение гиперповерхности в  $n$ -мерном пространстве имеет вид  $F(x_1, \dots, x_k) = 0$  при  $k < n$ , то координаты  $x_{k+1}, \dots, x_n$  остаются произвольными. В этом случае говорят, что гиперповерхность является цилиндрической гиперповерхностью с  $(n - k)$ -мерными образующими, построенной на гиперповерхности с тем же уравнением, в  $k$ -мерном подпространстве, натянутом на первые  $k$  базисных векторов, исходящих из начала координат.

**3. Гиперповерхности второго порядка.** В векторной форме уравнение гиперповерхности второго порядка можно записать в виде

$$(\mathcal{A}x, x) + 2(b, x) + c = 0,$$

где  $\mathcal{A}$  — самосопряженный оператор,  $b$  — вектор и  $c$  — число. Действительно, в виде  $(\mathcal{A}x, x)$  записывается квадратичная форма, составленная из членов второй степени полинома,  $2(b, x)$  является записью суммы членов первой степени, наконец,  $c$  — свободный член.

Выясним, как изменяется уравнение при переносе начала координат. Пусть  $x$  — координатный вектор при исходном начале координат,  $y$  — координатный вектор при новом начале и  $x_0$  — координатный вектор нового начала относительно исходного. Тогда, подставив  $x = x_0 + y$  в уравнение поверхности, получим, как легко видеть, преобразованное уравнение в виде

$$(\mathcal{A}y, y) + 2(\mathcal{A}x_0 + b, y) + c + 2(b, x_0) + (\mathcal{A}x_0, x_0) = 0.$$

Если уравнение  $\mathcal{A}x_0 + b = 0$  разрешимо, то за счет переноса начала можно в уравнении уничтожить первые степени координат. Если же уравнение  $\mathcal{A}x_0 + b = 0$  не имеет решений, то этого достигнуть нельзя. Таким образом, нужно рассмотреть два случая, в зависимости от разрешимости или неразрешимости уравнения  $\mathcal{A}x_0 + b = 0$ .

**4. Первый случай гиперповерхности второго порядка.** Пусть уравнение  $\mathcal{A}x_0 + b = 0$  разрешимо. Тогда, сдвинув начало координат на вектор  $x_0$ , приходим к уравнению

$$(\mathcal{A}y, y) + c' = 0,$$

где  $c' = c + 2(b, x_0) + (\mathcal{A}x_0, x_0)$ .

Теперь сделаем поворот осей, приняв за базис пространства векторов ортонормальный базис из собственных векторов оператора  $\mathcal{A}$ . Пусть этот базис образован векторами  $u_1, \dots, u_k, u_{k+1}, \dots, u_n$ , причем  $u_1, \dots, u_k$  принадлежат ненулевым собственным значениям  $\lambda_1, \dots, \lambda_k$ , а  $u_{k+1}, \dots, u_n$  принадлежат нулевому собственному значению. Обозначив через  $y'_1, \dots, y'_k, y'_{k+1}, \dots, y'_n$  координаты вектора  $y$  в этом базисе, получим уравнение гиперпо-

верхности в виде

$$\lambda_1 y_1'^2 + \dots + \lambda_k y_k'^2 + c' = 0.$$

Если  $k < n$ , то гиперповерхность будет цилиндрической с  $(n - k)$ -мерными образующими, построенной на гиперповерхности с уравнением  $\lambda_1 y_1'^2 + \dots + \lambda_k y_k'^2 + c' = 0$  в  $k$ -мерном подпространстве. Если  $c' = 0$ , то поверхность *коническая*, именно, если точка  $m$  с координатным вектором  $y$  лежит на поверхности, то и прямая, проходящая через начало координат и точку  $m$ , т. е. множество точек с координатными векторами  $ty$ ,  $-\infty < t < +\infty$ , целиком лежит на гиперповерхности. Если при этом  $\lambda_1, \dots, \lambda_k$  одного знака, то конус вырождается в одну точку — начало координат. Конусы классифицируются по максимальному числу коэффициентов одного знака.

Если же  $c' \neq 0$ , то, разделив обе части уравнения на  $-c'$ , приходим к уравнению

$$a_1 y_1'^2 + \dots + a_k y_k'^2 = 1.$$

Если все коэффициенты  $a_1, \dots, a_k$  отрицательны, то на гиперповерхности нет точек. Если все коэффициенты положительны, то для координат точек на гиперповерхности имеют место неравенства  $|y_k'| \leq 1/\sqrt{a_k}$ , так что гиперповерхность ограничена. В этом случае гиперповерхность в  $k$ -мерном пространстве носит название *эллипсоида* или, в случае  $a_1 = \dots = a_k$ , *сферы* радиуса  $1/\sqrt{a_1}$ .

Если же среди коэффициентов  $a_1, \dots, a_k$  имеются как положительные, так и отрицательные, то гиперповерхности (в  $k$ -мерном пространстве) носят название *гиперболоидов*. Гиперболоиды классифицируются по числу отрицательных коэффициентов  $a_1, \dots, a_k$ .

Конусы, эллипсоиды, гиперболоиды и построенные на них цилиндрические гиперповерхности носят название *центральных*, так как начало координат после преобразования к каноническому виду оказывается центром симметрии. Действительно, точки с координатными векторами  $y$  и  $-y$  одновременно принадлежат или не принадлежат гиперповерхности.

**5. Второй случай гиперповерхности второго порядка.** Пусть теперь уравнение  $\mathcal{A}x_0 + b = 0$  не разрешимо. Это возможно, только если размерность образа оператора  $\mathcal{A}$  меньше  $n$ , т. е. оператор имеет нетривиальное ядро и среди его собственных значений имеется число 0.

Напомним, что для самосопряженного оператора образ и ядро ортогонально дополнителны. Образ есть подпространство, натянутое на собственные векторы оператора, принадлежащие ненулевым собственным значениям, а ядро состоит из собственных векторов, принадлежащих собственному значению 0.

Разобьем вектор  $b$  на два слагаемых,  $b = b_1 + b_2$ , из которых первое принадлежит образу оператора  $\mathcal{A}$ , второе — его ортого-

нальному дополнению, т. е. ядру. В рассматриваемом случае  $b_2 \neq 0$ . Тогда уравнение  $\mathcal{A}x + b_1 = 0$  разрешимо, и все его решения получаются из частного решения  $x_1$  добавлением произвольного вектора из ядра оператора  $\mathcal{A}$ . Если  $x_2 = x_1 + z$  при  $z$  из ядра, то  $(\mathcal{A}x_2, x_2) = (\mathcal{A}x_1, x_1 + z) = (\mathcal{A}x_1, x_1) + (\mathcal{A}x_1, z) = (\mathcal{A}x_1, x_1) + (x_1, \mathcal{A}z) = (\mathcal{A}x_1, x_1)$ . Таким образом, для любого решения  $x_2$  уравнения  $\mathcal{A}x + b_1 = 0$  число  $(\mathcal{A}x_2, x_2)$  остается неизменным.

Будем искать вектор сдвига начала в виде  $x_0 = x_1 + tb_2$ , при вещественном  $t$ . Так как  $b_2$  принадлежит ядру  $\mathcal{A}$ , будут иметь место равенства  $\mathcal{A}x_0 + b_1 = 0$  и  $(\mathcal{A}x_0, x_0) = (\mathcal{A}x_1, x_1)$ . После такого сдвига начала уравнение примет вид

$$(\mathcal{A}y, y) + 2(\mathcal{A}x_0 + b_1, y) + 2(b_2, y) + c + 2(b_1, x_0) + \\ + 2(b_2, x_0) + (\mathcal{A}x_0, x_0) = 0.$$

Слагаемое  $2(\mathcal{A}x_0 + b_1, y)$  в левой части исчезает. Далее,  $(b_1, x_0) = (b_1, x_1 + tb_2) = (b_1, x_1)$ , ибо  $b_1$  и  $b_2$  ортогональны;  $(b_2, x_0) = (b_2, x_1) + t(b_2, b_2)$ ;  $(\mathcal{A}x_0, x_0) = (\mathcal{A}x_1, x_1)$ . Таким образом, уравнение принимает вид

$$(\mathcal{A}y, y) + 2(b_2, y) + 2t(b_2, b_2) + 2(b_2, x_1) + 2(b_1, x_1) + \\ + (\mathcal{A}x_1, x_1) + c = 0.$$

Если взять

$$t = - \frac{(2b_2, x_1) + 2(b_1, x_1) + (\mathcal{A}x_1, x_1) + c}{2(b_2, b_2)},$$

то уравнение примет вид

$$(\mathcal{A}y, y) + 2(b_2, y) = 0.$$

Пусть  $b_2 = -pv$ , где  $v$  — нормированный вектор. При этом уравнение примет вид

$$(\mathcal{A}y, y) = 2p(v, y).$$

Теперь сделаем поворот осей, приняв за новый базис нормированные собственные векторы  $u_1, \dots, u_k$ , принадлежащие ненулевым собственным значениям  $\lambda_1, \dots, \lambda_k$  оператора  $\mathcal{A}$ , и нормированные собственные векторы  $u_{k+1}, \dots, u_n$ , принадлежащие нулевому собственному значению, включив в их число вектор  $v$ . Пусть  $v = u_{k+1}$ .

Уравнение в новых координатах  $y'_1, \dots, y'_n$  примет вид

$$\lambda_1 y'^2_1 + \dots + \lambda_k y'^2_k = 2py'_{k+1}.$$

Гиперповерхности с такими уравнениями (в  $(k+1)$ -мерном пространстве) носят название *параболоидов*, причем *эллиптических*, если все  $\lambda_1, \dots, \lambda_k$  одного знака, и *гиперболических*, если среди  $\lambda_1, \dots, \lambda_k$  имеются числа противоположных знаков. Гиперболические параболоиды классифицируются по максимальному числу собственных значений  $\lambda_1, \dots, \lambda_k$  одного знака.

## § 7. Линейные отображения унитарного пространства в унитарное

**1. Сопряженные отображения.** Пусть  $S$  и  $T$  — два унитарных пространства и  $\mathcal{A}$  — линейное отображение  $S$  в  $T$ . Сопряженным с  $\mathcal{A}$  отображением  $\mathcal{A}^*$  называется отображение  $T$  в  $S$ , обладающее свойством  $(\mathcal{A}x, y) = (x, \mathcal{A}^*y)$  при любых  $x \in S$  и  $y \in T$ . Выберем в пространствах  $S$  и  $T$  ортонормальные базисы. Пусть  $A$  — матрица оператора  $\mathcal{A}$  по отношению к этим базисам. Записав скалярные произведения  $(\mathcal{A}x, y)$  через координаты векторов  $x$  и  $y$  и сделав такие же преобразования, как в аналогичной ситуации для оператора из  $S$  в  $S$ , легко получим, что поставленному требованию удовлетворяет оператор, матрица которого сопряжена (т. е. транспонирована к комплексно сопряженной) с матрицей  $A$ . Единственность сопряженного оператора и, тем самым, независимость от выбора базисов доказывается так же, как для операторов из  $S$  в  $S$ . Именно, если  $(\mathcal{A}x, y) = (x, \mathcal{A}^*y)$  и  $(\mathcal{A}x, y) = (x, \mathcal{B}y)$  при любых  $x \in S$ ,  $y \in T$ , то  $(x, (\mathcal{A}^* - \mathcal{B})y) = 0$  при всех  $x \in S$ , следовательно,  $(\mathcal{A}^* - \mathcal{B})y = 0$  при всех  $y \in T$ , а это и означает, что  $\mathcal{B} = \mathcal{A}^*$ .

Для операции сопряжения верны свойства:

$$1. (\mathcal{A}^*)^* = \mathcal{A}. \quad 2. (\mathcal{A}_1 + \mathcal{A}_2)^* = \mathcal{A}_1^* + \mathcal{A}_2^*. \quad 3. (c\mathcal{A})^* = \bar{c}\mathcal{A}^*.$$

4. Если  $\mathcal{A}$  отображает  $S_1$  в  $S_2$  и  $\mathcal{B}$  отображает  $S_2$  в  $S_3$ , то для  $\mathcal{B}\mathcal{A}$ , отображающего  $S_1$  в  $S_3$ , верно  $(\mathcal{B}\mathcal{A})^* = \mathcal{A}^*\mathcal{B}^*$ .

Доказательства ничем не отличаются от доказательств аналогичных свойств в ситуации операторов из  $S$  в  $S$ .

**Предложение 1.** Образ оператора  $\mathcal{A}$  есть ортогональное дополнение к ядру оператора  $\mathcal{A}^*$ .

Действительно, если  $y \in \ker \mathcal{A}^*$ , то при любом  $x = \mathcal{A}z \in \mathcal{A}S$  будет  $(x, y) = (\mathcal{A}z, y) = (z, \mathcal{A}^*y) = 0$ . Обратно, если  $y$  ортогонален всем векторам  $\mathcal{A}z$  из  $\mathcal{A}S$ , то  $(\mathcal{A}z, y) = (z, \mathcal{A}^*y) = 0$  при всех  $z \in S$ , следовательно,  $\mathcal{A}^*y = 0$ . Предложение доказано.

В силу симметрии  $\mathcal{A}$  и  $\mathcal{A}^*$  по отношению операции сопряжения, из предложения 1 следует

**Предложение 2.** Образ оператора  $\mathcal{A}^*$  есть ортогональное дополнение к ядру оператора  $\mathcal{A}$ .

**2. Каноническая форма матрицы линейного отображения унитарного пространства в унитарное.** Пусть  $\mathcal{A}$  — линейное отображение унитарного пространства  $S$  в унитарное пространство  $T$  и  $\mathcal{A}^*$  — сопряженное отображение. Рассмотрим оператор  $\mathcal{A}^*\mathcal{A}$ , отображающий  $S$  в  $S$ . Он самосопряжен, ибо  $(\mathcal{A}^*\mathcal{A})^* = \mathcal{A}^*\mathcal{A}^{**} = \mathcal{A}^*\mathcal{A}$ . Далее,  $\ker \mathcal{A}^*\mathcal{A} = \ker \mathcal{A}$ . Действительно, если  $\mathcal{A}^*\mathcal{A}x = 0$  при  $x \in S$ , то  $(\mathcal{A}^*\mathcal{A}x, x) = (\mathcal{A}x, \mathcal{A}x) = 0$ , откуда  $\mathcal{A}x = 0$ . Таким образом,  $\ker \mathcal{A}^*\mathcal{A} \subseteq \ker \mathcal{A}$ . Обратное включение тривиально.

Пусть  $P = \ker \mathcal{A}$ ,  $S_0 = P^\perp = \mathcal{A}^*T$ ,  $T_0 = \mathcal{A}S$  и  $Q = T_0^\perp = \ker \mathcal{A}^*$ . Так как  $S = S_0 \oplus P$ , то  $T_0 = \mathcal{A}S = \mathcal{A}S_0 + \mathcal{A}P = \mathcal{A}S_0$ . Таким образом,  $\mathcal{A}$  отображает  $S_0$  на все  $T_0$ . Аналогично,  $\mathcal{A}^*$  отображает

$T_0$  на все  $S_0$ . Очевидно, что ядро  $\mathcal{A}$  на  $S_0$  состоит только из нулевого вектора, и то же имеет место для оператора  $\mathcal{A}^*$  на  $T_0$ .

Оператор  $\mathcal{A}^*\mathcal{A}$  на  $S_0$  не только самосопряжен, но и положительно определен. Действительно, при  $x \in S_0$  и  $x \neq 0$  имеет место  $(\mathcal{A}^*\mathcal{A}x, x) = (\mathcal{A}x, \mathcal{A}x) > 0$ , ибо при  $x \neq 0$  и  $\mathcal{A}x \neq 0$ .

Положим  $\dim S = n$ ,  $\dim T = m$  и  $\dim S_0 = \dim T_0 = k$ . В  $S_0$  найдем ортонормированный базис  $u_1, \dots, u_k$  из собственных векторов оператора  $\mathcal{A}^*\mathcal{A}$ . Тогда  $\mathcal{A}^*\mathcal{A}u_i = \lambda_i u_i$ , причем  $\lambda_i > 0$ . Положим  $\lambda_i = \mu_i^2$ . Векторы  $\mathcal{A}u_i$  попарно ортогональны. Действительно,  $(\mathcal{A}u_i, \mathcal{A}u_j) = (u_i, \mathcal{A}^*\mathcal{A}u_j) = (u_i, \mu_j^2 u_j) = \mu_j^2 (u_i, u_j) = 0$ .

Положим  $v_i = \mu_i^{-1} \mathcal{A}u_i$ . Векторы  $v_i$  не только ортогональны, но и нормированны, ибо  $(v_i, v_i) = \mu_i^{-2} (\mathcal{A}u_i, \mathcal{A}u_i) = \mu_i^{-2} (\mathcal{A}^*\mathcal{A}u_i, u_i) = (u_i, u_i) = 1$ . Таким образом, векторы  $v_1, \dots, v_k$  образуют базис  $T_0$ . Ясно, что  $\mathcal{A}u_i = \mu_i v_i$ .

Пусть  $u_{k+1}, \dots, u_n$  — ортонормальный базис  $P$ ,  $v_{k+1}, \dots, v_m$  — ортонормальный базис  $Q$ . Тогда совокупности векторов  $u_1, \dots, u_k, u_{k+1}, \dots, u_n$  и  $v_1, \dots, v_k, v_{k+1}, \dots, v_m$  образуют ортонормальные базисы пространств  $S$  и  $T$ . По отношению к этим базисам оператор  $\mathcal{A}$  имеет следующую матрицу:

$$M = \begin{pmatrix} \mu_1 & 0 & \dots & 0 \\ 0 & \mu_2 & \dots & 0 \\ & & & 0_{k, n-k} \\ 0 & 0 & \dots & \mu_k \\ & 0_{m-k, k} & & 0_{m-k, n-k} \end{pmatrix}.$$

Числа  $\mu_1, \dots, \mu_k$  носят название *главных* или *сингулярных* значений оператора  $\mathcal{A}$ .

На языке матриц полученный результат можно сформулировать следующим образом.

Для любой комплексной  $m \times n$ -матрицы  $A$  существуют унитарные матрицы  $B$  и  $C$  такие, что  $B^*AC$  есть матрица вида  $M$ , причем  $k$  равно рангу матрицы.

Действительно, любая комплексная  $m \times n$ -матрица может рассматриваться как матрица линейного отображения  $n$ -мерного унитарного пространства  $S$  в  $m$ -мерное унитарное пространство  $T$  по отношению к некоторым ортонормальным базисам. Матрицы  $C$  и  $B$  преобразования координат от исходных базисов к базисам  $u_1, \dots, u_n$  и  $v_1, \dots, v_m$  унитарны. В силу формулы преобразования матрицы линейного отображения при преобразованиях координат, в новом базисе матрица вида  $M$  выражается посредством формулы  $B^{-1}AC = B^*AC$ . Число  $k = \dim T_0 = \dim \mathcal{A}S$  равно рангу матрицы  $A$ .

**3. Обобщенный обратный оператор.** Пусть  $\mathcal{A}$  — оператор, отображающий  $n$ -мерное унитарное пространство  $S$  в  $m$ -мерное

унитарное пространство  $T$ . Пусть  $S_0$ ,  $P$ ,  $T_0$  и  $Q$  — те же пространства, что и в п. 2. Полуобратный оператор, построенный исходя из разложений  $S = S_0 \oplus P$  и  $T = T_0 \oplus Q$ , называется *обобщенным обратным* и обозначается через  $\mathcal{A}^+$ . В этой ситуации операторы  $\mathcal{A}^+ \mathcal{A}$  и  $\mathcal{A} \mathcal{A}^+$  будут операторами ортогонального проектирования, т. е. будут самосопряжены.

Легко видеть, что если оператор  $\mathcal{B}$ , действующий из  $T$  в  $S$ , удовлетворяет условиям  $\mathcal{A} \mathcal{B} \mathcal{A} = \mathcal{A}$ ,  $\mathcal{B} \mathcal{A} \mathcal{B} = \mathcal{B}$ ,  $\mathcal{B} \mathcal{A}$  и  $\mathcal{A} \mathcal{B}$  самосопряжены, то  $\mathcal{B} = \mathcal{A}^+$ . Действительно, первые два условия показывают, что  $\mathcal{B}$  есть полуобратный оператор для некоторых разложений  $S = S_0 \oplus \ker \mathcal{A}$ ,  $T = \mathcal{A} S \oplus Q$ , оператор  $\mathcal{B} \mathcal{A}$  проектирует  $S$  на  $S_0$  параллельно  $\ker \mathcal{A}$ , а оператор  $\mathcal{A} \mathcal{B}$  проектирует  $T$  на  $T_0 = \mathcal{A} S$ . Из самосопряженности операторов  $\mathcal{A} \mathcal{B}$  и  $\mathcal{B} \mathcal{A}$  следует, что оба проектирования ортогональны, т. е.  $S_0 = (\ker \mathcal{A})^\perp$  и  $Q = (\mathcal{A} S)^\perp$ . Поэтому  $\mathcal{B} = \mathcal{A}^+$ .

Если ортонормальные базисы в  $S$  и  $T$  выбраны так, что  $m \times n$ -матрица оператора  $\mathcal{A}$  равна

$$\begin{pmatrix} \mu_1 & 0 & \dots & 0 \\ 0 & \mu_2 & \dots & 0 \\ & & & 0_{k, n-k} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \mu_k \\ & 0_{m-k, k} & & 0_{m-k, n-k} \end{pmatrix},$$

то, очевидно,  $\mathcal{A}^+$  будет иметь  $n \times m$ -матрицу такого же вида, только вместо  $\mu_1, \mu_2, \dots, \mu_k$  будут  $\mu_1^{-1}, \mu_2^{-1}, \dots, \mu_k^{-1}$ .

Понятие обобщенного обратного оператора естественно переносится на матрицы, так как каждую матрицу можно рассматривать как матрицу оператора по отношению к ортонормальным базисам.

Для вычисления матрицы  $A^+$ , обобщенной обратной для  $m \times n$ -матрицы  $A$  ранга  $k$ , можно, например, поступить так. Представить  $A$  в виде произведения  $BC$   $m \times k$ -матрицы  $B$  ранга  $k$  на  $k \times n$ -матрицу  $C$  ранга  $k$ . Тогда матрицы  $B^* B$  и  $CC^*$  самосопряжены и невырождены. Легко проверить, что  $A^+ = C^* (CC^*)^{-1} (B^* B)^{-1} B^*$ . Для этого нужно убедиться в выполнении равенств  $AA^+ A = A$ ,  $A^+ AA^+ = A^+$  и в самосопряженности  $A^+ A$  и  $AA^+$ , что не представляет труда.

**4. Роль обобщенного обратного оператора в теории систем линейных уравнений.** Сначала введем одно важное понятие. Пусть в унитарном пространстве  $S$  даны подпространство  $P$  и вектор  $z$ . *Расстоянием от вектора  $z$  до подпространства  $P$*  называется минимум длин векторов  $z - u$  при  $u \in P$ . Пусть  $z = x + y$  при  $x \in P$ ,  $y \in P^\perp$ . Тогда  $|z - u|^2 = (x - u + y, x - u + y) = (x - u, x - u) + (y, y)$ , ибо векторы  $x - u$  и  $y$  ортогональны. Ясно, что минимум реализуется при  $u = x$  и равен  $(y, y) = |y|^2$ . Таким образом, расстояние от  $z$  до  $P$  равно длине ортогональной проекции

вектора  $z$  на  $P^\perp$  и реализуется на векторе  $x$ , являющемся ортогональной проекцией  $z$  на  $P$ .

Обратимся теперь к системе линейных уравнений. Систему  $m$  линейных уравнений с  $n$  неизвестными в векторно-операторной форме можно рассматривать как задачу определения вектора  $x$  из уравнения  $\mathcal{A}x = f$ , где  $\mathcal{A}$  — оператор из  $n$ -мерного пространства  $S$  в  $m$ -мерное пространство  $T$ , а  $f$  — данный вектор в  $T$ . Для систем с комплексными коэффициентами (в частности, с вещественными) пространства  $S$  и  $T$  можно рассматривать как унитарные пространства с данными ортонормальными базисами. Вектора  $x$ , удовлетворяющего уравнению  $\mathcal{A}x = f$ , может не существовать. Для любого вектора  $x \in S$  вектор  $f - \mathcal{A}x \in T$  называется вектором невязки. *Обобщенным решением* или *решением в смысле наименьших квадратов* называется вектор  $x_0$ , при котором вектор невязки имеет минимальную длину. Векторы  $x$ , отличающиеся на слагаемые из ядра  $\mathcal{A}$ , дают один и тот же вектор невязки. Среди них имеется кратчайший. Он называется *нормальным обобщенным решением*.

Покажем, что вектор  $\mathcal{A}^+f$  дает нормальное обобщенное решение уравнения  $\mathcal{A}x = f$ . Действительно,  $\mathcal{A}\mathcal{A}^+f$  есть ортогональная проекция вектора  $f$  на  $T_0 = \mathcal{A}S$ . Поэтому на этом векторе невязка имеет минимальную длину. Далее,  $\mathcal{A}^+f \in S_0 = (\ker \mathcal{A})^\perp$ . Поэтому длина любого вектора  $\mathcal{A}^+f + y$  при  $y \in \ker \mathcal{A}$ , квадрат которой равен  $|\mathcal{A}^+f|^2 + |y|^2$ , имеет минимум при  $y = 0$ .

**5. Линейное отображение евклидова пространства в евклидово.** Теория линейных отображений евклидова пространства в евклидово ничем не отличается от теории отображений унитарных пространств с заменой унитарных преобразований координат на ортогональные. Имеет место такая же каноническая форма, существует обобщенный обратный оператор, играющий такую же роль, как в комплексном случае, для систем линейных уравнений с вещественными коэффициентами.

## § 8. Объем параллелепипеда в евклидовом пространстве

**1. Квадрат объема в общем случае.** Параллелепипедом, натянутым на  $m$  линейно независимых векторов  $v_1, v_2, \dots, v_m$  в  $n$ -мерном евклидовом пространстве, называется множество векторов  $t_1v_1 + t_2v_2 + \dots + t_mv_m$  при  $t_i$ , независимо изменяющимися на отрезке  $[0, 1]$ . Назовем  $(m-1)$ -мерный параллелепипед, натянутый на векторы  $v_1, v_2, \dots, v_{m-1}$ , основанием параллелепипеда, а расстояние от вектора  $v_m$  до подпространства, натянутого на  $v_1, v_2, \dots, v_{m-1}$ , — высотой параллелепипеда.

«Объемом» одномерного параллелепипеда  $\{tv_1\}$  называется длина вектора  $v_1$ . Для больших размерностей объем определяется индуктивно, как объем основания, умноженный на высоту.

**Теорема 1.** *Квадрат объема параллелепипеда равен определителю Грама  $G = \begin{vmatrix} (v_1, v_1) & \dots & (v_1, v_{m-1}) & (v_1, v_m) \\ \dots & \dots & \dots & \dots \\ (v_m, v_1) & \dots & (v_m, v_{m-1}) & (v_m, v_m) \end{vmatrix}$  совокупности векторов  $v_1, \dots, v_{m-1}, v_m$ .*

Доказательство проведем индукцией по числу  $m$  векторов. Для  $m = 1$  это верно, ибо  $|v_1|^2 = (v_1, v_1)$ . Допустим, что это верно для совокупности из  $m - 1$  векторов.

Пусть  $y$  — ортогональная проекция вектора  $v_m$  на ортогональное дополнение к подпространству  $P$ , натянутому на  $v_1, \dots, v_{m-1}$ . Эта проекция осуществляется параллельно подпространству  $P$ , так что  $y = v_m + a_1 v_1 + \dots + a_{m-1} v_{m-1}$  при некоторых  $a_1, \dots, a_{m-1}$ , и  $y$  ортогонален к векторам  $v_1, \dots, v_{m-1}$ .

Прибавим к последнему столбцу определителя  $G$  предшествующие, умноженные на  $a_1, \dots, a_{m-1}$ . В силу линейности скалярного произведения по второму аргументу, мы получим в последнем столбце числа  $(v_1, y), \dots, (v_{m-1}, y), (v_m, y)$ , из которых первые  $m - 1$  равны нулю. Последний элемент  $(v_m, y)$  последнего столбца равен  $(y - a_1 v_1 - \dots - a_{m-1} v_{m-1}, y) = (y, y) = |y|^2$ .

Длина вектора  $y$  равна высоте параллелепипеда, согласно определению расстояния от вектора до подпространства. Таким образом,  $G = |y|^2 \begin{vmatrix} (v_1, v_1) & \dots & (v_1, v_{m-1}) \\ \dots & \dots & \dots \\ (v_{m-1}, v_1) & \dots & (v_{m-1}, v_{m-1}) \end{vmatrix}$ . Последний определитель,

согласно индуктивному предположению, есть квадрат объема основания. Следовательно,  $G$  равен квадрату объема рассматриваемого параллелепипеда, что и требовалось доказать.

**2. Объем  $n$ -мерного параллелепипеда в  $n$ -мерном евклидовом пространстве.** Пусть  $v_1, v_2, \dots, v_n$  — линейно независимая совокупность векторов в  $n$ -мерном пространстве, и пусть матрица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{12} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

имеет своими столбцами координаты векторов  $v_1, v_2, \dots, v_n$  относительно некоторого ортонормального базиса  $e_1, e_2, \dots, e_n$ . Тогда элемент  $g_{ij}$  матрицы  $G = A^T A$  равен  $a_{1i} a_{1j} + a_{2i} a_{2j} + \dots + a_{ni} a_{nj} = (v_i, v_j)$ , т. е. матрица  $G = A^T A$  есть матрица Грама для совокупности векторов  $v_1, v_2, \dots, v_n$ . Имеем  $\det G = \det A^T A = (\det A)^2$ .

Таким образом, квадрат объема параллелепипеда равен квадрату определителя матрицы  $A$  и, следовательно, объем параллелепипеда равен абсолютной величине  $\det A$ .

Вскроем геометрический смысл знака определителя матрицы  $A$ . Скажем, что совокупность векторов  $v_1, v_2, \dots, v_n$  ориентирована так же, как базис  $e_1, e_2, \dots, e_n$ , если  $\det A > 0$ , и ориентирована противоположным образом, если  $\det A < 0$ .

Скажем, что базис  $v_1, v_2, \dots, v_n$  получается непрерывной деформацией из базиса  $e_1, e_2, \dots, e_n$ , если существует матрица  $A(t)$ , элементы которой непрерывно зависят от параметра  $t$ , меняющегося на отрезке  $[0, 1]$ , такая, что  $A(0) = E$  и  $A(1) = A$ , где  $A$  — матрица из координат векторов  $v_1, v_2, \dots, v_n$ , причем  $\det A(t) \neq 0$  при всех значениях  $t$ .

Покажем, что если базис  $v_1, v_2, \dots, v_n$  имеет одинаковую ориентацию с базисом  $e_1, e_2, \dots, e_n$ , то существует непрерывная деформация, переводящая  $e_1, e_2, \dots, e_n$  в  $v_1, v_2, \dots, v_n$ . С этой целью представим невырожденную матрицу  $A$  в виде произведения  $BH$  положительно определенной матрицы  $B$  на ортогональную матрицу  $H$ . Далее, матрицу  $B$  представим в виде  $C_1^{-1}DC_1$ , где  $D$  — диагональная матрица из положительных собственных значений  $\lambda_1, \lambda_2, \dots, \lambda_n$  матрицы  $B$ . Пусть  $D(t)$  — диагональная матрица, составленная из элементов  $e^{t \ln \lambda_k}$ ,  $k = 1, 2, \dots, n$ . Тогда  $D(0) = E$ ,  $D(1) = D$  и элементы  $D(t)$  меняются непрерывно. При этом  $\det D(t) = (\det D)^t \neq 0$ . Положим  $B(t) = C_1^{-1}D(t)C_1$ .

Матрица  $H$  собственно ортогональна, ибо  $\det A > 0$  и  $\det B > 0$ . Поэтому  $H$  допускает представление  $H = C_2^{-1}FC_2$ , где  $C_2$  — ортогональная матрица, а  $F$  — блочно-диагональная, составленная из 1 и блоков второго порядка вида  $\begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix}$  (включая «блоки» с  $\varphi = \pi$ ). Пусть  $F(t)$  — блочно-диагональная матрица, в которой каждый блок второго порядка  $\begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix}$  заменен на блок  $\begin{pmatrix} \cos t\varphi & \sin t\varphi \\ -\sin t\varphi & \cos t\varphi \end{pmatrix}$ . Матрица  $F(t)$  непрерывно зависит от  $t$  и при всех значениях  $t$  собственно ортогональна. Очевидно, что  $F(0) = E$  и  $F(1) = F$ . Положим  $H(t) = C_2^{-1}F(t)C_2$ . Ясно, что  $H(t)$  непрерывно зависит от  $t$ , собственно ортогональна при всех значениях  $t$ ,  $H(0) = E$  и  $H(1) = H$ .

Наконец, положим  $A(t) = B(t)H(t)$ . Матрица  $A(t)$  непрерывна при  $0 \leq t \leq 1$ ,  $\det A(t) = \det B(t) \neq 0$ ,  $A(0) = E$  и  $A(1) = A$ . Искомая деформация получена.

Если же ориентация  $v_1, v_2, \dots, v_n$  противоположна ориентации  $e_1, e_2, \dots, e_n$ , то непрерывной деформации базиса  $e_1, e_2, \dots, e_n$  в  $v_1, v_2, \dots, v_n$  не существует. Действительно, если матрица  $A(t)$  непрерывна при  $0 \leq t \leq 1$ ,  $A(0) = E$  и  $A(1) = A$ , причем  $\det A < 0$ , то  $\det A(t)$ , будучи непрерывной функцией от  $t$ , должен перейти от положительного значения  $\det A(0) = 1$  к отрицательному  $\det A(1) = \det A < 0$ , что возможно, только если при некотором значении  $t_0$ ,  $0 < t_0 < 1$ ,  $\det A(t_0) = 0$ , т. е. векторы  $v_1(t_0), v_2(t_0), \dots, v_n(t_0)$  с матрицей из координат, равной  $A(t_0)$ , линейно зависимы и не составляют базиса.

## ЭЛЕМЕНТЫ АЛГЕБРЫ ТЕНЗОРОВ

## § 1. Основные понятия

**1. Определение тензора.** Тензоры представляют собой многокомпонентные системы, элементы которых занумерованы двумя системами индексов — несколькими верхними и несколькими нижними, каждый из которых пробегает значения от 1 до  $n$ . Число нижних индексов называется *валентностью ковариантности*, число верхних — *валентностью контравариантности*, их сумма — *полной валентностью*.

Тензоры, у которых отсутствуют верхние индексы, называются *чисто ковариантными*, у которых отсутствуют нижние — *чисто контравариантными*. Если присутствуют те и другие, тензор называется *смешанным*. Так, компоненты трижды ковариантного и дважды контравариантного тензора имеют вид  $a_{ijk}^{pq}$ . Тензоры считаются связанными с  $n$ -мерным векторным пространством, в котором выбран базис, таким образом, что компоненты тензора при фиксированных индексах, кроме одного верхнего, образуют координаты вектора в выбранном базисе, компоненты же при фиксированных индексах, кроме одного нижнего, образуют координаты ковектора в дуальном базисе. При замене базиса компоненты тензора изменяются в соответствии с приведенным истолкованием индексов, нумерующих компоненты тензора.

В соответствии с данным определением набор координат вектора следует рассматривать как контравариантный тензор валентности 1 и нумеровать их следует верхними индексами.

В матрице преобразования координат элементы каждого столбца являются координатами векторов, именно, векторов нового базиса относительно исходного. Поэтому строки матрицы преобразования координат следует нумеровать верхними индексами. Элементы же каждой строки можно рассматривать как координаты ковекторов, т. е. линейных функций, посредством которых исходные координаты векторов выражаются через новые, и нумеровать их нижними индексами. При таких обозначениях матрица преобразования координат имеет вид  $(c_i^j)$ . Выражения исходных координат через новые имеют вид

$$x^j = \sum_i c_i^j x'^i,$$

а выражения новых координат через исходные имеют вид  $x'^i = \sum_k \gamma_k^i x^k$ , где  $(\gamma_k^i)$  — матрица, обратная к  $(c_i^j)$ . То, что эти две матрицы взаимно обратны, можно записать в форме  $\sum_i \gamma_k^i c_i^j = \delta_k^j$ .

Здесь  $\delta_k^j$  — символ Кронекера, т. е.  $\delta_k^j = 0$  при  $k \neq j$  и  $\delta_k^k = 1$ ,  $(\delta_k^j)$  — единичная матрица. Ввиду того, что обратная матрица является не только левой обратной, но и правой, верно, что

$$\sum_j c_i^j \gamma_j^k = \delta_i^k.$$

При транспонировании матрицы нужно поменять ролями верхние и нижние индексы. Напомним, что матрица преобразования координат транспонирована с матрицей замены базиса, так что формулы замены базиса имеют вид

$$e'_i = \sum_j c_j^i e_j$$

(суммирование по верхнему индексу матрицы  $(c_i^j)$ , а не по нижнему).

Напомним еще, что при преобразовании координат коэффициенты линейной функции  $l_1 x^1 + \dots + l_n x^n$ , т. е. координаты  $l_1, \dots, l_n$  соответствующего ковектора, преобразуются по формулам

$$l'_i = \sum_j c_j^i l_j,$$

т. е. совершенно по тем же формулам, что формулы замены базиса. Это и дает основание считать набор координат ковектора ковариантным тензором.

В соответствии с данным выше определением тензора и формулами преобразования координат вектора и ковектора мы приходим к следующему правилу преобразования компонент тензора при преобразовании координат:

$$a'^{pq}_{ijk} = \sum a^{\sigma\tau}_{\lambda\mu\nu} c_i^\lambda c_j^\mu c_k^\nu \gamma_\sigma^p \gamma_\tau^q.$$

Здесь суммирование производится по индексам  $\lambda, \mu, \nu, \sigma, \tau$ , меняющимся от 1 до  $n$ .

Это правило изменения компонент при преобразовании координат может рассматриваться и как определение тензора.

**2. Сокращенные тензорные обозначения.** В формулах преобразования компонент тензора при преобразовании координат, в частности, наборов координат вектора и ковектора, происходит суммирование при изменении некоторых индексов в одних и тех же пределах — от 1 до  $n$ , причем во всех рассмотренных в п. 1 ситуациях индекс, по которому осуществляется суммирование, входит два раза — как нижний и как верхний. Эти обстоятельства делают

излишним указание пределов для индекса суммирования и, более того, само употребление знака  $\sum$  становится не необходимым, если условиться считать, что как только в выражении встречается одинаковое обозначение для некоторых нижнего и верхнего индекса, то по этому индексу осуществляется суммирование. Так, формула преобразования компонент тензора записывается без знака  $\sum$  в виде  $a'^{pq}_{ijk} = a^{\sigma\tau}_{\lambda\mu\nu} c^{\lambda}_i c^{\mu}_j c^{\nu}_k \gamma^p_{\sigma} \gamma^q_{\tau}$ . Действительно, здесь каждый из индексов  $\lambda, \mu, \nu, \sigma, \tau$  встречается как верхний и как нижний и, следовательно, по всем этим индексам производится суммирование.

Соответственно, формулы преобразования координат для координат вектора и коковектора записываются в виде  $x'^i = \gamma^i_{\alpha} x^{\alpha}$ ,  $l'_i = c^{\alpha}_i l_{\alpha}$ . Значение коковектора (линейной функции) с координатами  $l_i$  на векторе с координатами  $x^j$  записывается в виде  $l_i x^i$ . Элементы  $f^i_j$  произведения матриц  $A = (a^i_j)$  и  $B = (b^j_i)$  запишутся в виде  $f^i_j = a^i_k b^k_j$ .

Эти сокращенные обозначения оказываются удобными иногда и за пределами алгебры.

**3. Примеры тензоров.** Примеры контравариантного и ковариантного тензоров валентности 1 мы уже видели — это наборы координат вектора в некотором базисе и, соответственно, коковектора в дуальном базисе.

В качестве следующего примера рассмотрим матрицу коэффициентов линейного оператора. Она может рассматриваться как тензор, один раз контравариантный и один раз ковариантный. Действительно, строки матрицы следует занумеровать верхними индексами, столбцы — нижними. Равенство  $y = Ax$  запишется в виде  $y^i = a^i_j x^j$ . Матричная форма записи матрицы оператора при преобразовании координат  $A \rightarrow C^{-1}AC$  совпадает с тензорной записью  $a'^i_j = a^k_m \gamma^i_k c^m_j$ . Суммирование по  $m$  соответствует умножению справа на матрицу преобразования координат, суммирование по  $k$  соответствует умножению слева на обратную матрицу.

В частности, символ Кронекера, связанный с единичным оператором, является тензором, однократно ковариантным и контравариантным. Матрица коэффициентов квадратичной формы, рассматриваемой как функция от координат вектора, есть дважды ковариантный тензор. Действительно, сама квадратичная форма есть  $a_{ij} x^i x^j$ . При преобразовании координат  $x^i$  заменяются на  $c^i_k x'^k$ , значение формы превратится в  $a_{ij} c^i_k c^j_m x'^k x'^m$ , т. е. ее коэффициенты превращаются в  $a_{ij} c^i_k c^j_m = a'_{km}$ , преобразуясь по правилу преобразования дважды ковариантного тензора. Суммирование по  $j$  равносильно умножению матрицы формы справа на матрицу преобразования, суммирование по  $i$  можно рассматривать как умножение слева на матрицу, транспонированную с матрицей

преобразования координат, в полном совпадении с формулой преобразования  $A \rightarrow C^T A C$ . Тензор коэффициентов квадратичной формы обладает свойством симметрии  $a_{ij} = a_{ji}$ , которое, разумеется, сохраняется при преобразовании координат.

*Полилинейной функцией* от нескольких векторов называется функция, линейная относительно каждого вектора. Рассмотрим полилинейную функцию от трех векторов одного и того же  $n$ -мерного пространства и двух ковекторов. В координатной записи она имеет вид  $a_{ijk}^{pq} x^i x^j x^k y_p y_q$ . Здесь  $x^i$  — координаты векторов,  $y_s$  — координаты ковекторов в дуальном базисе. Набор коэффициентов  $a_{ijk}^{pq}$  является тензором, трижды ковариантным и дважды контравариантным.

В следующей главе мы познакомимся с некоторым один раз контравариантным и два раза ковариантным тензором, естественно возникающим в пределах самой алгебры. Тензоры более высоких валентностей играют существенную роль в геометрии римановых пространств и в теоретической физике.

## § 2. Действия над тензорами

**1. Сложение и умножение на число.** Суммой двух тензоров одинакового типа называется тензор, компоненты которого равны суммам соответствующих компонент слагаемых:

$$(a + b)_{ijk}^{pq} = a_{ijk}^{pq} + b_{ijk}^{pq}.$$

То, что сумма тензоров действительно является тензором, ясно из формулы преобразования компонент при замене базиса.

Произведением числа  $\alpha$  на тензор называется тензор, полученный из исходного умножением всех компонент на  $\alpha$ :

$$(\alpha a)_{ijk}^{pq} = \alpha a_{ijk}^{pq}.$$

Из этих определений ясно, что тензоры одинакового типа составляют векторное пространство, размерность которого равна степени  $n$  с показателем, равным полной валентности.

**2. Умножение тензоров.** Произведением тензоров  $a_{ijk}^{pq}$  и  $b_{\alpha\beta}^{\lambda}$  называется система чисел  $d_{ijk\alpha\beta}^{pq\lambda} = a_{ijk}^{pq} b_{\alpha\beta}^{\lambda}$  в предположении, что все индексы независимо принимают допустимые значения. Легко видеть, что произведение тензоров есть тензор. Действительно, при замене базиса  $e'_m = c_m^\nu e_\nu$  компоненты преобразуются по формуле

$$d_{fgh\eta\theta}^{rs\kappa} = a_{ijk}^{pq} c_f^i c_g^j c_h^k c_\eta^r c_\theta^s c_\lambda^\kappa b_{\alpha\beta}^{\lambda} c_\alpha^a c_\beta^b c_\eta^c c_\theta^d c_\lambda^e = d_{ijk\alpha\beta}^{pq\lambda} c_f^i c_g^j c_h^k c_\eta^r c_\theta^s c_\lambda^\kappa c_\alpha^a c_\beta^b c_\eta^c c_\theta^d c_\lambda^e,$$

т. е. по формуле изменения компонент тензора пятикратно ковариантного и трехкратно контравариантного. При умножении тензоров их валентности складываются.

Аналогично определяется произведение любого числа тензоров.

Тензор называется *разложимым*, если его можно представить в виде произведения тензоров валентности 1.

**Предложение 1.** *Любой тензор можно представить в виде линейной комбинации разложимых тензоров.*

**Доказательство.** Зафиксируем базис пространства  $e_1, \dots, e_n$  и рассмотрим векторы  $e_i$  и ковекторы  $f^j$ , составляющие дуальный базис. Их координаты равны нулю, кроме одной, равной единице. Тензор, равный произведению тензоров из координат этих векторов и ковекторов, имеет единственную компоненту, равную 1, и остальные нули, причем 1 можно получить в любом месте тензора. Следовательно, любой тензор является их линейной комбинацией.

Наименьшее число разложимых тензоров, линейной комбинацией которых является данный тензор, называется его *рангом*. Легко видеть, что тензор полной валентности 2 имеет ранг, равный рангу соответствующей матрицы. Вопрос об определении ранга полной валентности 3 и выше еще не получил алгоритмического решения в общем виде, и возможно, что даже вопрос о существовании алгоритма не является бесспорным.

**3. Свертка.** Пусть имеется тензор  $a_{ijk}^{pq}$ , имеющий как верхние, так и нижние индексы. Приравнивая один верхний индекс к одному нижнему, мы должны, по соглашению об обозначениях, просуммировать по этому индексу, и в результате получится система элементов, в верхних и нижних номерах которых останется на одну единицу меньше, так что можно положить  $b_{ij}^p = a_{ijk}^{pk}$ . Эта операция называется *сверткой* тензора.

**Предложение 2.** *Свертка произведения тензора на символ Кронекера, как по верхнему, так и по нижнему индексу этого символа, не меняет тензор по существу и сводится только к переименованию индекса.*

Действительно, сумма  $a_{ijk}^{pq} \delta_q^s$  имеет лишь одно слагаемое, отличное от нуля, именно то, для которого значение символа Кронекера равно 1, т. е. при  $q = s$ . Поэтому  $a_{ijk}^{pq} \delta_q^s = a_{ijk}^{ps}$ . Аналогично,  $a_{ijk}^{pq} \delta_s^k = a_{ijs}^{pq}$ .

**Предложение 3.** *Результатом свертки тензора является тензор.*

**Доказательство.** Пусть дан тензор  $a_{ijk}^{pq}$ . Обозначим  $a_{ijk}^{pk}$  через  $b_{ij}^p$ . Пусть  $e'_\alpha = e_\alpha^\beta e_\beta$  — замена базиса. Тогда компоненты тензора  $a_{ijk}^{pq}$  преобразуются по формуле

$$a'_{\lambda\mu\nu}{}^{\sigma\tau} = a_{ijk}^{pq} c_\lambda^i c_\mu^j c_\nu^k c_p^\sigma c_q^\tau.$$

Переход к  $b'_{\lambda\mu}{}^\sigma$  требует положить  $\nu = \tau$  и просуммировать по  $\nu$ . Это дает  $b'_{\lambda\mu}{}^\sigma = a_{ijk}^{pq} c_\lambda^i c_\mu^j c_p^\sigma c_q^\nu$ . Но сумма  $c_\nu^k c_q^\nu$  равна  $\delta_q^k$ , и сумма

$a_{ijk}^{pq} \delta_q^k$  по  $q$  и  $k$  равна сумме  $a_{ijk}^{pk} = b_{ij}^p$ . Итак,

$$b_{\lambda\mu}^{\prime\sigma} = b_{ij}^p c_{\lambda}^i c_{\mu}^j \gamma_p^{\sigma}.$$

Это значит, что  $b_{ij}^p$  действительно есть тензор.

### § 3. Симметричные и антисимметричные тензоры

**1. Применение подстановки к индексам ковариантного тензора.** Пусть  $a_{i_1 i_2 \dots i_m}$  — ковариантный тензор валентности  $m$  и  $\sigma$  — некоторая подстановка чисел  $1, 2, \dots, m$ . Применяв эту подстановку к номерам индексов, мы получим систему чисел, занумерованную  $m$  индексами  $j_1, j_2, \dots, j_m$ , где  $j_1 = i_{1\sigma}, \dots, j_m = i_{m\sigma}$ . Из формул преобразования компонент тензора, которые имеют одинаковый вид для всех индексов, заключаем, что мы снова получим  $m$ -ковариантный тензор. Операцию применения подстановки к номерам индексов можно рассматривать как обобщение операции транспонирования матрицы.

**2. Симметричные тензоры.** Тензор называется *симметричным*, если он не меняется в результате всех подстановок номеров индексов, т. е. если его компоненты не изменяются при всех перестановках индексов.

Примером симметричного ковариантного тензора валентности  $m$  при индексах, меняющихся от 1 до  $n$ , может служить набор коэффициентов формы степени  $m$  от  $n$  переменных, если сомножители в каждом одночлене рассмотреть во всех возможных порядках и коэффициент разделить поровну по всем записям одночлена. Запись такой формы принимает вид

$$a_{i_1 i_2 \dots i_m} x^{(i_1)} x^{(i_2)} \dots x^{(i_m)}$$

(верхние индексы мы ставим в скобки, чтобы не перепутать с показателями степени, которые здесь естественно возникают при равных значениях индексов) с симметричным тензором коэффициентов.

Иногда применяется операция симметризации тензора. Эта операция заключается в том, что производятся все  $m!$  подстановок номеров индексов, результаты складываются и делятся на  $m!$ . В результате операции симметризации получается симметричный тензор.

Нетрудно проследить, что тензор коэффициентов произведения двух форм равен результату симметризации произведения тензоров коэффициентов перемножаемых форм.

Симметризацию тензора иногда применяют по части индексов и применяют ее не только к ковариантным, но и к смешанным тензорам, в последнем случае по всем (или части) нижним индексам и отдельно по всем (или части) верхним индексам.

**3. Антисимметричные тензоры.** Ковариантный тензор  $a_{i_1 i_2 \dots i_m}$  называется *антисимметричным*, если две его компоненты, получающиеся одна из другой переменной местами двух индексов, отличаются только знаком. Ясно, что тогда любая компонента с хотя бы одной парой одинаковых значений индексов равна нулю. Далее, если система индексов получается из другой посредством четной подстановки, то компоненты равны, если же системы индексов связаны нечетной подстановкой, то они отличаются знаком. Полилинейная форма  $F(x_1, \dots, x_m) = a_{i_1 i_2 \dots i_m} x_{i_1}^{i_1} x_{i_2}^{i_2} \dots x_{i_m}^{i_m}$  с антисимметричным тензором коэффициентов антисимметрична, т. е.  $F(x_1, \dots, x_i, \dots, x_j, \dots, x_m) = -F(x_1, \dots, x_j, \dots, x_i, \dots, x_m)$ . Если валентность  $m$  меньше числа  $n$  возможных значений для индексов, то в индексации каждой компоненты встретятся одинаковые значения, так что все компоненты тензора равны нулю.

Интересен случай, когда  $m = n$ . В этом случае ненулевые компоненты будут иметь индексы  $(i_1, i_2, \dots, i_n)$ , среди которых нет равных, т. е. они представляют собой перестановки чисел  $1, 2, \dots, n$ . Если положить  $a_{1, 2, \dots, n} = a$ , то остальные компоненты равны

$$a \cdot (-1)^{\text{inv}(i_1, i_2, \dots, i_n)}.$$

Соответствующая полилинейная форма будет равна

$$a \sum (-1)^{\text{inv}(i_1, i_2, \dots, i_n)} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = a \det \begin{pmatrix} x_1^1 & x_1^2 & \dots & x_1^n \\ x_2^1 & x_2^2 & \dots & x_2^n \\ \dots & \dots & \dots & \dots \\ x_n^1 & x_n^2 & \dots & x_n^n \end{pmatrix}.$$

Подобно симметризации рассматривается антисимметризация, при которой все тензоры, получающиеся при подстановках индексов, складываются со знаками  $+$  или  $-$  в зависимости от четности или нечетности подстановки индексов.

## § 4. Тензорные произведения векторных пространств

**1. Определение тензорного произведения.** Пусть  $S$  и  $T$  — два векторных пространства над полем  $K$ . Рассмотрим пары векторов  $(x, y)$  при  $x \in S$ ,  $y \in T$  и их формальные суммы

$$(x_1, y_1) + (x_2, y_2) + \dots + (x_k, y_k).$$

Введем следующие эквивалентности:

- 1)  $(\alpha x, y) \sim (x, \alpha y)$  при  $\alpha \in K$ ;
- 2)  $(x_1, y) + (x_2, y) \sim (x_1 + x_2, y)$ ;
- 3)  $(x, y_1) + (x, y_2) \sim (x, y_1 + y_2)$ .

Две формальные суммы пар будем считать *эквивалентными*, если от одной к другой можно перейти посредством конечного



Покажем, что эта функция принимает одинаковые значения на эквивалентных суммах пар. Это достаточно проверить для эквивалентностей 1), 2), 3). Получаем

- 1)  $(f_i, h_j)(\alpha x, y) = f_i(\alpha x)h_j(y) = \alpha f_i(x)h_j(y)$ ,  
 $(f_i, h_j)(x, \alpha y) = f_i(x)h_j(\alpha y) = \alpha f_i(x)h_j(y)$ ;
- 2)  $(f_i, h_j)[(x_1, y) + (x_2, y)] = f_i x_1 \cdot h_j y + f_i x_2 \cdot h_j y$ ,  
 $(f_i, h_j)(x_1 + x_2, y) = f_i(x_1 + x_2) \cdot h_j y = f_i x_1 \cdot h_j y + f_i x_2 \cdot h_j y$ .

Проверка для эквивалентности 3) аналогична. Таким образом, функция  $(f_i, h_j)$  определена на классах эквивалентных пар как линейная функция.

Допустим теперь, что имеется зависимость

$$c_{11}(e_1 \otimes g_1) + \dots + c_{1m}(e_1 \otimes g_m) + \dots + c_{n1}(e_n \otimes g_1) + \dots + c_{nm}(e_n \otimes g_m) = 0.$$

Применим к этому равенству функцию  $(f_i, h_j)$ . Ясно, что ее значения на всех произведениях базисных векторов, кроме  $e_i \otimes g_j$ , равны нулю, а значение на  $e_i \otimes g_j$  равно 1. Поэтому  $c_{ij} = 0$  при всех  $i$  и  $j$ . Таким образом, элементы  $e_i \otimes g_j$  составляют базис пространства  $S \otimes T$ , причем размерность этого пространства равна  $mn$ .

**3. Тензорное произведение нескольких пространств.** Тензорное произведение нескольких пространств  $S_1, S_2, \dots, S_k$  вводится аналогично тензорному произведению двух пространств. Рассматриваются наборы компонент  $(x_1, x_2, \dots, x_k)$  при  $x_i \in S_i$  и их формальные суммы. Вводятся действия сложения (формально) и умножения на элементы основного поля, посредством присоединения множителя к первой компоненте. Множество таких формальных сумм становится векторным пространством (бесконечномерным при бесконечном основном поле). Вводятся эквивалентности 1)  $(\alpha x_1, x_2, \dots, x_k) \sim (x_1, \alpha x_2, \dots, x_k) \sim \dots \sim (x_1, x_2, \dots, \alpha x_k)$ ; 2)  $(x_1, \dots, x'_i + x''_i, \dots, x_k) \sim (x_1, \dots, x'_i, \dots, x_k) + (x_1, \dots, x''_i, \dots, x_k)$ . Две формальные суммы рассматриваемых наборов считаются эквивалентными, если от одной из них можно перейти к другой посредством конечного числа эквивалентностей вида 1), 2). Структура векторного пространства формальных сум наборов компонент переносится на множество классов эквивалентности. Получившееся пространство называется *тензорным произведением*  $S_1 \otimes S_2 \otimes \dots \otimes S_k$  пространств  $S_1, S_2, \dots, S_k$ . Класс, содержащий набор  $(x_1, x_2, \dots, x_k)$ , обозначается  $x_1 \otimes x_2 \otimes \dots \otimes x_k$ . Тензорные произведения базисов пространств  $S_1, S_2, \dots, S_k$  составляют базис  $S_1 \otimes S_2 \otimes \dots \otimes S_k$ . Это доказывается аналогично подробно разобранному выше случаю  $k=2$ . Поэтому размерность тензорного произведения пространств равна произведению размерностей этих пространств.

**4. Инвариантное определение тензора.** Сейчас мы дадим определение тензора, отличное от данного в § 1, но, разумеется, тесно

с ним связанное. Пусть дано векторное пространство  $S$  и сопряженное с ним пространство  $S^*$ . Элементы тензорного произведения  $m$  экземпляров  $S$  и  $k$  экземпляров  $S^*$  называются  $m$  раз *контравариантными* и  $k$  раз *ковариантными тензорами*. Если выбран базис  $e_1, e_2, \dots, e_n$  пространства  $S$  и дуальный с ним базис  $f^1, \dots, f^n$  пространства  $S^*$ , то тензоры представляются в виде

$$a_{i_1 \dots i_k}^{j_1 \dots j_m} e_{i_1} \otimes \dots \otimes e_{i_m} \otimes f^{j_1} \otimes \dots \otimes f^{j_m}.$$

Из формул преобразования координат следует, что набор коэффициентов  $a_{i_1 \dots i_k}^{j_1 \dots j_m}$  составляет  $k$  раз ковариантный и  $m$  раз контравариантный тензор в смысле определения, данного в § 1.

Данное здесь определение тензора хорошо своей инвариантностью, в его формулировке никак не участвует выбор базиса пространства. Однако в приложениях тензоров чаще оказывается более удобным определение через компоненты и формулы преобразования.

**5. Действия над тензорами в свете инвариантного определения.** Действия сложения и умножения на скаляры совпадают с одноименными действиями в пространстве тензоров данного типа. Действие умножения тензоров равносильно их тензорному умножению как векторов в своих пространствах. Это с очевидностью следует из представления тензоров через базис:

$$\begin{aligned} & (a_{i_1 \dots i_k}^{j_1 \dots j_m} e_{i_1} \otimes \dots \otimes e_{i_m} \otimes f^{j_1} \otimes \dots \otimes f^{j_m}) \otimes \\ & \quad \otimes (b_{p_1 \dots p_s}^{q_1 \dots q_t} e_{q_1} \otimes \dots \otimes e_{q_t} \otimes f^{p_1} \otimes \dots \otimes f^{p_s}) = \\ & = a_{i_1 \dots i_k}^{j_1 \dots j_m} b_{p_1 \dots p_s}^{q_1 \dots q_t} e_{i_1} \otimes \dots \otimes e_{i_m} \otimes f^{j_1} \otimes \dots \otimes f^{j_m} \otimes \\ & \quad \otimes e_{q_1} \otimes \dots \otimes e_{q_t} \otimes f^{p_1} \otimes \dots \otimes f^{p_s}. \end{aligned}$$

Операция свертки заключается в том, что в каждом слагаемом суммы тензорных произведений

$$x_{i_1} \otimes \dots \otimes x_{i_s} \otimes \dots \otimes x_{i_m} \otimes y^{j_1} \otimes \dots \otimes y^{j_t} \otimes \dots \otimes y^{j_k}$$

выбираются одинаково для всех слагаемых один ковектор  $y^{j_t}$  и один вектор  $x_{j_s}$ , они выбрасываются, но при этом появляется в качестве множителя значение ковектора  $y^{j_t}$  на векторе  $x_{j_s}$ . Инвариантность этой операции легко проследить. Если ее выполнить в записи тензора через базис:

$$a_{i_1 \dots i_t}^{j_1 \dots j_s} e_{i_1} \otimes \dots \otimes e_{i_s} \otimes \dots \otimes e_{i_m} \otimes f^{j_1} \otimes \dots \otimes f^{j_t} \otimes \dots \otimes f^{j_k},$$

мы получим, что значение  $f^{j_t}$  на  $e_{j_s}$  отлично от нуля и равно 1 только при  $j_s = i_t$ , и при фиксированных остальных индексах нужно сложить получившиеся свободные члены, что и сводится к

суммированию по  $i_t$  компонент  $a_{i_1 \dots i_t \dots i_t \dots i_k}^{j_1 \dots j_t \dots j_t \dots j_m}$ , т. е. описанная операция свертки в инвариантной форме совпадает со сверткой при задании тензора компонентами.

**6. «Прямоугольные» тензоры.** Компоненты тензора полной валентности  $m$  естественно сопоставляются точкам с целыми координатами от 1 до  $n$  ( $n$  — размерность пространства) в  $m$ -мерном пространстве. Они образуют как бы  $m$ -мерно кубическую таблицу, подобно тому, как при полной валентности 2 компоненты располагаются в виде квадратной матрицы. Аналогами прямоугольных матриц могут служить компоненты тензоров, связанных с несколькими пространствами.

Пусть даны пространства  $S_1, S_2, \dots, S_r$  над одним и тем же полем  $K$ . Рассмотрим тензорное произведение нескольких экземпляров  $S_1$  и  $S_1^*$ , нескольких экземпляров  $S_2$  и  $S_2^*$  и т. д. Векторы получившегося пространства будут иметь вид

$$a_{i_1 i_2 \dots i_k, p_1 p_2 \dots p_s}^{j_1 j_2 \dots j_l, q_1 q_2 \dots q_t} e_{j_1} \otimes \dots \otimes e_{j_l} \otimes f^{i_1} \otimes \dots \otimes f^{i_k} \otimes g_{q_1} \otimes \dots \otimes g_{q_t} \otimes h^{p_1} \otimes \dots \otimes h^{p_s} \otimes \dots$$

Здесь индексы  $i_1, \dots, i_k, j_1, \dots, j_l$  принимают значения от 1 до  $n_1 = \dim S_1$ , индексы  $q_1, \dots, q_t$  и  $p_1, \dots, p_s$  принимают значения от 1 до  $n_2 = \dim S_2$  и т. д.;  $e_1, \dots, e_{n_1}$  — базис  $S_1$ ,  $f_1, \dots, f_{n_1}$  — дуальный базис  $S_1^*$ ,  $g_1, \dots, g_{n_2}$  и  $h_1, \dots, h_{n_2}$  — базисы  $S_2$  и  $S_2^*$  и т. д.

Компоненты при преобразованиях координат в пространствах  $S_1, S_2, \dots$  изменяются по правилам преобразования компонент тензора, только первая группа индексов связана с  $S_1$ , вторая группа с  $S_2$  и т. д. Сложение, умножение на скаляры и умножение тензоров выполняются по тем же правилам, что и для обычных тензоров. Свертка допустима только по нижнему и верхнему индексам из одной группы.

## § 1. Общие сведения

**1. Определение и простейшие свойства алгебр.** В различных разделах математики возникает потребность рассматривать векторные пространства (над данным полем  $K$ ), в которых кроме действий сложения и умножения на скаляры определено еще действие умножения, сопоставляющее каждой упорядоченной паре векторов третий вектор того же пространства — их «произведение». В этой ситуации всегда естественно предполагать, что результат умножения  $xu$  линеен по каждому из множителей при фиксированном втором, т. е.

$$(c_1x_1 + c_2x_2)u = c_1x_1u + c_2x_2u, \quad x(c_1y_1 + c_2y_2) = c_1xy_1 + c_2xy_2.$$

Пространство с умножением, удовлетворяющим такому требованию билинейности, называется *алгеброй* над полем  $K$ .

Иначе можно сказать, что алгебра есть одновременно кольцо и линейное (векторное) пространство с естественным согласованием кольцевого умножения и векторных действий. Именно, сложение в кольце и сложение в векторном пространстве совпадают, а свойства дистрибутивности для умножения «усиливаются» до линейности по каждому множителю, для чего достаточно потребовать, чтобы  $(sx)y = x(sy) = sxy$  при любых  $s \in K$  и  $x, y$  из алгебры.

Читатель уже неоднократно встречался с алгебрами. Напомним некоторые знакомые примеры алгебр.

1. Поле  $\mathbb{C}$  комплексных чисел над полем  $\mathbb{R}$  вещественных чисел образует, очевидно, алгебру размерности 2.

2. Кольцо квадратных матриц порядка  $n$  с элементами из поля  $K$  образует алгебру над этим полем размерности  $n^2$ .

3. Кольцо многочленов  $K[t]$  образует алгебру бесконечной размерности над полем  $K$ .

4. Пусть  $f$  — фиксированный многочлен степени  $n$  из  $K[t]$ . Классы сравнений по модулю  $f$  образуют алгебру размерности  $n$ .

Все эти алгебры ассоциативны. Все они, кроме алгебры квадратных матриц, коммутативны. Примером неассоциативной алгебры может служить пространство векторов в трехмерном евклидовом пространстве с умножением в смысле векторного умножения.

Мы будем рассматривать только конечномерные алгебры.

С каждым элементом  $x$  алгебры  $A$  связаны два оператора, действующие в линейном пространстве алгебры. Это оператор *пра-*

вого умножения  $\mathcal{R}_x: y \mapsto yx$ , сопоставляющий каждому элементу  $y \in A$  его произведение на  $x$  справа, и оператор *левого умножения*  $\mathcal{L}_x: y \mapsto xy$ . Оператор  $\mathcal{R}_x$  линеен в силу линейности умножения в алгебре относительно левого множителя. Далее, отображение  $x \mapsto \mathcal{R}_x$  пространства алгебры  $A$  в пространство  $S$  линейных операторов тоже линейно в силу линейности умножения в алгебре относительно правого множителя. Аналогично, линеен оператор  $\mathcal{L}_x$  и линейно отображение  $x \mapsto \mathcal{L}_x$ . Операторы правого и левого умножения связаны очевидным соотношением:  $\mathcal{L}_x(y) = \mathcal{R}_y(x)$ .

Задание некоторого линейного отображения  $x \mapsto \varphi_x$  данного векторного пространства  $A$  в пространство  $S$  линейных операторов, действующих в  $A$ , можно рассматривать как задание алгебры, для которой операторы  $\varphi_x$  суть операторы правого умножения. Действительно, если для элементов  $x, y \in A$  положить  $yx = \varphi_x(y)$ , то линейность этого умножения относительно первого множителя обуславливается линейностью операторов  $\varphi_x$ , а линейность относительно второго множителя — линейностью отображения  $x \mapsto \varphi_x$ . Аналогично алгебра может быть задана и посредством задания операторов левого умножения.

Две алгебры  $A$  и  $B$  называются *изоморфными*, если существует взаимно однозначное линейное отображение  $A$  на  $B$ , преобразующее произведение прообразов в произведение образов.

Например, алгебра  $C$  комплексных чисел (как алгебра над полем  $R$ ) изоморфна алгебре вещественных матриц вида  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ . Действительно, отображение  $\varphi: \varphi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  линейно, взаимно однозначно и

$$\begin{aligned} \varphi[(a + bi)(c + di)] &= \\ &= \begin{pmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \varphi(a + bi)\varphi(c + di). \end{aligned}$$

Взаимно однозначное соответствие

$$(a, b, c) \leftrightarrow \begin{pmatrix} 0 & c & b \\ -c & 0 & a \\ -b & -a & 0 \end{pmatrix}$$

между тройками вещественных чисел и антисимметричными матрицами третьего порядка есть изоморфизм алгебр, если тройки умножать по правилу векторного умножения векторов, заданных в декартовой системе координат, а «произведением» матриц  $L$  и  $M$  считать  $L \circ M = LM - ML$ .

**2. Структурные константы алгебры.** Для того чтобы описать правило умножения в данной конечномерной алгебре, достаточно задать «таблицу умножения» для какого-либо ее базиса, т. е. записать произведение каждой пары элементов выбранного базиса в виде линейной комбинации его элементов:  $e_i e_j = a_{ij}^k e_k$ ;  $a_{ij}^k \in K$  (мы пользуемся тензорными обозначениями). Константы  $a_{ij}^k$  назы-

ваются *структурными константами* алгебры. Покажем, что они составляют дважды ковариантный и один раз контравариантный тензор. Пусть  $\hat{f}_p = c_p^i e_i$  — новый базис алгебры. Тогда  $e_k = \gamma_k^r \hat{f}_r$ . Далее,  $\hat{f}_p \hat{f}_q = c_p^i c_q^j e_i e_j = c_p^i c_q^j a_{ij}^k e_k = a_{ij}^k c_p^i c_q^j \gamma_k^r \hat{f}_r$ , так что новые структурные константы  $a_{ij}^k c_p^i c_q^j \gamma_k^r$  получены из исходных по правилу преобразования дважды ковариантного и один раз контравариантного тензора. По этой причине набор структурных констант называют также структурным тензором.

Если алгебры  $A$  и  $B$  изоморфны, то в соответствующих (в силу изоморфизма) базисах структурные константы совпадают. Ясно и обратное, если у двух алгебр структурные константы совпадают, то сопоставление базисных элементов осуществляет изоморфизм алгебр. Поэтому для изоморфизма двух алгебр необходимо и достаточно, чтобы в них существовали базисы, определяющие одинаковые структурные тензоры. Следовательно, для того чтобы алгебры, заданные структурными тензорами в некоторых базисах, были изоморфны, необходимо и достаточно, чтобы эти структурные тензоры были связаны соотношением  $a_{pq}^r = a_{ij}^k c_p^i c_q^j \gamma_k^r$  при некоторых  $c_p^i$ .

**3. Некоторые классы алгебр.** Как уже было сказано выше, алгебры с ассоциативным умножением называются ассоциативными алгебрами. Ассоциативность будет иметь место, если выполнены  $n^3$  равенств:  $(e_i e_j) e_k = e_i (e_j e_k)$ , где  $e_1, \dots, e_n$  — какой-либо базис алгебры. Запишем это условие в терминах структурных констант. Имеем:  $e_i e_j = a_{ij}^p e_p$ ,  $(e_i e_j) e_k = a_{ij}^p e_p e_k = a_{ij}^p a_{pk}^q e_q$ . Далее,  $e_i e_k = a_{ik}^r e_r$ ,  $e_i (e_j e_k) = a_{jk}^r e_i e_r = a_{jk}^r a_{ir}^q e_q$ . Таким образом, условие ассоциативности имеет вид  $a_{ij}^p a_{pk}^q = a_{jk}^r a_{ir}^q$ .

Положив  $a_{ij}^p a_{pk}^q = a_{jk}^r a_{ir}^q = b_{ijk}^q$ , получим, что  $b_{ijk}^q$  есть тензор структурных констант для тройных произведений  $e_i e_j e_k = b_{ijk}^q e_q$  ассоциативной алгебры.

В терминах операторов умножения условие ассоциативности формулируется проще и естественнее. Именно, ассоциативность эквивалентна каждому из трех следующих свойств операторов умножения (записанных как левые операторы, т. е. первым действующим считается тот, который записан справа):

$$1) \mathcal{R}_{xy} = \mathcal{R}_y \mathcal{R}_x, \quad 2) \mathcal{R}_x \mathcal{L}_y = \mathcal{L}_y \mathcal{R}_x, \quad 3) \mathcal{L}_{xy} = \mathcal{L}_x \mathcal{L}_y.$$

Алгебра называется *коммутативной*, если  $xy = yx$  при любых  $x$  и  $y$  из алгебры. Алгебра называется *антикоммутативной*, если квадрат любого ее элемента равен нулю. В этом случае для любых  $x$  и  $y$  из алгебры выполнено соотношение  $xy = -yx$ , ибо

$$0 = (x + y)(x + y) = x^2 + yx + xy + y^2 = yx + xy.$$

Алгебра называется *алгеброй Ли*, если она антикоммутативна и для любых трех ее элементов выполнено *соотношение Якоби*:

$$x(yz) + y(zx) + z(xy) = 0.$$

Среди алгебр, встречающихся в приложениях, алгебры Ли играют особую роль. В частности, они тесно связаны с группами Ли.

Любая ассоциативная алгебра может быть «превращена» в алгебру Ли посредством введения нового «умножения»  $\circ$  по правилу  $x \circ y = xy - yx$ . Ясно, что  $x \circ x = 0$  при любом  $x$ . Соотношение же Якоби легко проверяется:

$$x \circ (y \circ z) + y \circ (z \circ x) + z \circ (x \circ y) = x(yz - zy) - (yz - zy)x + \\ + y(zx - xz) - (zx - xz)y + z(xy - yx) - (xy - yx)z = 0.$$

Алгебра (не обязательно ассоциативная) называется *алгеброй с делением*, если уравнение  $xy = z$  разрешимо относительно  $x$  при данных  $y \neq 0$  и  $z$ . Другими словами, алгебры с делением характеризуются тем, что все операторы правого умножения, кроме нулевого, невырождены. В алгебрах с делением уравнение  $xy = z$  при  $y \neq 0$  разрешимо относительно  $x$  однозначно, ибо невырожденный оператор имеет нулевое ядро. В частности, из равенства  $xy = 0$  следует, что при  $y \neq 0$   $x = 0$  и что  $x \neq 0$  возможно только при  $y = 0$ . Но это значит, что любой оператор левого умножения, кроме умножения на 0, имеет нулевое ядро и, следовательно, невырожден. Поэтому и каждое уравнение  $xy = z$  при  $x \neq 0$  разрешимо относительно  $y$ .

Легко видеть, что над полем  $\mathbb{C}$  не существует алгебр с делением, кроме самого  $\mathbb{C}$ . Действительно, если размерность  $n$  алгебры с делением больше 1, то в ней существует два линейно независимых элемента  $x$  и  $y$ . Рассмотрим соответствующие им операторы правого умножения  $\mathcal{R}_x$  и  $\mathcal{R}_y$  и их матрицы  $R_x$  и  $R_y$  в некотором базисе. В силу невырожденности операторов правого умножения  $\det R_x \neq 0$  и  $\det R_y \neq 0$ . Рассмотрим элемент  $x + ty$  при  $t \in \mathbb{C}$ . Оператор правого умножения на него есть  $R_x + tR_y$ . Его определитель  $\det(R_x + tR_y) = \det R_x + \dots + t^n \det R_y$  есть полином степени  $n$  от  $t$ , следовательно, обращается в 0 при некотором значении  $t$ . Это невозможно в алгебре с делением, ибо  $x + ty \neq 0$ , и, следовательно, оператор  $\mathcal{R}_x + t\mathcal{R}_y$  должен быть невырожден. Что касается алгебр размерности 1, то, как легко видеть, их существует только две, с точностью до изоморфизма, — алгебра с нулевым умножением (т. е. алгебра, в которой произведение любых двух элементов равно 0) и  $\mathbb{C}$ . Над полем вещественных чисел алгебры с делением существуют — в частности, поле  $\mathbb{C}$ . С важной алгеброй размерности 4 мы познакомимся в следующем параграфе.

**4. Идеалы алгебры.** Правым идеалом алгебры  $A$  называется подпространство  $J$  такое, что при любых  $y \in J$ ,  $x \in A$  будет  $yx \in J$ . Другими словами, правый идеал алгебры есть подпространство, инвариантное для всех операторов правого умножения. Аналогично определяется левый идеал алгебры. Подпространство, являющееся правым идеалом и левым идеалом одновременно, называется *двусторонним идеалом*. Ясно, что в коммутативной или в антикомму- тативной алгебре все идеалы двусторонние.

Двусторонние идеалы играют в теории алгебр такую же роль, как нормальные подгруппы в теории групп: именно они, и только они, являются ядрами гомоморфизмов алгебр. *Гомоморфизмом*, или *гомоморфным отображением* алгебры  $A$  в алгебру  $B$  называется линейное отображение  $\varphi: A \rightarrow B$ , сохраняющее умножение, т. е. такое, что  $\varphi(xy) = \varphi(x)\varphi(y)$ .

Легко видеть, что ядро  $J$  любого гомоморфизма  $\varphi$  алгебры  $A$  есть двусторонний идеал. Действительно, если  $y \in J$ , то  $\varphi(y) = 0$ , но тогда  $\varphi(xy) = \varphi(x)\varphi(y) = 0$  и  $\varphi(yx) = \varphi(y)\varphi(x) = 0$  при любом  $x \in A$ . Значит,  $xy \in J$  и  $yx \in J$ , т. е.  $J$  есть двусторонний идеал.

Для того чтобы показать, что любой двусторонний идеал есть ядро некоторого гомоморфизма, нужно осуществить построение факторалгебры  $A/J$ , т. е. ввести естественным образом действие умножения в факторпространстве  $A/J$ . Вспомним, что факторпространство  $A/J$  состоит из классов сравнений по модулю  $J$ . Линейной комбинацией классов считается класс, содержащий такую же линейную комбинацию представителей, и этот класс не зависит от выбора представителей в силу очевидного свойства сравнений по подпространству. Введем столь же естественным способом действие умножения классов. Именно, произведением двух классов назовем класс, содержащий произведение любой пары представителей от умножаемых классов. Корректность этого определения, т. е. независимость класса от выбора представителей, обеспечивается следующей леммой.

**Л е м м а.** Если  $J$  — двусторонний идеал алгебры  $A$  и если  $x_1 \equiv y_1 \pmod{J}$  и  $x_2 \equiv y_2 \pmod{J}$ , то  $x_1x_2 \equiv y_1y_2 \pmod{J}$ .

**Доказательство.**  $x_1x_2 - y_1y_2 = x_1(x_2 - y_2) + (x_1 - y_1)y_2 \in J$ , ибо  $x_2 - y_2 \in J$ ,  $x_1 - y_1 \in J$  и  $J$  есть двусторонний идеал. Лемма доказана.

Итак, в факторпространстве  $A/J$  мы ввели умножение. Его линейность относительно каждого из сомножителей следует из билинейности умножения в алгебре  $A$ . Ясно, что  $A/J$  есть гомоморфный образ алгебры  $A$  при «естественном» отображении, соотносящем каждому элементу  $x \in A$  содержащий его класс. То что это отображение гомоморфно, следует из определения действий в  $A/J$ .

Справедлива также следующая теорема.

**Т е о р е м а 1.** Гомоморфный образ алгебры изоморфен факторалгебре по ядру гомоморфизма.

Доказательство почти очевидно — легко проследить, что прообразами будут классы по ядру, т. е. элементы факторалгебры, и их умножение соответствует умножению образов.

Алгебра, не имеющая двусторонних идеалов, кроме себя и нуля, называется *простой* алгеброй.

Легко видеть, что алгебры с делением могут быть охарактеризованы как алгебры, не имеющие правых (левых) идеалов, кроме себя и нуля, и отличные от алгебры размерности 1 с нулевым умножением.

**5. Присоединение единицы.** Единицей алгебры  $A$  называется элемент  $1$ , удовлетворяющий требованиям  $1 \cdot x = x \cdot 1 = x$  при любом  $x \in A$ . Единица в алгебре может существовать, может и не существовать. Если существует, то только одна: если  $1'$  и  $1''$  — две единицы, то  $1'1'' = 1''$ , так как  $1'$  — единица, и  $1'1'' = 1'$ , ибо  $1''$  — тоже единица, т. е.  $1' = 1''$ .

Однако всегда можно погрузить алгебру  $A$  в алгебру  $\tilde{A}$  на единицу большей размерности так, что в алгебре  $\tilde{A}$  единица есть. Действительно, положим  $\tilde{A} = K e \oplus A$  и введем в  $\tilde{A}$  умножение по правилу:  $(c_1 e + x_1)(c_2 e + x_2) = c_1 c_2 e + c_1 x_2 + c_2 x_1 + x_1 x_2$  при любых  $c_1, c_2 \in K, x_1, x_2 \in A$ . Ясно, что введенное умножение билинейно, так что  $\tilde{A}$  — алгебра. Далее,  $e(se + x) = se + x$  и  $(se + x)e = se + x$ , так что  $e$  есть единица алгебры  $\tilde{A}$ . Действия над элементами из  $A$  внутри  $\tilde{A}$  не отличаются от действий над ними внутри  $A$ .

Переход от алгебры  $A$  к алгебре  $\tilde{A}$  называется *внешним присоединением единицы*. Если в исходной алгебре  $A$  единица была, то в расширенной алгебре она перестает быть единицей. Ясно, что алгебра  $A$  является двусторонним идеалом для  $\tilde{A}$  и факторалгебра  $\tilde{A}/A$  изоморфна полю  $K$ .

Легко проверяется, что если алгебра  $A$  ассоциативна, то и  $\tilde{A}$  ассоциативна; если  $A$  коммутативна, то и  $\tilde{A}$  коммутативна. Но, например, антикоммутативность (и лиевость) алгебры не сохраняется при внешнем присоединении единицы, так что эта операция для антикоммутативных (и лиевых) алгебр не целесообразна.

## 6. Вложение ассоциативной алгебры в алгебру матриц.

**Теорема 2.** Ассоциативная алгебра с единицей размерности  $n$  над полем  $K$  изоморфна некоторой подалгебре алгебры квадратных матриц порядка  $n$ . Если единицы нет, то возможно погружение в том же смысле в алгебру матриц порядка  $n$  или  $n + 1$ .

**Доказательство.** Пусть  $\mathcal{L}_x$  — оператор левого умножения на элемент  $x$  в ассоциативной алгебре  $A$  размерности  $n$ . Из ассоциативности  $x(yz) = (xy)z$  следует, что умножить слева на  $x$  все равно, что сперва умножить на  $y$ , потом на  $x$ . Это значит, что  $\mathcal{L}_{xy} = \mathcal{L}_x \mathcal{L}_y$  (при левой записи операторов), т. е. что отображение  $x \mapsto \mathcal{L}_x$  есть не только линейное отображение пространства алгебры  $A$  в пространство операторов, но и гомоморфизм алгебры  $A$  в алгебру операторов. Ядро этого гомоморфизма состоит из тех элементов  $x \in A$ , которые аннулируют все элементы алгебры при умножении слева, т. е. таких, что  $xz = 0$  при всех  $z \in A$ . Если таких элементов нет в алгебре  $A$ , кроме нуля, то отображение  $x \mapsto \mathcal{L}_x$  есть изоморфное отображение алгебры на подалгебру алгебры линейных операторов, состоящую из операторов левого умножения. В свою очередь, алгебра всех линейных операторов, действующих в пространстве алгебры  $A$ , изоморфна алгебре квадратных матриц порядка  $n$ . Ясно, что если алгебра содержит  $1$ , то  $x \cdot 1 = x$ , и ядро отображения  $x \mapsto \mathcal{L}_x$  состоит только из нуля. Поэтому для алгебр с единицей теорема доказана.

Если же ядро нетривиально, то перейдем к алгебре  $\tilde{A}$  посредством внешнего присоединения единицы. Обозначим через  $\tilde{\mathcal{L}}_x$  оператор умножения на  $x \in A$  в алгебре  $\tilde{A}$ . Ясно, что снова  $\tilde{\mathcal{L}}_x \tilde{\mathcal{L}}_y = \tilde{\mathcal{L}}_{xy}$  при любых  $x, y \in A$ . Но на этот раз ядро гомоморфизма  $x \mapsto \tilde{\mathcal{L}}_x$  состоит только из нуля, ибо из  $x \cdot 1 = 0$  следует  $x = 0$ . Таким образом, отображение  $x \mapsto \tilde{\mathcal{L}}_x$  есть изоморфизм алгебры  $A$  в алгебру операторов, действующих в пространстве алгебры  $\tilde{A}$ , которая, в свою очередь, изоморфна алгебре матриц порядка  $n + 1$ .

## § 2. Алгебра кватернионов

**1. Определение.** Алгеброй кватернионов называется алгебра размерности 4 над основным полем, обладающая единицей 1 и имеющая базис  $1, i, j, k$  со следующей таблицей умножения:  $i^2 = j^2 = k^2 = -1$ ,  $ij = -ji = k$ ,  $jk = -kj = i$ ,  $ki = -ik = j$ .

Основное поле может быть взято произвольно. Наиболее интересной для приложений является алгебра кватернионов над полем  $\mathbb{R}$  вещественных чисел, которая и будет исследоваться в дальнейшем.

Прежде всего установим ассоциативность алгебры кватернионов. Для этого следует проверить 27 равенств (три возможности для каждого из трех множителей в равенствах  $(ab)c = a(bc)$ , проверяемых для базисных элементов  $i, j, k$ ). Мы избежим этого, установив изоморфизм алгебры кватернионов над  $\mathbb{R}$  и некоторой алгебры матриц специального вида над  $\mathbb{C}$ . Именно, единице 1 сопоставим единичную матрицу  $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  второго порядка, эле-

менту  $i$  алгебры кватернионов — матрицу  $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$  (здесь элемент матрицы  $i \in \mathbb{C}$  — обычная мнимая единица, так что нами сознательно допущена путаница в обозначениях — буква  $i$  обозначает в одном контексте два разных объекта), элементу  $j$  сопоставим матрицу  $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  и элементу  $k$  — матрицу  $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ . Равенства  $I^2 = J^2 = K^2 = -E$ ,  $IJ = -JI = K$ ,  $JK = -KJ = I$ ,  $KI = -IK = J$  легко проверяются. Они означают, что пространство матриц, натянутое на матрицы  $E, I, J, K$ , образует алгебру, изоморфную алгебре кватернионов.

На основании ассоциативности умножения матриц мы заключаем об ассоциативности алгебры кватернионов.

Заметим, что если за основное поле принято поле  $\mathbb{C}$  комплексных чисел, то алгебра кватернионов (над  $\mathbb{C}$ ) окажется изоморфной алгебре  $M_2(\mathbb{C})$  всех квадратных матриц второго порядка над  $\mathbb{C}$ , ибо матрицы  $E, I, J, K$  линейно независимы над  $\mathbb{C}$  и их линейные комбинации заполняют всю алгебру  $M_2(\mathbb{C})$ .

**2. Связь алгебры кватернионов с векторами в трехмерном евклидовом пространстве.** Пусть  $\alpha = a + bi + cj + dk$  — кватернион. Число  $a$  называется *скалярной частью* кватерниона. Кватернион

$bi + cj + dk$  называется *векторной частью* кватерниона  $\alpha$ . Кватернионы с нулевой скалярной частью будем называть *векторами*, они, естественно, изображаются как векторы трехмерного евклидова пространства.

Пусть  $u_1 = b_1i + c_1j + d_1k$  и  $u_2 = b_2i + c_2j + d_2k$  — два вектора. Вычислим их произведение (в алгебре кватернионов)

$$\begin{aligned} u_1 u_2 = & b_1 i b_2 i + b_1 i c_2 j + b_1 i d_2 k + c_1 j b_2 i + c_1 j c_2 j + c_1 j d_2 k + \\ & + d_1 k b_2 i + d_1 k c_2 j + d_1 k d_2 k = -b_1 b_2 - c_1 c_2 - d_1 d_2 + (c_1 d_2 - d_1 c_2) i + \\ & + (d_1 b_2 - b_1 d_2) j + (b_1 c_2 - c_1 b_2) k = -(u_1, u_2) + [u_1, u_2] \end{aligned}$$

(здесь  $[u_1, u_2]$  — векторное произведение векторов  $u_1$  и  $u_2$ ).

Таким образом, скалярной частью кватерниона  $u_1 u_2$  оказывается скалярное произведение векторов  $u_1, u_2$ , взятое с обратным знаком. Векторная же часть кватерниона  $u_1 u_2$  равна векторному произведению векторов  $u_1, u_2$ . Тем самым операция умножения векторов как элементов алгебры кватернионов как бы объединяет оба умножения векторов — скалярное и векторное.

Далее, легко видеть, что

$$u_2 u_1 = -(u_2, u_1) + [u_2, u_1] = -(u_1, u_2) - [u_1, u_2].$$

Отсюда

$$(u_1, u_2) = -\frac{1}{2}(u_1 u_2 + u_2 u_1), \quad [u_1, u_2] = \frac{1}{2}(u_1 u_2 - u_2 u_1).$$

Из последней формулы немедленно следует известное в векторной алгебре соотношение Якоби  $[[u_1, u_2], u_3] + [[u_2, u_3], u_1] + [[u_3, u_1], u_2] = 0$ . Достаточно принять во внимание связь между ассоциативными алгебрами и алгебрами Ли (см. п. 3 § 1).

**3. Алгебра кватернионов как алгебра с делением.** Пусть дан кватернион  $\alpha = a + bi + cj + dk = a + u$ . Кватернион  $\bar{\alpha} = a - bi - cj - dk = a - u$ , отличающийся от  $\alpha$  знаком векторной части, называется *сопряженным* с кватернионом  $\alpha$ . Ясно, что  $\bar{\bar{\alpha}} = \alpha$ .

Умножим кватернион  $\alpha$  на сопряженный  $\bar{\alpha}$ . Получим  $\alpha \bar{\alpha} = (a + u)(a - u) = a^2 + au - au - u^2 = a^2 + (u, u) - [u, u] = a^2 + (u, u) = a^2 + b^2 + c^2 + d^2$ . Поэтому, если  $\alpha \neq 0$ , то  $\alpha \bar{\alpha} > 0$ . Заметим еще, что  $\alpha \bar{\alpha} = \bar{\alpha} \alpha$ .

Число  $\sqrt{\alpha \bar{\alpha}} = \sqrt{a^2 + b^2 + c^2 + d^2}$  называется *модулем* кватерниона  $\alpha$  и обозначается через  $|\alpha|$ . Теперь легко установить, что каждый отличный от нуля кватернион  $\alpha$  имеет обратный. Действительно,  $\left(\frac{1}{\alpha \bar{\alpha}} \bar{\alpha}\right) \alpha = \alpha \left(\frac{1}{\alpha \bar{\alpha}} \bar{\alpha}\right) = 1$ , так что обратным кватернионом для  $\alpha$  является  $\frac{1}{\alpha \bar{\alpha}} \cdot \bar{\alpha}$ . Таким образом, алгебра кватернионов над полем  $\mathbb{R}$  есть алгебра с делением.

Заметим, что здесь существенно было использовано то обстоятельство, что за основное поле принято поле  $\mathbb{R}$ : заключение о не-

равенстве нулю  $a^2 + b^2 + c^2 + d^2$  при  $\alpha \neq 0$  было бы неверно, например, для поля  $\mathbb{C}$  или поля вычетов по простому модулю.

#### 4. Тождество Эйлера.

**Теорема 3.** *Модуль произведения двух кватернионов равен произведению модулей сомножителей.*

**Доказательство.** Сначала докажем, что кватернион, сопряженный с произведением двух кватернионов, равен произведению сопряженных кватернионов, взятых в обратном порядке. Действительно, пусть  $\alpha = a + u$ ,  $\beta = b + v$ , где  $a, b \in \mathbb{R}$ ,  $u$  и  $v$  — векторы. Тогда  $\alpha\beta = ab + av + bu + uv = ab - (u, v) + av + bu + [u, v]$ . Далее,  $\beta\bar{\alpha} = ab - av - bu + vu = ab - (v, u) - av - bu + [v, u] = ab - (u, v) - av - bu - [u, v] = \overline{\alpha\beta}$ . Теперь имеем  $|\alpha\beta|^2 = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta\bar{\beta}\bar{\alpha} = \alpha|\beta|^2\bar{\alpha} = |\beta|^2|\alpha|^2$ , откуда  $|\alpha\beta| = |\alpha||\beta|$ , что и требовалось доказать.

Распишем теперь тождество  $|\alpha\beta|^2 = |\alpha|^2|\beta|^2$  через компоненты кватернионов, положив  $\alpha = a_1 - b_1i - c_1j - d_1k$ ,  $\beta = a_2 + b_2i + c_2j + d_2k$ , так что  $\alpha\beta = a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2 + (a_1b_2 - b_1a_2 - c_1d_2 + d_1c_2)i + (a_1c_2 + b_1d_2 - c_1a_2 - d_1b_2)j + (a_1d_2 - b_1c_2 + c_1b_2 - d_1a_2)k$ . Получим известное тождество Эйлера:

$$\begin{aligned} (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = \\ = (a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + (a_1b_2 - b_1a_2 - c_1d_2 + d_1c_2)^2 + \\ + (a_1c_2 + b_1d_2 - c_1a_2 - d_1b_2)^2 + (a_1d_2 - b_1c_2 + c_1b_2 - d_1a_2)^2, \end{aligned}$$

позволяющее выразить произведение двух сумм четырех квадратов в виде суммы четырех квадратов билинейных выражений. Аналогичные тождества имеют место для сумм двух квадратов (это тождество связано с умножением комплексных чисел) и для сумм восьми квадратов. Это последнее тождество связано с умножением в так называемой алгебре Кэли — некоторой уже не ассоциативной алгебре с делением размерности 8. Оказывается, что аналогичных тождеств для сумм  $n$  квадратов, кроме перечисленных при  $n = 2, 4, 8$  (и тривиального тождества при  $n = 1$ ), не существует.

**5. Вращения трехмерного евклидова пространства.** Пусть  $u, v, w$  — тройка попарно ортогональных векторов единичной длины, ориентированная так же, как тройка  $i, j, k$ . Тогда, согласно правилу умножения векторов в алгебре кватернионов, получим  $u^2 = v^2 = w^2 = -1$ . Далее,  $uv = -(u, v) + [u, v] = [u, v] = w$ . Здесь мы воспользовались тем, что векторное произведение взаимно ортогональных единичных векторов равно единичному вектору, ортогональному к ним обоим и направленному в соответствии с ориентацией базисных векторов  $i, j, k$ . Аналогично,  $vu = -w$ ,  $vw = -wv = u$ ,  $wu = -uw = v$ . Таким образом, правило умножения векторов  $u, v, w$  ничем не отличается, кроме обозначений, от правила умножения векторов  $i, j, k$ . Иными словами, отображение  $1 \mapsto 1, i \mapsto u, j \mapsto v, k \mapsto w$  задает изоморфизм алгебры ква-

тернионов на себя, т. е. автоморфизм этой алгебры. Линейное преобразование пространства векторов, отображающее тройку  $i, j, k$  на тройку  $u, v, w$ , есть, очевидно, собственно ортогональное преобразование, ибо эти две тройки образуют ортонормальные одинаково ориентированные базисы пространства векторов. Ясно, что любое собственно ортогональное преобразование пространства векторов определяет некоторый автоморфизм алгебры кватернионов.

Все автоморфизмы получаются указанным способом. Действительно, пусть  $u, v, w$  — образы  $i, j, k$  при некотором автоморфизме. Тогда  $u^2 = v^2 = w^2 = -1$ ,  $uv = -vu = w$ ,  $vw = -wv = u$  и  $wu = -uw = v$ . Из равенства  $u^2 = -1$  заключаем, что кватернион  $u$  есть вектор единичной длины. Действительно, пусть  $u = a + u_1$ , где  $a$  — скалярная часть  $u$ . Тогда  $-1 = u^2 = a^2 + 2au_1 - |u_1|^2$ , откуда  $2au_1 = 0$ . Если допустить, что  $u_1 \neq 0$ , то  $-1 = a^2$ , что невозможно. Поэтому  $u_1 \neq 0$  и, следовательно,  $a = 0$ ,  $|u| = |u_1| = 1$ . По той же причине кватернионы  $v$  и  $w$  — тоже векторы единичной длины. Далее, из того, что скалярная часть кватерниона  $uv = w$  равна нулю, мы заключаем, что векторы  $u$  и  $v$  ортогональны. По той же причине ортогональны векторы  $v, w$  и  $w, u$ , так что  $u, v, w$  составляют тройку попарно ортогональных единичных векторов. Ориентация этой тройки совпадает с ориентацией тройки  $i, j, k$ , ибо в противном случае было бы  $uv = -w$ , а не  $uv = w$ .

Пусть теперь  $\alpha$  — некоторый кватернион единичного модуля. Ясно, что отображение  $x \mapsto \alpha^{-1}x\alpha$  есть автоморфизм алгебры кватернионов и, следовательно, он осуществляет некоторое собственное вращение пространства векторов. Рассмотрим его подробнее. Пусть  $\alpha = a + u_0$ , где  $a$  — скалярная часть  $\alpha$ . Тогда  $a^2 + |u_0|^2 = 1$ , так что можно положить  $a = \cos \varphi$ ,  $|u_0| = \sin \varphi$ ,  $0 \leq \varphi \leq \pi$ . Тогда  $\alpha = \cos \varphi + u \sin \varphi$ , где  $u$  — вектор единичной длины (если  $\alpha = \pm 1$ , то  $u_0 = 0$ , и в качестве  $u$  можно взять любой единичный вектор). Пусть теперь  $v$  — какой-либо вектор единичной длины, ортогональный вектору  $u$ , и пусть  $w = uv$ . Выясним, как действует автоморфизм  $x \mapsto \alpha^{-1}x\alpha$  на векторы  $u, v, w$ . Ясно, что  $\alpha$  и  $u$  коммутируют, так что  $\alpha^{-1}u\alpha = u$ . Далее,

$$\alpha^{-1} = \bar{\alpha} = \cos \varphi - u \sin \varphi,$$

$$\begin{aligned} \alpha^{-1}v\alpha &= (\cos \varphi - u \sin \varphi)v(\cos \varphi + u \sin \varphi) = \\ &= (v \cos \varphi - w \sin \varphi)(\cos \varphi + u \sin \varphi) = \\ &= v \cos^2 \varphi - w \sin \varphi \cos \varphi + vu \sin \varphi \cos \varphi - wu \sin^2 \varphi = \\ &= v(\cos^2 \varphi - \sin^2 \varphi) - 2w \sin \varphi \cos \varphi = v \cos 2\varphi - w \sin 2\varphi, \\ \alpha^{-1}w\alpha &= (w \cos \varphi + v \sin \varphi)(\cos \varphi + u \sin \varphi) = v \sin 2\varphi + w \cos 2\varphi. \end{aligned}$$

Итак, автоморфизм  $x \mapsto \alpha^{-1}x\alpha$  не меняет вектор  $u$  и поворачивает на угол  $-2\varphi$  плоскость, натянутую на векторы  $v$  и  $w$  (считаем положительным направление вращения от  $v$  к  $w$ ), т. е. вращает пространство векторов вокруг оси, проходящей через вектор

$u$ , на угол  $-2\varphi$ . Известно, что всякое собственное вращение трехмерного пространства есть поворот вокруг некоторой оси на некоторый угол, так что любое собственное вращение может рассматриваться как трансформация  $x \mapsto \alpha^{-1}x\alpha$  посредством кватерниона  $\alpha$  единичным модулем.

Заметим, что преобразование  $x \mapsto \alpha^{-1}x\alpha$  при  $|\alpha| \neq 1$  не дает ничего нового, ибо, если положить  $\alpha = |\alpha|\alpha_0$ , то  $|\alpha_0| = 1$  и  $\alpha^{-1}x\alpha = \alpha_0^{-1}x\alpha_0$  при любом кватернионе  $x$ .

В любой ассоциативной алгебре с единицей обратимый элемент  $\alpha$  порождает автоморфизм алгебры  $x \mapsto \alpha^{-1}x\alpha$ . Такие автоморфизмы называются внутренними автоморфизмами алгебры. Полученный ранее результат показывает, что все автоморфизмы алгебры кватернионов внутренние.

Кватернионы единичного модуля образуют, очевидно, группу относительно умножения. Сопоставление каждому такому кватерниону вращения  $x \mapsto \alpha^{-1}x\alpha$  трехмерного пространства векторов есть, очевидно, гомоморфное отображение, ибо  $(\alpha\beta)^{-1}x\alpha\beta = \beta^{-1}(\alpha^{-1}x\alpha)\beta$ , т. е. произведению кватернионов отвечает произведение вращений. Ядро этого гомоморфизма состоит только из элементов  $\pm 1$ . Действительно,  $\alpha = a + bi + cj + dk$  принадлежит ядру, если  $\alpha^{-1}x\alpha = x$  при любом векторе  $x$ , т. е. если  $x\alpha = \alpha x$ . Положив  $x = i$ , получим  $c = d = 0$ , а положив  $x = j$ , получим  $b = d = 0$ . Итак,  $\alpha = a = \pm 1$ , ибо  $|\alpha| = |a| = 1$ .

Тем самым мы получили, что группа  $SO(3)$  собственных вращений трехмерного пространства изоморфна факторгруппе группы кватернионов единичного модуля по подгруппе  $\{\pm 1\}$ .

Представление трехмерных вращений при помощи кватернионов очень удобно тем, что кватернион, связанный с вращением, определяет непосредственно его геометрические характеристики — ось вращения и угол поворота. При обычном задании вращения при помощи ортогональной матрицы для определения оси вращения и угла нужно произвести некоторые, хотя и несложные, вычисления. Закон умножения кватернионов тоже проще (по форме записи) закона умножения матриц третьего порядка.

Заметим еще, что группа кватернионов с единичным модулем изоморфна группе  $SU(2)$  унитарных матриц второго порядка с определителем, равным единице. Действительно, кватерниону  $\alpha = a + bi + cj + dk$  соответствует, в силу описанного в п. 1 изоморфизма, матрица  $A = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ , сопряженному кватерниону  $\bar{\alpha} = a - bi - cj - dk$  — матрица  $\begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix} = A^*$ . Из равенства  $\alpha\bar{\alpha} = 1$  следует  $AA^* = E$ , т. е. матрица унитарна. Далее,  $\det A = a^2 + b^2 + c^2 + d^2 = 1$ . Обратное, если матрица  $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  унитарна и  $\det A = 1$ , то равенство  $A^{-1} = A^*$  дает  $\delta = \bar{\alpha}$ ,  $\gamma = -\bar{\beta}$ , т. е.  $A = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ .

Таким образом, отображение  $\alpha \mapsto A$  осуществляет изоморфизм группы кватернионов единичного модуля и группы  $SU(2)$ .

**6. Вращения четырехмерного пространства.** Рассмотрим четырехмерное пространство кватернионов как евклидово, с естественной метрикой: если  $x = a_1 + b_1i + c_1j + d_1k$ ,  $y = a_2 + b_2i + c_2j + d_2k$ , то  $(x, y) = a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2 = \operatorname{Re}(\bar{x}y) = \operatorname{Re}(x\bar{y})$ .

Пусть  $\beta$  — кватернион,  $|\beta| = 1$ . Покажем, что как оператор левого умножения на  $\beta$ , так и оператор правого умножения являются ортогональными операторами. Действительно,

$$(\beta x, \beta y) = \operatorname{Re}(\overline{\beta x} \beta y) = \operatorname{Re}(\bar{x} \bar{\beta} \beta y) = \operatorname{Re}(\bar{x} y) = (x, y)$$

и

$$(x\beta, y\beta) = \operatorname{Re}(x\beta \overline{y\beta}) = \operatorname{Re}(x\beta \bar{y} \bar{\beta}) = \operatorname{Re}(x\bar{y}) = (x, y).$$

Более того, оба эти оператора собственно ортогональны. Для доказательства положим  $\beta = \cos \varphi + u \sin \varphi$  и возьмем в качестве базиса векторы  $1, u, v, w$ , где  $v$  — какой-либо единичный вектор, ортогональный вектору  $u$ , и  $w = uv$ . Тогда

$$\beta \cdot 1 = \cos \varphi + u \sin \varphi,$$

$$\beta \cdot u = -\sin \varphi + u \cos \varphi,$$

$$\beta \cdot v = v \cos \varphi + w \sin \varphi,$$

$$\beta \cdot w = -v \sin \varphi + w \cos \varphi.$$

Таким образом, в рассматриваемом базисе оператор левого умножения на  $\beta$  имеет матрицу, составленную из двух одинаковых блоков определителя  $+1$ . Аналогично

$$1 \cdot \beta = \cos \varphi + u \sin \varphi,$$

$$u \cdot \beta = -\sin \varphi + u \cos \varphi,$$

$$v \cdot \beta = v \cos \varphi - w \sin \varphi,$$

$$w \cdot \beta = w \sin \varphi + w \cos \varphi,$$

так что матрица оператора правого умножения на  $\beta$  тоже имеет определитель, равный  $+1$ .

Заметим, что в базисе  $1, u, w, v$  оператор правого умножения имеет матрицу, состоящую из двух одинаковых блоков. Базис  $1, u, v, w$  получается из исходного  $1, i, j, k$  посредством собственно ортогонального преобразования координат, а базис  $1, u, w, v$  получается из исходного посредством несобственно ортогонального преобразования координат.

Рассмотрим теперь оператор двустороннего умножения:  $x \mapsto \gamma^{-1}x\beta$ , где  $\gamma$  и  $\beta$  — кватернионы единичного модуля. Этот оператор есть произведение собственно ортогонального оператора левого умножения на  $\gamma^{-1}$  и собственно ортогонального оператора правого умножения на  $\beta$ , поэтому он тоже собственно ортогонален.

Покажем, что любой собственно ортогональный оператор в пространстве кватернионов представляется в виде оператора двусто-

роного умножения. Действительно, пусть  $\varphi$  — такой оператор и пусть  $\varphi(1) = \alpha$ . Тогда  $|\alpha| = 1$  и  $\psi(x) = \varphi(x)\alpha^{-1}$  оставляет 1 на месте, и, следовательно, преобразует в себя ортогональное к 1 трехмерное пространство векторов, индуцируя в нем собственнo ортогональный оператор. Следовательно,  $\psi(x) = \gamma^{-1}x\gamma$  при некотором кватернионе  $\gamma$  единичного модуля и  $\varphi(x) = \gamma^{-1}x\beta$  при  $\beta = \gamma\alpha$ .

Рассмотрим (внешнее) прямое произведение  $G$  двух экземпляров группы кватернионов единичного модуля и каждому элементу  $\lambda = (\gamma, \beta) \in G$  этой группы сопоставим оператор  $x \mapsto \gamma^{-1}x\beta$ . Тогда произведению элементов из  $G$  соответствует произведение операторов. Действительно, пусть  $\lambda_1 = (\gamma_1, \beta_1)$ ,  $\lambda_2 = (\gamma_2, \beta_2)$ . Элементу  $\lambda_1\lambda_2 = (\gamma_1\gamma_2, \beta_1\beta_2)$  соответствует оператор  $x \mapsto (\gamma_1\gamma_2)^{-1}x\beta_1\beta_2 = = \gamma_2^{-1}(\gamma_1^{-1}x\beta_1)\beta_2$ , применение которого равносильно последовательному применению операторов, соответствующих элементам  $\lambda_1$  и  $\lambda_2$ . Таким образом, мы задали гомоморфное отображение группы  $G$  на группу вращений четырехмерного пространства. Ядро этого гомоморфизма состоит из таких пар  $(\gamma, \beta)$ , для которых  $\gamma^{-1}x\beta = x$  при всех  $x$ . Положив  $x = 1$ , получим, что  $\gamma = \beta$ . Из  $\beta^{-1}x\beta = x$  при всех  $x$  следует, как мы видели в предыдущем пункте, что  $\beta = \pm 1$ . Итак, ядро состоит из элементов  $(1, 1)$  и  $(-1, -1)$ .

Таким образом, мы доказали следующую теорему.

**Теорема 4.** *Группа  $SO(4)$  собственнo ортогональных преобразований четырехмерного пространства изоморфна факторгруппе прямого произведения двух групп кватернионов единичного модуля по подгруппе, состоящей из  $(1, 1)$  и  $(-1, -1)$ .*

Заметим еще, что группа  $SO(4)$  содержит циклическую подгруппу второго порядка, образованную операторами  $\pm \mathcal{E}$ , где  $\mathcal{E}$  — тождественный оператор. Факторгруппа  $PSO(4)$  группы  $SO(4)$  по этой подгруппе изоморфна, как легко видеть, прямому произведению двух групп  $SO(3)$ .

Такое разложение группы  $SO(4)$  ставит ее в исключительное положение среди групп  $SO(n)$ . Именно, все группы  $SO(n)$  при нечетном  $n \geq 3$  простые и факторгруппы  $PSO(n)$  групп  $SO(n)$  по подгруппе  $\{\pm \mathcal{E}\}$  при четном  $n \geq 6$  тоже простые.

Установленное разложение группы  $SO(4)$  показывает, что в ней имеются два замечательных нормальных делителя, соответствующих операторам правого и левого умножения в алгебре кватернионов. Интересно охарактеризовать эти группы в терминах самой группы  $SO(4)$ . Это нетрудно сделать. Выше мы видели, что каждый оператор правого умножения и каждый оператор левого умножения имеет в некотором ортонормальном базисе матрицу, состоящую из двух одинаковых блоков второго порядка. Оказывается, что этим свойством вполне характеризуются элементы  $SO(4)$ , допускающие реализацию в виде оператора правого или левого умножения. Действительно, пусть оператор  $\mathcal{A} \neq \pm \mathcal{E}$  обладает этим свойством. Тогда  $\mathcal{A}^2 - 2 \cos \varphi \mathcal{A} + 1 = 0$ , ибо этому

уравнению удовлетворяют оба блока. Отсюда следует, что каков бы ни был вектор  $x$ , векторы  $x$  и  $\mathcal{A}x$  линейно независимы, порождают инвариантное двумерное подпространство и ортогональное дополнение к нему тоже инвариантно. Пусть  $\mathcal{A}$  действует в пространстве алгебры кватернионов и пусть  $\beta = \mathcal{A}(1)$ . Кватернион  $\beta$  будет иметь единичный модуль и будет отличаться от  $\pm 1$ , ибо  $1$  и  $\beta$  линейно независимы. Положим  $\beta = \cos \varphi + u \sin \varphi$ . Пусть  $v$  — какой-либо вектор, ортогональный векторам  $u$  и  $w = uv$ . Тогда либо в базисе  $1, u, v, w$ , либо в базисе  $1, u, w, v$  матрица оператора  $\mathcal{A}$  будет состоять из двух равных блоков. В первом случае  $\mathcal{A}$  есть оператор левого умножения на  $\beta$ , во втором — правого. Итак, мы получили следующее.

1. Элементы  $SO(4)$ , имеющие в некотором ортонормальном базисе матрицу, состоящую из двух равных блоков второго порядка, разбиваются на два класса в зависимости от ориентации этого базиса. Эти два класса имеют общими элементами лишь  $\pm \mathcal{E}$ .
  2. Элементы каждого класса образуют группу по умножению.
  3. Элементы из разных классов коммутируют.
- Прямое доказательство этих утверждений без обращения к алгебре кватернионов не просто.

### § 3. Внешняя алгебра

**1. Определение внешней алгебры.** Под названием *внешней алгебры* известна ассоциативная алгебра, введение которой, в частности, полезно при построении теории интегрирования в многомерных пространствах. Внешняя алгебра (над данным полем  $K$ ) строится, если задано некоторое векторное пространство над тем же полем. Элементами внешней алгебры являются формальные «внешние» произведения векторов, причем попарное умножение векторов считается антикоммутативным. Никаких соотношений, кроме тех, которые следуют из дистрибутивности, ассоциативности и антикоммутативности, при умножении векторов не предполагается. Строже определение внешней алгебры можно дать различными способами. Мы дадим следующее формальное определение.

Пусть  $N = \{1, 2, \dots, n\}$  — множество чисел, составляющее отрезок натурального ряда  $\mathbb{N}$ . Символами  $\Gamma, \Gamma_1, \Gamma_2, \dots$  будем обозначать подмножества множества  $N$ , включая само  $N$  и пустое множество  $\emptyset$ . Каждому  $\Gamma \subset N$  сопоставим базисный элемент  $e_\Gamma$  внешней алгебры. Тем самым размерность конструируемой алгебры равна числу подмножеств множества  $N$ , т. е.  $2^n$ . Действие умножения во внешней алгебре обозначается знаком  $\wedge$ . Для базисных элементов оно задается следующим образом:

1. Если  $\Gamma_1 \cap \Gamma_2 \neq \emptyset$ , то  $e_{\Gamma_1} \wedge e_{\Gamma_2} = 0$ .
2. Если  $\Gamma_1 \cap \Gamma_2 = \emptyset$ , то  $e_{\Gamma_1} \wedge e_{\Gamma_2} = (-1)^{\text{inv}(\Gamma_1, \Gamma_2)} e_{\Gamma_1 \cup \Gamma_2}$ .

Здесь  $\text{inv}(\Gamma_1, \Gamma_2)$  обозначает число инверсий, которое образуют числа, составляющие  $\Gamma_1$ , с числами, составляющими  $\Gamma_2$ .

**2. Ассоциативность.** Докажем ассоциативность умножения во внешней алгебре. Пусть  $\Gamma_1, \Gamma_2$  и  $\Gamma_3$  — три подмножества множества  $N$ . Нам нужно доказать, что  $(e_{\Gamma_1} \wedge e_{\Gamma_2}) \wedge e_{\Gamma_3} = e_{\Gamma_1} \wedge (e_{\Gamma_2} \wedge e_{\Gamma_3})$ .

Допустим сначала, что хотя бы одно из множеств  $\Gamma_1 \cap \Gamma_2, \Gamma_1 \cap \Gamma_3, \Gamma_2 \cap \Gamma_3$  непусто. В этом случае обе части равенства равны нулю. Действительно, левая часть равна нулю, ибо непусто либо  $\Gamma_1 \cap \Gamma_2$ , либо  $(\Gamma_1 \cup \Gamma_2) \cap \Gamma_3$ . Аналогично, правая часть равна нулю, ибо непусто либо  $\Gamma_2 \cap \Gamma_3$ , либо  $\Gamma_1 \cap (\Gamma_2 \cup \Gamma_3)$ .

Теперь допустим, что  $\Gamma_1 \cap \Gamma_2 = \Gamma_1 \cap \Gamma_3 = \Gamma_2 \cap \Gamma_3 = \emptyset$ . Имеем

$$\begin{aligned} (e_{\Gamma_1} \wedge e_{\Gamma_2}) \wedge e_{\Gamma_3} &= (-1)^{\text{inv}(\Gamma_1, \Gamma_2)} e_{\Gamma_1 \cup \Gamma_2} \wedge e_{\Gamma_3} = \\ &= (-1)^{\text{inv}(\Gamma_1, \Gamma_2) + \text{inv}(\Gamma_1 \cup \Gamma_2, \Gamma_3)} e_{\Gamma_1 \cup \Gamma_2 \cup \Gamma_3}; \\ e_{\Gamma_1} \wedge (e_{\Gamma_2} \wedge e_{\Gamma_3}) &= (-1)^{\text{inv}(\Gamma_2, \Gamma_3)} e_{\Gamma_1} \wedge e_{\Gamma_2 \cup \Gamma_3} = \\ &= (-1)^{\text{inv}(\Gamma_2, \Gamma_3) + \text{inv}(\Gamma_1, \Gamma_2 \cup \Gamma_3)} e_{\Gamma_1 \cup \Gamma_2 \cup \Gamma_3}. \end{aligned}$$

Но  $\text{inv}(\Gamma_1 \cup \Gamma_2, \Gamma_3) = \text{inv}(\Gamma_1, \Gamma_3) + \text{inv}(\Gamma_2, \Gamma_3)$  и  $\text{inv}(\Gamma_1, \Gamma_2 \cup \Gamma_3) = \text{inv}(\Gamma_1, \Gamma_2) + \text{inv}(\Gamma_1, \Gamma_3)$ . Поэтому  $(e_{\Gamma_1} \wedge e_{\Gamma_2}) \wedge e_{\Gamma_3} = e_{\Gamma_1} \wedge (e_{\Gamma_2} \wedge e_{\Gamma_3})$ .

**3. Градуировка.** Степенью базисного элемента  $e_{\Gamma}$  внешней алгебры называется число элементов, составляющих  $\Gamma$ . Элемент  $\sum_{\Gamma} a_{\Gamma} e_{\Gamma}$  называется однородным, если все базисные элементы, входящие с ненулевыми коэффициентами, имеют одинаковую степень. Эта степень называется степенью однородного элемента. Нулевой элемент алгебры причисляется к однородным элементам любой степени. Ясно, что однородные элементы фиксированной степени  $k$  образуют линейное подпространство в пространстве внешней алгебры, и его размерность равна числу  $k$ -элементных подмножеств множества  $N$ , т. е. числу сочетаний  $C_n^k$ . Ясно также, что произведение двух однородных элементов есть однородный элемент, степень которого равна сумме степеней сомножителей, если эта сумма не превышает  $n$ . Если же сумма степеней двух однородных элементов больше  $n$ , то их произведение равно нулю, ибо в этом случае подмножества, индексирующие любую пару базисных элементов, входящих в сомножители, имеют непустое пересечение.

Разложение внешней алгебры в прямую сумму подпространств однородных элементов называется ее градуировкой.

Вообще, алгебра конечной или бесконечной размерности называется *градуированной*, если она может быть разложена в прямую сумму подпространств  $U_k, k = 0, 1, 2, \dots$ , причем если  $x \in U_k, y \in U_l$ , то  $xy \in U_{k+l}$ . Разумеется, если градуированная алгебра имеет конечную размерность, то пространства  $U_k$  при достаточно больших  $k$  состоят только из 0. Примером градуированной алгебры может служить алгебра многочленов от одной или нескольких переменных. Эта алгебра имеет бесконечную размерность.

Элементы внешней алгебры нулевой степени являются кратными элементом  $e_{\emptyset}$ , который, очевидно, есть единица внешней алгебры. Поэтому элементы нулевой степени естественно отожде-

ставить с элементами основного поля и называть *скалярами*. Элементы первой степени образуют  $n$ -мерное пространство, натянутое на базисные векторы  $e_1, e_2, \dots, e_n$  (мы обозначаем одноэлементные множества  $\{1\}, \dots, \{n\}$  просто  $1, \dots, n$ , что здесь не приведет к недоразумению). Элементы первой степени будем называть *векторами* и образованное ими пространство считать пространством, над которым построена внешняя алгебра.

Однородные элементы степени 2 называются *бивекторами*, степени 3 — *тривекторами* и т. д.; общий термин — *поливекторы*.

Как уже было сказано, пространство  $r$ -векторов имеет размерность  $C_n^r$ . В частности, пространство  $n$ -векторов одномерно, его элементы имеют вид  $se_n$  при  $s \in K$ ; пространство  $(n-1)$ -векторов  $n$ -мерно, и вообще, пространства  $r$ -векторов и  $(n-r)$ -векторов имеют одинаковую размерность. Из определения произведения ясно, что  $e_\Gamma = e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}$ , если  $\Gamma = \{i_1, i_2, \dots, i_r\}$  и  $i_1 < i_2 < \dots < i_r$ . Поэтому общий вид  $r$ -вектора есть

$$\sum_{i_1 < i_2 < \dots < i_r} c^{i_1 i_2 \dots i_r} e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}.$$

Если  $(j_1, j_2, \dots, j_r)$  — какая-либо перестановка чисел  $i_1, i_2, \dots, i_r$ , то  $e_{j_1} \wedge e_{j_2} \wedge \dots \wedge e_{j_r} = (-1)^{\text{inv}(j_1, j_2, \dots, j_r)} e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}$ .

Выписав индексы  $i_1, i_2, \dots, i_r$  во всех возможных порядках и положив  $b^{i_1 i_2 \dots i_r} = \frac{1}{r!} (-1)^{\text{inv}(j_1, j_2, \dots, j_r)} c^{i_1 i_2 \dots i_r}$ , получим запись  $r$ -вектора в тензорной форме:  $b^{i_1 i_2 \dots i_r} e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}$ . Совокупность коэффициентов  $b^{i_1 i_2 \dots i_r}$  составляет антисимметричный контравариантный тензор.

#### 4. Свойства внешнего умножения векторов.

Предложение 1. Пусть  $f$  — вектор. Тогда  $f \wedge f = 0$ .

Действительно, если  $f = a_1 e_1 + a_2 e_2 + \dots + a_n e_n$ , то  $f \wedge f = \sum_{i=1}^n \sum_{j=1}^n a_i a_j (e_i \wedge e_j) = \sum_{j=1}^n a_j^2 (e_j \wedge e_j) + \sum_{i < j} a_i a_j (e_i \wedge e_j + e_j \wedge e_i) = 0$ , ибо  $e_i \wedge e_i = 0$ ,  $e_i \wedge e_j = e_{\{i, j\}}$  и  $e_j \wedge e_i = -e_{\{i, j\}}$  при  $i < j$ .

Предложение 2. Пусть  $f_1$  и  $f_2$  — два вектора. Тогда  $f_1 \wedge f_2 = -f_2 \wedge f_1$ .

Действительно,  $0 = (f_1 + f_2) \wedge (f_1 + f_2) = f_1 \wedge f_1 + f_1 \wedge f_2 + f_2 \wedge f_1 + f_2 \wedge f_2 = f_1 \wedge f_2 + f_2 \wedge f_1$ .

Предложение 3. Если во внешнем произведении  $f_1 \wedge \dots \wedge f_k$  имеется хотя бы одна пара равных сомножителей, то оно равно нулю.

Действительно, попарно переставляя соседние множители, добьемся того, чтобы равные оказались рядом.

Предложение 4. Пусть  $f_1, f_2, \dots, f_k$  — векторы и  $(\alpha_1, \alpha_2, \dots, \alpha_k)$  — перестановка чисел  $1, 2, \dots, k$ . Тогда  $f_{\alpha_1} \wedge f_{\alpha_2} \wedge \dots \wedge f_{\alpha_k} = (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_k)} f_1 \wedge f_2 \wedge \dots \wedge f_k$ .

**Доказательство.** От расположения  $f_{\alpha_1}, f_{\alpha_2}, \dots, f_{\alpha_k}$  можно перейти к расположению  $f_1, f_2, \dots, f_k$  посредством транспозиций соседних элементов. При каждой такой транспозиции меняется знак внешнего произведения. Четность или нечетность числа нужных транспозиций совпадает с четностью или нечетностью числа инверсий  $\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_k)$ , что и доказывает предложение.

Пусть теперь даны векторы  $f_1, f_2, \dots, f_m$ ,  $m \leq n$ , и пусть  $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_k\}$  — подмножество множества  $\{1, 2, \dots, m\}$ . Будем считать, что  $\gamma_1 < \gamma_2 < \dots < \gamma_k$ . Внешнее произведение  $f_{\gamma_1} \wedge f_{\gamma_2} \wedge \dots \wedge f_{\gamma_k}$  назовем стандартным (по отношению к выбранной нумерации векторов  $f_1, f_2, \dots, f_m$ ) и обозначим через  $F_\Gamma$ . Ясно, что если индексы  $\alpha_1, \alpha_2, \dots, \alpha_k$  составляют множество  $\Gamma$ , так что лишь порядком отличаются от  $\gamma_1, \gamma_2, \dots, \gamma_k$ , то  $f_{\alpha_1} \wedge f_{\alpha_2} \wedge \dots \wedge f_{\alpha_k} = (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_k)} F_\Gamma$ . Это следует из предложения 4.

**Предложение 5.**  $F_{\Gamma_1} \wedge F_{\Gamma_2} = 0$ , если  $\Gamma_1 \cap \Gamma_2 \neq \emptyset$ , и  $F_{\Gamma_1} \wedge F_{\Gamma_2} = (-1)^{\text{inv}(\Gamma_1, \Gamma_2)} F_{\Gamma_1 \cup \Gamma_2}$ , если  $\Gamma_1 \cap \Gamma_2 = \emptyset$ .

**Доказательство.** Пусть  $\Gamma_1 = \{\gamma_1, \dots, \gamma_k\}$ ,  $\gamma_1 < \gamma_2 < \dots < \gamma_k$ , и  $\Gamma_2 = \{\gamma_{k+1}, \dots, \gamma_l\}$ ,  $\gamma_{k+1} < \dots < \gamma_l$ . Тогда  $F_{\Gamma_1} \wedge F_{\Gamma_2} = f_{\gamma_1} \wedge f_{\gamma_2} \wedge \dots \wedge f_{\gamma_k} \wedge f_{\gamma_{k+1}} \wedge \dots \wedge f_{\gamma_l}$ . Если  $\Gamma_1 \cap \Gamma_2 \neq \emptyset$ , то среди множителей в последнем произведении найдутся равные, и произведение равно 0. Если же  $\Gamma_1 \cap \Gamma_2 = \emptyset$ , то

$$F_{\Gamma_1} \wedge F_{\Gamma_2} = (-1)^{\text{inv}(\gamma_1, \gamma_2, \dots, \gamma_k, \gamma_{k+1}, \dots, \gamma_l)} F_{\Gamma_1 \cup \Gamma_2} = (-1)^{\text{inv}(\Gamma_1, \Gamma_2)} F_{\Gamma_1 \cup \Gamma_2},$$

ибо  $\text{inv}(\gamma_1, \gamma_2, \dots, \gamma_k, \gamma_{k+1}, \dots, \gamma_l) = \text{inv}(\Gamma_1, \Gamma_2)$ .

**5. Автоморфизмы внешней алгебры.** Пусть векторы  $f_1, \dots, f_n$  линейно независимы и число их равно размерности пространства векторов, так что они образуют базис. Докажем, что элементы  $F_\Gamma$ , когда  $\Gamma$  пробегает все подмножества множества  $N = \{1, \dots, n\}$ , составляют базис внешней алгебры. Число элементов  $F_\Gamma$  равно, очевидно, размерности внешней алгебры, так что нам достаточно показать, что элементы  $F_\Gamma$  порождают внешнюю алгебру как векторное пространство. Но это почти очевидно — исходные базисные элементы  $e_1, \dots, e_n$  являются линейными комбинациями  $f_1, \dots, f_n$ , и, следовательно, при любом  $\Gamma \subset N$ ,  $e_\Gamma = e_{\gamma_1} \wedge e_{\gamma_2} \wedge \dots \wedge e_{\gamma_k}$  есть линейная комбинация внешних произведений векторов  $f_1, \dots, f_n$ , взятых по  $K$ . Все такие произведения либо равны нулю, либо с точностью до знаков являются стандартными произведениями. Таким образом, стандартные произведения  $F_\Gamma$  порождают в виде линейной комбинации все базисные элементы  $e_\Gamma$  внешней алгебры, а значит, и все элементы внешней алгебры являются их линейными комбинациями, что и требовалось доказать.

Заметим, что из приведенного рассуждения следует линейная независимость всех  $2^n$  стандартных произведений  $F_\Gamma$  и, в частности, неравенство нулю каждого из них.

Итак, наряду с исходной системой базисных элементов  $\{e_\Gamma | \Gamma \subset N\}$  внешней алгебры можно взять в качестве базиса любую систему  $\{F_\Gamma | \Gamma \subset N\}$ , где  $F_\Gamma$  — стандартные произведения, построенные, исходя из какого-либо базиса  $f_1, \dots, f_n$  пространства векторов. В силу предложения 5 таблицы умножения для  $\{F_\Gamma | \Gamma \subset N\}$  и  $\{e_\Gamma | \Gamma \subset N\}$  одинаковы, т. е. переход от базиса  $\{e_\Gamma\}$  к базису  $\{F_\Gamma\}$  есть автоморфизм внешней алгебры. Сами элементы  $e_\Gamma$  и  $F_\Gamma$  получаются из нумерованных базисов  $e_1, \dots, e_n$  и  $f_1, \dots, f_n$  пространства векторов одинаковым способом — посредством составления стандартных произведений для каждого  $\Gamma \subset N$ .

**6. Условие линейной независимости векторов в терминах внешней алгебры.**

**Теорема 6.** *Для того чтобы система векторов  $f_1, f_2, \dots, f_k$  была линейно независимой, необходимо и достаточно, чтобы  $f_1 \wedge f_2 \wedge \dots \wedge f_k \neq 0$ .*

**Доказательство.** Пусть система  $f_1, f_2, \dots, f_k$  линейно зависима. Тогда ее можно дополнить до базиса  $f_1, f_2, \dots, f_k, f_{k+1}, \dots, f_n$ . В силу сказанного в п. 5 стандартные произведения  $f_{\gamma_1} \wedge f_{\gamma_2} \wedge \dots \wedge f_{\gamma_k}$ ,  $\gamma_1 < \dots < \gamma_k$ , все отличны от нуля, в частности,  $f_1 \wedge f_2 \wedge \dots \wedge f_k \neq 0$ .

Если же система  $f_1, f_2, \dots, f_k$  линейно зависима, то один из ее векторов  $f_j$  есть линейная комбинация остальных:  $f_1, \dots, f_{j-1}, f_{j+1}, \dots, f_k$  и произведение  $f_1 \wedge \dots \wedge f_k = f_1 \wedge \dots \wedge f_{j-1} \wedge \wedge (c_1 f_1 + \dots + c_{j-1} f_{j-1} + c_{j+1} f_{j+1} + \dots + c_k f_k) \wedge f_{j+1} \wedge \dots \wedge f_k$  есть линейная комбинация внешних произведений, в каждом из которых имеется пара равных сомножителей. Все они равны нулю. Тем самым теорема доказана.

**7. Внешнее произведение  $n$  векторов.** Пусть  $f_1, \dots, f_n$  — система из  $n$  векторов в пространстве с базисом  $e_1, \dots, e_n$ :

$$\begin{aligned} f_1 &= a_{11}e_1 + a_{12}e_2 + \dots + a_{1n}e_n, \\ f_2 &= a_{21}e_1 + a_{22}e_2 + \dots + a_{2n}e_n, \\ &\vdots \\ f_n &= a_{n1}e_1 + a_{n2}e_2 + \dots + a_{nn}e_n. \end{aligned}$$

Матрицу коэффициентов  $(a_{ij})$  обозначим через  $A$ .

Рассмотрим  $f_1 \wedge f_2 \wedge \dots \wedge f_n$ . Из предыдущего ясно, что это произведение есть однородный элемент степени  $n$ , и, следовательно, лишь множителем  $\alpha$  отличается от  $e_N = e_1 \wedge e_2 \wedge \dots \wedge e_n$ . Из свойств внешних произведений мы можем без вычислений сказать о некоторых свойствах этого множителя. Из дистрибутивности внешнего умножения следует, что этот множитель есть линейная функция от каждого из сомножителей, т. е. линейная функция от элементов каждой строки матрицы  $A$ . Далее, этот множитель меняет знак при перестановке двух сомножителей, т. е. при перестановке двух строк матрицы. Наконец, если матрица  $A$  единичная, т. е.  $f_j = e_j$ ,  $j = 1, 2, \dots, n$ , то множитель  $\alpha$  равен 1. Мы знаем,

что этими свойствами обладает определитель матрицы  $A$ , и, более того, можно показать, что определитель характеризуется этими свойствами. Таким образом, должна быть верна формула:

$$f_1 \wedge f_2 \wedge \dots \wedge f_n = \det A e_1 \wedge e_2 \wedge \dots \wedge e_n. \quad (1)$$

Убедимся в этом прямым вычислением. Имеем

$$f_1 \wedge f_2 \wedge \dots \wedge f_n = \sum_{\alpha_1, \dots, \alpha_n=1}^n a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n} e_{\alpha_1} \wedge e_{\alpha_2} \wedge \dots \wedge e_{\alpha_n}.$$

Здесь индексы  $\alpha_1, \alpha_2, \dots, \alpha_n$  независимо пробегает значения  $1, 2, \dots, n$ . Значительная часть слагаемых в правой части равна нулю. Именно, это будет, если среди значений индексов  $\alpha_1, \alpha_2, \dots, \alpha_n$  встретится хотя бы пара равных. Если же значения  $\alpha_1, \alpha_2, \dots, \alpha_n$  попарно различны, то они образуют перестановку чисел  $1, 2, \dots, n$ , и тогда

$$e_{\alpha_1} \wedge e_{\alpha_2} \wedge \dots \wedge e_{\alpha_n} = (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)} e_1 \wedge e_2 \wedge \dots \wedge e_n.$$

Итак,

$$\begin{aligned} f_1 \wedge f_2 \wedge \dots \wedge f_n &= \\ &= \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (-1)^{\text{inv}(\alpha_1, \alpha_2, \dots, \alpha_n)} a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n} e_1 \wedge e_2 \wedge \dots \wedge e_n = \\ &= \det A e_1 \wedge e_2 \wedge \dots \wedge e_n, \end{aligned}$$

согласно определению определителя (под знаком суммы  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  пробегает все перестановки чисел  $1, 2, \dots, n$ ).

Заметим, что если базисные векторы  $e_1, e_2, \dots, e_n$  заменить на любую систему векторов  $g_1, g_2, \dots, g_n$  (быть может, зависимую), то в силу п. 4 все вычисления сохраняются, так что если

$$\begin{aligned} f_1 &= a_{11}g_1 + \dots + a_{1n}g_n, \\ &\vdots \\ f_n &= a_{n1}g_1 + \dots + a_{nn}g_n, \end{aligned}$$

где  $g_1, g_2, \dots, g_n$  — любая система векторов, то  $f_1 \wedge \dots \wedge f_n = \det A g_1 \wedge \dots \wedge g_n$ , где  $A = (a_{ij})$ .

Выведем теперь в качестве следствий из формулы (1) некоторые свойства определителей, ранее полученные другими средствами.

**Следствие 1.** Для того чтобы векторы  $f_1, \dots, f_n$  были линейно независимы, необходимо и достаточно, чтобы  $\det A \neq 0$ .

Для этого заключения достаточно сопоставить формулу (1) с теоремой 6.

**Следствие 2** (теорема об определителе произведения двух квадратных матриц). Пусть

$$\begin{aligned} f_1 &= b_{11}g_1 + \dots + b_{1n}g_n, & g_1 &= c_{11}e_1 + \dots + c_{1n}e_n, \\ f_2 &= b_{21}g_1 + \dots + b_{2n}g_n, & g_2 &= c_{21}e_1 + \dots + c_{2n}e_n, \\ &\vdots & &\vdots \\ f_n &= b_{n1}g_1 + \dots + b_{nn}g_n, & g_n &= c_{n1}e_1 + \dots + c_{nn}e_n, \end{aligned} \quad \text{и}$$





$$= \sum_{\Gamma} \left( \sum_{(a_1, \dots, a_k)} (-1)^{\text{inv}(a_1, \dots, a_k)} a_{1a_1} \dots a_{ka_k} \right) G_{\Gamma} = \sum_{\Gamma} A_{\Gamma} G_{\Gamma}, \text{ так как}$$

$$\sum_{(a_1, \dots, a_k)} (-1)^{\text{inv}(a_1, \dots, a_k)} a_{1a_1} \dots a_{ka_k} = \begin{vmatrix} a_{1\gamma_1} & \dots & a_{1\gamma_k} \\ \dots & \dots & \dots \\ a_{k\gamma_1} & \dots & a_{k\gamma_k} \end{vmatrix} = A_{\Gamma} \text{ согла-}$$

сно определению определителя.

Заметим еще, что если  $f_1 = a_{11}g_1 + \dots + a_{1m}g_m, \dots, f_k = a_{k1}g_1 + \dots + a_{km}g_m$  и  $k > m$ , то  $f_1 \wedge \dots \wedge f_k = 0$ , ибо в этой ситуации векторы  $f_1, \dots, f_k$  образуют линейно зависимую систему. В том же легко убедиться и формальной проверкой — в выражении  $f_1 \wedge \dots \wedge f_k$  через внешние произведения  $g_1, \dots, g_m$  мы в каждом слагаемом будем встречаться с равными множителями.

Из доказанной формулы легко выводятся еще некоторые свойства определителей.

Следствие 4 (теорема Бине — Коши об определителе произведения двух прямоугольных матриц). Пусть

$$A = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \dots & \dots & \dots \\ b_{k1} & \dots & b_{km} \end{pmatrix}, \quad C = \begin{pmatrix} c_{11} & \dots & c_{1k} \\ \dots & \dots & \dots \\ c_{m1} & \dots & c_{mk} \end{pmatrix},$$

где  $A = BC$ , причем  $k < m$ . Пусть  $\Gamma = \{\gamma_1, \dots, \gamma_k\}$ , где  $\gamma_1 < \gamma_2 < \dots < \gamma_k$ . Положим

$$B_{\Gamma} = \begin{vmatrix} b_{1\gamma_1} & \dots & b_{1\gamma_k} \\ \dots & \dots & \dots \\ b_{k\gamma_1} & \dots & b_{k\gamma_k} \end{vmatrix} \quad \text{и} \quad C^{\Gamma} = \begin{vmatrix} c_{\gamma_1 1} & \dots & c_{\gamma_1 k} \\ \dots & \dots & \dots \\ c_{\gamma_k 1} & \dots & c_{\gamma_k k} \end{vmatrix}.$$

Тогда  $\det A = \sum_{\Gamma} B_{\Gamma} C^{\Gamma}$ , где сумма распространена на все  $k$ -элементные подмножества множества  $M = \{1, 2, \dots, m\}$ .

Доказательство. Пусть

$$\begin{aligned} f_1 &= b_{11}g_1 + \dots + b_{1m}g_m, & g_1 &= c_{11}e_1 + \dots + c_{1k}e_k, \\ &\dots & &\dots \\ f_k &= b_{k1}g_1 + \dots + b_{km}g_m, & g_m &= c_{m1}e_1 + \dots + c_{mk}e_k, \end{aligned}$$

причем  $e_1, \dots, e_k$  линейно независимы. Тогда

$$\begin{aligned} f_1 &= a_{11}e_1 + \dots + a_{1k}e_k, \\ &\dots \\ f_k &= a_{k1}e_1 + \dots + a_{kk}e_k. \end{aligned}$$

Поэтому, с одной стороны,  $f_1 \wedge \dots \wedge f_k = \det A e_1 \wedge \dots \wedge e_k$ , с другой стороны,  $f_1 \wedge f_2 \wedge \dots \wedge f_k = \sum_{\Gamma} B_{\Gamma} g_{\gamma_1} \wedge g_{\gamma_2} \wedge \dots \wedge g_{\gamma_k}$ .



пробегают все  $k$ -элементные подмножества, а  $\Delta$  — все  $(n-k)$ -элементные подмножества множества  $N$ . Ясно, что  $e_\Gamma \wedge e_\Delta = 0$ , если  $\Gamma \cap \Delta$  непусто, а пусто оно, только если  $\Delta = \Gamma'$ . Следовательно,

$$\det A e_N = f_1 \wedge \dots \wedge f_n = \sum_{\Gamma} \sum_{\Delta} A_{1\Gamma} A_{2\Delta} e_\Gamma \wedge e_\Delta =$$

$$= \sum_{\Gamma} A_{1\Gamma} A_{2\Gamma'} e_\Gamma \wedge e_{\Gamma'} = \sum_{\Gamma} A_{1\Gamma} A_{2\Gamma'} (-1)^{\text{inv}(\Gamma, \Gamma')} e_N.$$

Пусть  $\Gamma = \{\gamma_1, \dots, \gamma_k\}$  и  $\gamma_1 < \gamma_2 < \dots < \gamma_k$ . Все элементы, меньшие, чем  $\gamma_1$ , находятся в  $\Gamma'$ , поэтому  $\gamma_1$  составляет  $\gamma_1 - 1$  инверсий с элементами из  $\Gamma'$ , далее, все элементы, меньшие, чем  $\gamma_2$ , кроме  $\gamma_1$ , находятся в  $\Gamma'$ , так что  $\gamma_2$  составляет  $\gamma_2 - 2$  инверсий с элементами из  $\Gamma'$  и т. д. Таким образом,  $\text{inv}(\Gamma, \Gamma') = \gamma_1 + \dots + \gamma_k - 1 - \dots - k = \gamma_1 + \dots + \gamma_k - \frac{1}{2}k(k+1)$ . Итак,  $\det A = \sum_{\Gamma} (-1)^{\gamma_1 + \dots + \gamma_k - \frac{1}{2}k(k+1)} A_{1\Gamma} A_{2\Gamma'}$ , что и требовалось доказать.

Переставляя строки, легко доказать теорему Лапласа в общем случае, когда в матрице  $A$  выбраны любые  $k$  строчек. Мы предоставляем это читателю.

**Следствие 6** (критерий линейной независимости в терминах ранга матрицы). *Для того чтобы векторы  $f_1 = a_{11}e_1 + \dots + a_{1n}e_n, \dots, f_k = a_{k1}e_1 + \dots + a_{kn}e_n$  были линейно независимы, необходимо и достаточно, чтобы хотя бы один минор  $k$ -го порядка матрицы  $A = (a_{ij})$  был отличен от нуля.*

Действительно, для линейной независимости необходимо и достаточно, чтобы  $f_1 \wedge \dots \wedge f_k \neq 0$ . Но  $f_1 \wedge \dots \wedge f_k = \sum_{\Gamma} A_{\Gamma} e_{\Gamma}$ , и для  $f_1 \wedge \dots \wedge f_k \neq 0$  необходимо и достаточно, чтобы хотя бы один из миноров  $A_{\Gamma}$  был отличен от нуля.

**9. Внешняя алгебра над пространством Евклида.** Пусть в пространстве векторов имеется структура евклидова пространства, т. е. основное поле есть поле  $\mathbb{R}$  вещественных чисел и в пространстве определено скалярное произведение. Пусть базис  $e_1, \dots, e_n$ , исходя из которого строится внешняя алгебра, ортонормален. Продолжим евклидову структуру на все пространство внешней алгебры, считая базис  $\{e_{\Gamma}\}$  ортонормальным, так что скалярное произведение элементов  $x = \sum_{\Gamma} x_{\Gamma} e_{\Gamma}$  и  $y = \sum_{\Gamma} y_{\Gamma} e_{\Gamma}$  равно  $\sum_{\Gamma} x_{\Gamma} y_{\Gamma}$ .

При таком соглашении однородные элементы разных степеней будут ортогональны, так что градуировка определяет разложение пространства внешней алгебры в прямую ортогональную сумму подпространств однородных элементов.

**Предложение 8.** Пусть  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  — две системы векторов. Тогда скалярное произведение  $k$ -векторов  $f_1 \wedge \dots \wedge f_k$  и  $g_1 \wedge \dots \wedge g_k$  равно

$$\begin{vmatrix} (f_1, g_1) & (f_1, g_2) & \dots & (f_1, g_k) \\ \dots & \dots & \dots & \dots \\ (f_k, g_1) & (f_k, g_2) & \dots & (f_k, g_k) \end{vmatrix}.$$

В частности, квадрат длины  $k$ -вектора  $f_1 \wedge \dots \wedge f_k$  равен определителю Грама  $\begin{vmatrix} (f_1, f_1) & \dots & (f_1, f_k) \\ \vdots & \ddots & \vdots \\ (f_k, f_1) & \dots & (f_k, f_k) \end{vmatrix}$ , т. е. совпадает с квадратом объема параллелепипеда, натянутого на векторы  $f_1, \dots, f_k$ .

Доказательство. Пусть

$$\begin{aligned} f_1 &= b_{11}e_1 + \dots + b_{1n}e_n, & g_1 &= c_{11}e_1 + \dots + c_{1n}e_n, \\ &\vdots & &\vdots \\ f_k &= b_{k1}e_1 + \dots + b_{kn}e_n, & g_k &= c_{k1}e_1 + \dots + c_{kn}e_n. \end{aligned}$$

Обозначим через  $B_\Gamma$ ,  $C_\Gamma$  миноры, «вырезаемые» множеством  $\Gamma$  из матриц  $B = (b_{ij})$ ,  $C = (c_{ij})$ . Как мы уже знаем,

$$F = f_1 \wedge \dots \wedge f_k = \sum_\Gamma B_\Gamma e_\Gamma, \quad G = g_1 \wedge \dots \wedge g_k = \sum_\Gamma C_\Gamma e_\Gamma.$$

Поэтому  $(F, G) = \sum_\Gamma B_\Gamma C_\Gamma = \det BC^T$  в силу теоремы Бине — Коши ( $C^T$  — транспонированная матрица). Согласно правилу умножения матриц  $BC^T = \begin{pmatrix} b_{11}c_{11} + \dots + b_{1n}c_{1n} & \dots & b_{11}c_{k1} + \dots + b_{1n}c_{kn} \\ \vdots & \ddots & \vdots \\ b_{k1}c_{11} + \dots + b_{kn}c_{1n} & \dots & b_{k1}c_{k1} + \dots + b_{kn}c_{kn} \end{pmatrix} =$   
 $= \begin{pmatrix} (f_1, g_1) & \dots & (f_1, g_k) \\ \vdots & \ddots & \vdots \\ (f_k, g_1) & \dots & (f_k, g_k) \end{pmatrix}$ , что и требовалось доказать.

Чтобы получить частный случай, включенный в формулировку предложения, достаточно положить  $g_1 = f_1, \dots, g_k = f_k$ .

Заметим, что скалярное произведение  $(F, G)$   $k$ -векторов зависит лишь от скалярных произведений  $(f_i, g_i)$ , т. е. от взаимного расположения этих двух систем векторов друг относительно друга, но не от выбора системы координат. В частности, отсюда следует, что если  $f_1, \dots, f_n$  — ортонормальный базис исходного пространства и  $\{F_\Gamma\}$  — стандартные произведения базисных элементов, то для двух  $k$ -элементных подмножеств  $\Gamma_1$  и  $\Gamma_2$

$$(F_{\Gamma_1}, F_{\Gamma_2}) = (e_{\Gamma_1}, e_{\Gamma_2}) = \begin{cases} 0, & \text{если } \Gamma_1 \neq \Gamma_2, \\ 1, & \text{если } \Gamma_1 = \Gamma_2, \end{cases}$$

ибо скалярные произведения векторов, составляющих  $F_{\Gamma_1}$  и  $F_{\Gamma_2}$ , равны соответствующим скалярным произведениям векторов, составляющих  $e_{\Gamma_1}$  и  $e_{\Gamma_2}$ .

Таким образом, ортогональное преобразование координат в пространстве векторов вызывает ортогональные преобразования во всех пространствах  $k$ -векторов, а следовательно, и во всем пространстве внешней алгебры, ибо оно разлагается в прямую ортогональную сумму пространств поливекторов.

**10. Внешнее произведение векторов как направленный объем.** Пусть задана упорядоченная система линейно независимых векто-

ров  $f_1, \dots, f_k$  в  $n$ -мерном евклидовом пространстве  $\mathbb{R}^n$ . Напомним, что объем параллелепипеда, натянутого на эту систему, равен квадратному корню из определителя Грама:  $V^2(f_1, \dots, f_k) = \det((f_i, f_j))$ . Если  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  — два базиса некоторого

$k$ -мерного подпространства  $P$  в  $\mathbb{R}^n$  и  $g_i = \sum_{j=1}^k c_{ij} f_j$ ,  $i = 1, 2, \dots, k$ , то  $V(g_1, \dots, g_k) = |\det(c_{ij})| V(f_1, \dots, f_k)$ . Если  $\det(c_{ij}) > 0$ , системы  $g_1, \dots, g_k$  и  $f_1, \dots, f_k$  одинаково ориентированы, если же  $\det(c_{ij}) < 0$ , то их ориентации противоположны. Напомним, что если  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  одинаково ориентированы, то существует непрерывный путь, соединяющий две эти системы, т. е. существует система векторов  $h_1(t), \dots, h_k(t)$ , непрерывно зависящая от вещественного параметра  $t$ ,  $0 \leq t \leq 1$ , и такая, что  $h_i(0) = f_i$ ,  $h_i(1) = g_i$  и при любом  $t$  из промежутка  $0 < t < 1$  система векторов  $h_1(t), \dots, h_k(t)$  остается базисом подпространства  $P$ . Если же  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  имеют противоположную ориентацию, то такого пути не существует.

Теперь докажем теорему, вскрывающую геометрическое значение внешнего умножения векторов.

**Теорема 9.** Пусть  $f_1, \dots, f_k$  — линейно независимая система векторов в  $n$ -мерном евклидовом пространстве  $\mathbb{R}^n$ , и пусть  $g_1, \dots, g_k$  — другая система векторов. Для того чтобы имело место равенство

$$f_1 \wedge f_2 \wedge \dots \wedge f_k = g_1 \wedge g_2 \wedge \dots \wedge g_k, \quad (3)$$

необходимо и достаточно, чтобы системы  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  порождали одно и то же подпространство в  $\mathbb{R}^n$ , были бы в нем одинаково ориентированы и объемы  $V(f_1, \dots, f_k)$  и  $V(g_1, \dots, g_k)$  были бы равны.

**Доказательство.** Докажем сначала необходимость. Пусть равенство (3) выполнено. Тогда при любом  $i$ ,  $1 \leq i \leq k$ , будет  $f_1 \wedge f_2 \wedge \dots \wedge f_k \wedge g_i = 0$  и, следовательно, система  $f_1, \dots, f_k, g_i$  линейно зависима, откуда в силу независимости  $f_1, \dots, f_k$  сле-

дует, что  $g_i = \sum_{j=1}^k c_{ij} f_j$ ,  $i = 1, 2, \dots, k$ . Тогда  $g_1 \wedge \dots \wedge g_k = \det(c_{ij}) f_1 \wedge \dots \wedge f_k$ , так что  $\det(c_{ij}) = +1$ . Следовательно, системы  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  порождают одно и то же подпространство и одинаково в нем ориентированы. Так как  $V(g_1, \dots, g_k) = |\det(c_{ij})| V(f_1, \dots, f_k)$ , объемы равны.

Докажем теперь достаточность. Пусть  $f_1, \dots, f_k$  и  $g_1, \dots, g_k$  порождают одно и то же подпространство, имеют одинаковые

ориентации и  $V(f_1, \dots, f_k) = V(g_1, \dots, g_k)$ . Тогда  $g_i = \sum_{j=1}^k c_{ij} f_j$ , причем  $\det(c_{ij}) > 0$  и  $|\det(c_{ij})| = 1$ , т. е.  $\det(c_{ij}) = 1$ . Ясно, что  $g_1 \wedge \dots \wedge g_k = \det(c_{ij}) f_1 \wedge \dots \wedge f_k = f_1 \wedge \dots \wedge f_k$ .

Доказанная теорема позволяет трактовать  $f_1 \wedge f_2 \wedge \dots \wedge f_k$  как «направленный объем» параллелепипеда, натянутого на  $f_1, \dots, f_k$ . Действительно, это внешнее произведение определяет как величину объема, так и его «направление», т. е. подпространство, в котором этот объем сосредоточен, и ориентацию в этом подпространстве. В этом смысле внешнее произведение системы векторов обобщает векторное произведение пары векторов в трехмерном пространстве. Напомним, что векторное произведение равно по величине площади параллелограмма, натянутого на пару векторов, а его направление характеризует плоскость, порожденную парой векторов и ориентацию пары на этой плоскости.

**11. Подпространства однородных элементов дополнительных степеней.** Пусть  $S_k$  и  $S_{n-k}$  — подпространства однородных элементов степеней  $k$  и  $n-k$  в пространстве внешней алгебры. Размерности этих подпространств совпадают. Если  $u \in S_k$  и  $v \in S_{n-k}$ , то  $u \wedge v$  принадлежит одномерному подпространству  $S_n$  элементов степеней  $n$ . Пусть  $e_1, \dots, e_n$  — какой-либо базис в  $S_1$ . Тогда  $u \wedge v = a(u, v) e_1 \wedge e_2 \wedge \dots \wedge e_n$ . Ясно, что коэффициент  $a(u, v)$  есть при фиксированном  $v$  линейная функция от  $u$ . Очевидно, что порожденное тем самым отображение  $S_{n-k}$  в пространство  $S_k^*$ , сопряженное с  $S_k$ , линейно и его ядро состоит только из 0. Из совпадения размерностей  $S_{n-k}$  и  $S_k^*$  следует, что это отображение есть изоморфизм. Так определенный изоморфизм пространств  $S_{n-k}$  и  $S_k^*$  зависит от выбора базиса  $e_1, \dots, e_n$ , но зависит «слабо» — он определен с точностью до множителя  $\det(c_{ij})$ , где  $(c_{ij})$  — матрица перехода от исходного базиса к другому. В частности, если  $\det(c_{ij}) = +1$ , то изоморфизм  $S_{n-k}$  и  $S_k^*$  сохраняется при замене базиса  $e_1, \dots, e_n$  на базис  $f_1, \dots, f_n$  при  $f_i = \sum_{j=1}^n c_{ij} e_j$ .

Если за исходный базис в пространстве  $S_k$  взяты элементы  $e_\Gamma = e_{\gamma_1} \wedge \dots \wedge e_{\gamma_k}, \gamma_1 < \dots < \gamma_k$ , то сопряженным базисом в  $S_{n-k}$  будет система элементов  $(-1)^{\text{inv}(\Gamma, \Gamma')} e_{\Gamma'}$ , где  $\Gamma' = N \setminus \Gamma$ , что непосредственно следует из закона умножения во внешней алгебре.

Допустим, что исходное пространство  $S_1$  евклидово и базис  $e_1, e_2, \dots, e_n$  ортонормальный. Тогда пространства  $S_k$  и  $S_{n-k}$ , тоже имеют структуру евклидова пространства при ортонормальных базисах  $\{e_\Gamma\}$  и  $\{e_{\Gamma'}\}$ . Напомним, что для евклидова пространства  $S$  имеется естественный изоморфизм между  $S$  и сопряженным пространством  $S^*$ , именно, образом элемента  $y \in S$  при этом изоморфизме является функционал  $f_y(x) = (x, y)$ . Наличие этого изоморфизма позволяет отождествить  $S$  и  $S^*$ . Эти соображения делают естественным введение следующего понятия. Будем считать, что элемент  $u \in S_k$  квазиравен элементу  $v \in S_{n-k}$  и писать  $u \approx v$ , если  $u$  и  $v$  индуцируют в  $S_k$  одинаковые функционалы, т. е. при любом  $w \in S_k$  имеет место равенство  $w \wedge v = (w, u) e_1 \wedge \dots \wedge e_n$ . Ясно,

что квазиравные  $k$ - и  $(n-k)$ -векторы  $u$  и  $v$  имеют одинаковые координаты в базисах  $\{e_\Gamma\}$  и  $\{(-1)^{\text{Inv}(\Gamma, \Gamma')} e_{\Gamma'}\}$  при  $\Gamma' = N \setminus \Gamma$ . Отношение квазиравенства «почти симметрично», именно, если  $u \approx v$ , то  $v \approx (-1)^{k(n-k)} u$ . Отношение квазиравенства зависит от выбора базиса, но, очевидно, не изменяется при собственно ортогональном преобразовании координат. При несобственно ортогональном преобразовании квазиравные поливекторы превращаются в квазипротивоположные, т. е. если до преобразования было  $u \approx v$ , то после преобразования станет  $u \approx -v$  (конечно, при определении квазиравенства по отношению к новым базисным векторам). Это следует из того, что если  $f_1, \dots, f_n$  получается из  $e_1, \dots, e_n$  несобственно ортогональным преобразованием, то  $f_1 \wedge \dots \wedge f_n = -e_1 \wedge \dots \wedge e_n$ .

Выясним теперь, какой элемент из  $S_{n-k}$  квазиравен внешнему произведению  $g_1 \wedge \dots \wedge g_k \in S_k$  линейно независимых векторов  $g_1, \dots, g_k$ . С этой целью выберем в подпространстве  $P$ , натянутом на  $g_1, \dots, g_k$ , ортонормальный базис  $f_1, \dots, f_k$ , причем так, чтобы ориентации системы векторов  $g_1, \dots, g_k$  и  $f_1, \dots, f_k$  были одинаковы. Тогда  $g_1 \wedge \dots \wedge g_k = V f_1 \wedge \dots \wedge f_k$ , где  $V$  — объем параллелепипеда, натянутого на  $g_1, \dots, g_k$ . Дополним  $f_1, \dots, f_k$  до ортонормального базиса  $f_1, \dots, f_k, f_{k+1}, \dots, f_n$  пространства  $S_1$ , имеющего одинаковую ориентацию с исходным базисом  $e_1, \dots, e_n$ . Тогда, в силу сказанного выше,

$$g_1 \wedge \dots \wedge g_k \approx V f_{k+1} \wedge \dots \wedge f_n.$$

Векторы  $f_{k+1}, \dots, f_n$  составляют базис ортогонального дополнения  $P^\perp$  к подпространству  $P$ . Если в этом пространстве взять любую систему векторов  $h_{k+1}, \dots, h_n$ , имеющих одинаковую ориентацию с  $f_{k+1}, \dots, f_n$  и с объемом параллелепипеда  $V$ , то  $g_1 \wedge \dots \wedge g_k \approx h_{k+1} \wedge \dots \wedge h_n$ . Итак, если векторы  $h_{k+1}, \dots, h_n$  ортогональны векторам  $g_1, \dots, g_k$ , объемы параллелепипедов, натянутых на  $g_1, \dots, g_k$  и  $h_{k+1}, \dots, h_n$ , одинаковы и ориентация системы векторов  $g_1, \dots, g_k, h_{k+1}, \dots, h_n$  совпадает с ориентацией исходного базиса  $e_1, \dots, e_n$ , то  $g_1 \wedge \dots \wedge g_k \approx h_{k+1} \wedge \dots \wedge h_n$ .

Рассмотрим случай  $n = 3$  и  $k = 2$ . В этом случае  $g_1 \wedge g_2 \approx h_3$ , где  $h_3$  — ортогональный к  $g_1$  и  $g_2$  вектор, длина которого равна площади параллелограмма, натянутого на  $g_1, g_2$ , и ориентация  $g_1, g_2, h_3$  совпадает с ориентацией исходного базиса. Таким образом, вектор  $h_3$ , квазиравный бивектору  $g_1 \wedge g_2$  (при  $n = 3$ ), есть не что иное, как векторное произведение  $[g_1, g_2]$ .

Заметим, что квазиравенство  $g_1 \wedge \dots \wedge g_k \approx h_{k+1} \wedge \dots \wedge h_n$  равносильно равенству компонент этих поливекторов по отношению к базисам  $\{e_\Gamma\}$  и  $\{(-1)^{\text{Inv}(\Gamma, \Gamma')} e_{\Gamma'}\}$  при  $\Gamma' = N \setminus \Gamma$ . Это равенство может быть сформулировано как равенство миноров  $k$ -го порядка, составленных из первых  $k$  столбцов матрицы координат векторов  $g_1, \dots, g_k, h_{k+1}, \dots, h_n$ , их алгебраическим дополнениям. Формальная проверка таких соотношений не совсем тривиальна.

## СПИСОК ЛИТЕРАТУРЫ

- Архангельский А. В. Конечномерные векторные пространства. — М.: Изд-во МГУ, 1982.
- Боревич З. И. Определители и матрицы. — М.: Наука, 1970.
- Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1979.
- Гельфанд И. М. Лекции по линейной алгебре. — М.: Наука, 1971.
- Кострикин А. И. Введение в алгебру. — М.: Наука, 1977.
- Кострикин А. И. и Манин Ю. И. Линейная алгебра и геометрия. — М.: Изд-во МГУ, 1980.
- Курош А. Г. Курс высшей алгебры. — М.: Наука, 1975.
- Ленг С. Алгебра. — М.: Мир, 1968.
- Мальцев А. И. Основы линейной алгебры. — М.: Наука, 1975.
- Фаддеев Д. К. и Соминский И. С. Сборник задач по высшей алгебре. — М.: Наука, 1977.