

ВАН-ДЕР ВАРДЕН

СОВРЕМЕННАЯ
АЛГЕБРА

I

ОГИЗ-ГОСТЕХИЗДАТ-1947

Б. Л. ван-дер-ВАРДЕН

СОВРЕМЕННАЯ АЛГЕБРА

ЧАСТЬ I

**- ПЕРЕВОД С НЕМЕЦКОГО
Д. А. РАЙКОВА**

**ПОД РЕДАКЦИЕЙ, С ПРЕДИСЛОВИЕМ И ДОБАВЛЕНИЕМ
А. Г. КУРОША**

**О Г И З
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1947 ЛЕНИНГРАД**

Редактор *О. Н. Головин*. Техн. редактор *Н. А. Тумаркина*. Подписано к печати 17/V 1947 г.
21,25 печ. л. 23,10 уч.-изд. л. 45600 тип. зн. в печ. л. Тираж 8 000 экз.
А-04565. Цена книги 14 р. Переплёт 1 р. 50 к. Заказ № 4101.

4-я типография им. Евг. Соколовой треста «Полиграфкнига» ОГИЗа при Совете
Министров СССР. Ленинград, Исамайловский пр., 29.

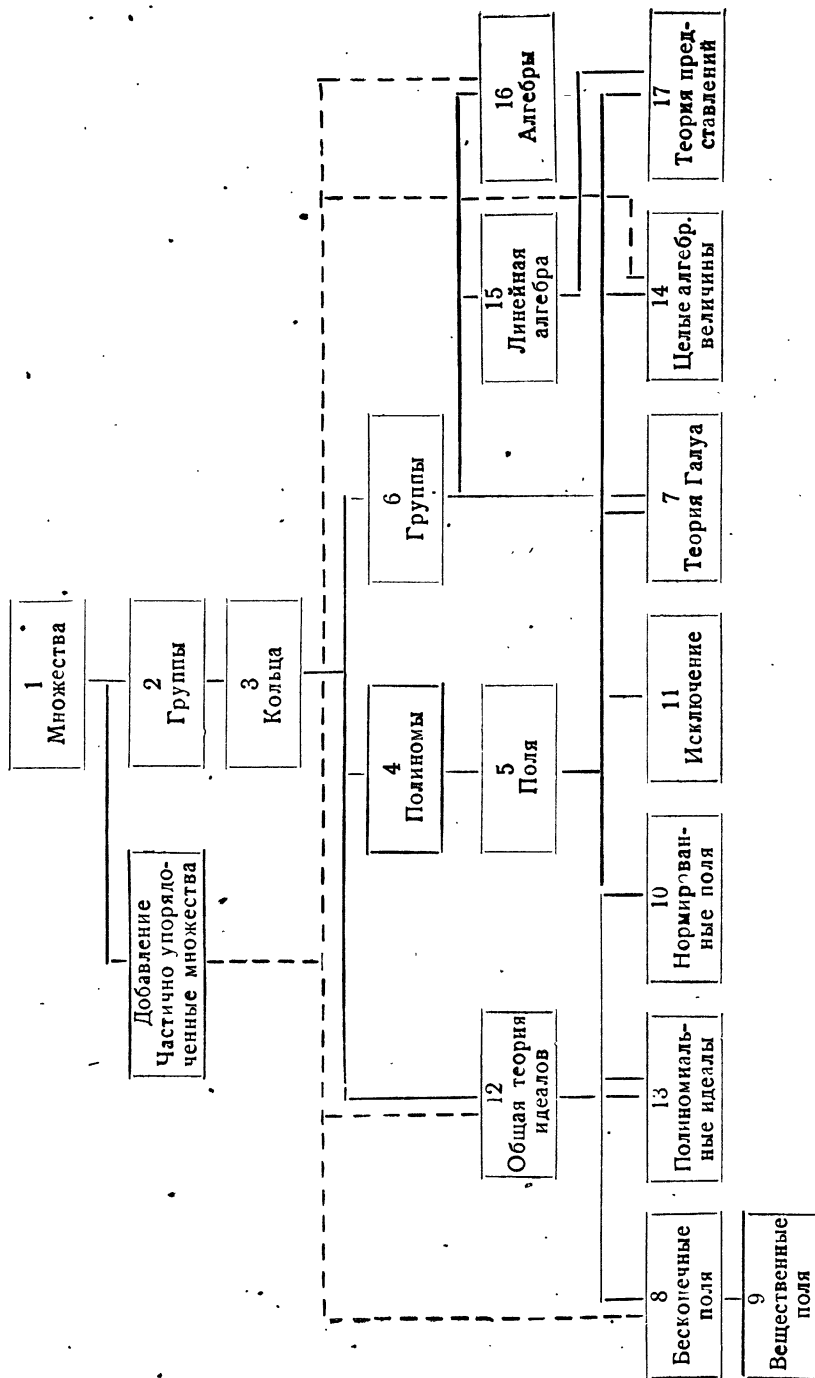
ОГЛАВЛЕНИЕ.

Схема зависимости глав	6
Предисловие редактора	7
Предисловие автора ко второму изданию первой части	10
Введение	13
Глава первая. Числа и множества	16
§ 1. Множества	16
§ 2. Отображения. Мощности	18
§ 3. Натуральный ряд	19
§ 4. Конечные и счётные множества	23
§ 5. Разбиения на классы	26
Глава вторая. Группы	28
§ 6. Понятие группы	28
§ 7. Подгруппы	37
§ 8. Операции над комплексами. Смежные классы	41
§ 9. Изоморфизмы и автоморфизмы	44
§ 10. Гомоморфизмы. Нормальные делители. Факторгруппы	48
Глава третья. Кольца и поля	53
§ 11. Кольца	53
§ 12. Гомоморфизм и изоморфизм	60
§ 13. Отношения	62
§ 14. Векторные пространства и алгебры	65
§ 15. Кольца полиномов	70
§ 16. Идеалы. Факторкольца	73
§ 17. Делимость. Простые идеалы	78
§ 18. Эвклидовы кольца и кольца главных идеалов	80
§ 19. Разложение на множители	84
Глава четвёртая. Целые рациональные функции	91
§ 20. Дифференцирование	91
§ 21. Корни	92
§ 22. Интерполяционные формулы	94
§ 23. Разложение на множители	100
§ 24. Признаки неприводимости	103

§ 25. Разложение на множители конечным числом проб	108
§ 26. Симметрические функции	109
§ 27. Результат двух полиномов	115
§ 28. Результат как симметрическая функция корней	118
§ 29. Разложение рациональных функций на простейшие дроби	121
Глава пятая. Теория полей	124
§ 30. Подполе. Простое поле	124
§ 31. Присоединение	127
§ 32. Простые расширения поля	128
§ 33. Линейная зависимость величин над телом	134
§ 34. Линейные уравнения над телом	139
§ 35. Алгебраические расширения полей	142
§ 36. Корни из единицы	148
§ 37. Поля Галуа (конечные поля)	153
§ 38. Сепарабельные и несепарабельные расширения	157
§ 39. Совершенные и несовершенные поля. Корневое поле	163
§ 40. Простота алгебраических расширений. Теорема о примитивном элементе	165
§ 41. Нормы и следы	168
§ 42. Выполнение конструкций теории полей с помощью конечного числа шагов	175
Глава шестая. Продолжение теории групп	180
§ 43. Группы с операторами	180
§ 44. Операторные изоморфизм и гомоморфизм	182
§ 45. Две теоремы об изоморфизмах	184
§ 46. Нормальные и композиционные ряды	185
§ 47. Прямые произведения	190
§ 48. Простота знакопеременной группы	193
§ 49. Транзитивность и примитивность	194
Глава седьмая. Теория Галуа	198
§ 50. Группа Галуа	198
§ 51. Основная теорема теории Галуа	201
§ 52. Сопряженные группы, поля и элементы полей	205
§ 53. Поля деления круга	206
§ 54. Периоды уравнения деления круга	210
§ 55. Циклические поля и двучленные уравнения	216
§ 56. Разрешимость уравнений в радикалах	220
§ 57. Общее уравнение n -ной степени	224
§ 58. Уравнения второй, третьей и четвертой степеней	226
§ 59. Построения с помощью циркуля и линейки	233
§ 60. Метациклические уравнения простой степени	238
§ 61. Вычисление группы Галуа. Уравнения с симметрической группой	241

Глава восьмая. Бесконечные расширения полей	246
§ 62. Алгебраически замкнутые поля	246
§ 63. Простые трансцендентные расширения	254
§ 64. Степень трансцендентности	258
§ 65. Дифференцирование алгебраических функций	261
Глава девятая. Вещественные поля	267
§ 66. Расположенные поля	268
§ 67. Определение вещественных чисел	271
§ 68. Корни вещественных функций	279
§ 69. Поле комплексных чисел	284
§ 70. Алгебраическая теория вещественных полей	287
§ 71. Теоремы существования для формально вещественных полей	293
§ 72. Суммы квадратов	297
Глава десятая. Нормированные поля	300
§ 73. Нормирования	300
§ 74. Полные расширения	306
§ 75. Нормирования поля рациональных чисел. Архимедовские нормирования числовых полей	312
§ 76. Нормирование алгебраических расширений	315
Добавление. Частично упорядоченные множества	325
Предметный указатель	332

Схема зависимости глав.



ПРЕДИСЛОВИЕ РЕДАКТОРА.

В мировой математической литературе нашего времени «Современная алгебра» Ван-дер-Вардена, бесспорно, занимает одно из значительнейших мест. Её первое издание, опубликованное в 1930—1931 гг., явилось завершением блестящего периода в истории алгебры, периода её теоретико-множественной перестройки, в первую очередь связанного с именами Штейница, Артина и Эммы Нётер. Сразу же по выходе в свет книга стала настольной для алгебраистов всего мира; она определяла характер, а отчасти и пути, дальнейших алгебраических исследований; на ней воспитывались (и продолжают воспитываться) молодые алгебраисты. Больше того, влияние этой книги сказывалось далеко за пределами алгебры — достаточно указать, что кандидатские планы подавляющего большинства молодых советских математиков, всех математиков, проходивших свою аспирантуру в последние годы, включали в себя алгебраический экзамен по тем или иным главам книги Ван-дер-Вардена (вышедшей в русском переводе Л. Я. Окунева в 1934—1937 гг.).

Во втором издании, опубликованном в 1937—1940 гг. (первая часть вышла из печати в 1937 г.; вторая часть — в 1940 г.), автор существенно переработал и дополнил книгу. Следует особо отметить включение целой главы, посвящённой теории нормированных полей («Bewertungstheorie»), а также значительное развитие теории простых алгебр в двух последних главах, — то и другое в образцовом изложении. Автору не удалось, однако, в полной мере отразить новейшее развитие алгебраических идей. Так, в книге никак не проявилась вполне определившаяся за эти годы тенденция к изучению неассоциативных колец и, в частности, не нашли места хотя бы основы общей теории колец и алгебр Ли. Далее, читатель, изучив книгу, не узнает ни определения структуры, ни роли этого понятия в теории групп и теории колец, ни его связи с теорией проктивных геометрий. Наконец, уже в первом

издании автор ограничился изложением лишь тех простейших сведений из теории групп, которые были ему необходимы для построения теории колец, теории Галуа и линейной алгебры. Второе издание в этой части ничем не отличается от первого, и читатель, желающий овладеть теорией групп или хотя бы познакомиться с её основными достижениями, должен будет обращаться к специальной литературе. Таким образом, книга никак не может сейчас рассматриваться как энциклопедия современной алгебраической науки. Она, однако, полностью сохраняет и, повидимому, ещё долго будет сохранять роль лучшего в своей области учебного пособия, и поэтому новый перевод книги, отражающий улучшения, внесённые автором во второе издание, вполне оправдан.

Настоящий перевод содержит некоторые отступления от оригинального текста второго издания. Автор внёс во второе издание ряд изменений, вызванных тем стремлением к «финитности», о котором он сам говорит в своём предисловии, и которое практически выразилось в изгнании из книги материала, использующего трансфинитную индукцию, а иногда — всего лишь аксиому выбора. Результатом этих изменений явилось заметное обеднение некоторых глав книги, в первую очередь общей теории полей, основная теорема которой — теорема Штейница о существовании алгебраически замкнутых алгебраических расширений — во втором издании доказывается лишь для счётного случая; утверждение автора, что именно этот случай является для приложений важнейшим, не соответствует, по нашему мнению, истинному положению вещей. Мы не считали, что в алгебраическом образовании молодых математиков должен принудительно отражаться этот поворот в математическом мировоззрении автора, и поэтому местами восстановили текст первого издания. В других случаях, принципиально менее существенных или же таких, где переход от счётного случая к общему для читателя, владеющего трансфинитной индукцией, не представит затруднений (например, в теории формально вещественных полей), мы сохранили новый текст автора. Что же касается самой теоремы Штейница, то мы не могли просто восстановить её доказательство из первого издания, так как это доказательство нуждается в некоторой доработке, и предпочли включить в книгу новое доказательство, опирающееся не на трансфинитную индукцию, а на индукцию по частично упорядоченному множеству с условием мини

мальности. Это позволило, в частности, не восстанавливать доказательство теоремы Цермело, содержащееся в первом издании; необходимые же сведения о частично упорядоченных множествах, и без того в значительной части излагавшиеся (на языке теории идеалов) в двенадцатой главе книги, выделены в особое Добавление в конце первой части книги.

Другие отступления от авторского текста вызваны тем, что при подготовке второго издания второй части книги автор допустил некоторые недосмотры, особенно в пятнадцатой главе. Так, в первом издании эта глава включала в себя теорию систем линейных уравнений. Во втором издании автор с полным основанием перенёс указанную теорию в пятую главу, но, к сожалению, забыл исключить её из пятнадцатой главы. Мы пересмотрели также библиографическую часть книги и дополнили её указаниями на некоторые наиболее существенные работы последних лет; с другой стороны, все ссылки на немецкую учебную литературу заменены указаниями на соответствующую литературу, имеющуюся на русском языке.

Москва, январь 1946 г.

А. Курош.

ПРЕДИСЛОВИЕ АВТОРА КО ВТОРОМУ ИЗДАНИЮ ПЕРВОЙ ЧАСТИ.

Предпринимая новую обработку текста первой части, я стремился к тому, чтобы второе издание предлагаемой книги вновь стояло на уровне современного состояния алгебры. Для этого прежде всего оказалось необходимым подробнее и систематичнее изложить основы теории нормированных полей, посвятив ей особую главу. Неоценимую помощь при составлении этой новой главы оказал мне М. Дойринг.

Во-вторых, представилась возможность, не нарушая общей целевой установки книги, сделать из её первой части пригодное для начинающих элементарное руководство по алгебре (за вычетом теории определителей). Для этой цели была перенесена из второй части в первую эйлеровская теория результатов, а также теория линейных уравнений; добавлен параграф о разложении на простейшие дроби; расширен материал, относящийся к дифференцированию, а также интерполированию; дано элементарное обоснование учения о разложении на множители и, кроме того, внесены многочисленные отдельные изменения, облегчающие усвоение текста. Понятия векторного пространства и алгебры (гиперкомплексной системы) я ввожу теперь уже в первой части, доказывая при этом некоторые основные теоремы о размерностях, нормах и следах сразу во всей требуемой общности (а не для коммутативного лишь случая, как в первом издании).

В-третьих, я попытался по возможности избежать в алгебре рискованных теоретико-множественных способов доказательства. К сожалению, вполне «финитное» построение алгебры с устранением всех неконструктивных доказательств существования невозможно без больших жертв. Пришлось бы существенные части алгебры вовсе изъять, либо формулировать теоремы со столь большим числом ограничений, что изложение стало бы неудобоваримым и во всяком случае недоступным для начинающего. Однако, мне представилось возможным собрать здесь, по крайней мере, те краеугольные камни финитного обоснования алгебры, которыми мы уже обладаем сейчас. В теории полей я осуществил это, изложив вопрос о выполнении конструкций теории полей в конечное число шагов так, чтобы отсюда непосредственно можно было извлечь интуиционистское обоснование теории в той степени, в какой оно вообще возможно. Учение о раз-

ложении на множители также изложено элементарно и тем самым более финитно.

В осуществление той же тенденции, в настоящем издании целиком выпущены те части теории полей, которые основываются на постулате выбора и теореме о полном упорядочении. Решающим при этом было признание того, что полным упорядочением поля вносится в алгебру чуждый элемент, а также то соображение, что почти для всех применений вполне достаточен специальный случай счётных полей, когда полное упорядочение заменяется перечислением элементов поля. Прекрасные идеи классического мемуара Штейница об алгебраической теории полей (к тому же вышедшего теперь отдельной книгой) вполне выявляются уже в счётном случае.

Удалив рассуждения, опирающиеся на полное упорядочение, мы получили возможность, несмотря на включение упомянутого выше дополнительного материала, обойтись без увеличения объёма книги.

Многочисленными мелкими улучшениями, в большинстве методического характера, я обязан созидательной критике ряда друзей, которым выражаю здесь свою сердечную благодарность. Я надеюсь, что более элементарное, а во многих местах и более подробное изложение повысит ценность книги, особенно для начинающих математиков.

Лейпциг, январь 1937 г.

ВВЕДЕНИЕ.

Цель книги. «Абстрактное», «формальное» или «аксиоматическое» направление, которому алгебра обязана своим новым подъёмом в последнее время, привело прежде всего к образованию ряда новых понятий, открытию новых связей и получению многочисленных результатов в теории полей, теории идеалов, теории групп и теории алгебр. Ввести читателя в весь этот мир понятий и является главной целью настоящей книги.

В соответствии с этим на первый план выдвинулись общие понятия и методы. Однако и частные результаты классической алгебры нашли своё место в рамках нового построения.

Распределение материала. Указания для читателя. Чтобы развить с достаточной ясностью общие точки зрения, господствующие в «абстрактной» алгебре, было необходимо прежде всего заново изложить основы теории групп и элементарной алгебры.

Эти вводные части оказалось возможным дать сжато (но без пробелов), поскольку в последнее время появилось большое количество хороших изложений теории групп, классической алгебры и теории полей. Более подробное изложение начинающий найдёт теперь всюду ¹⁾.

¹⁾ По теории групп укажем:

Speiser A., Die Theorie der Gruppen von endlicher Ordnung, 2 Aufl. Berlin, Julius Springer, 1927, 3 Aufl., 1937.

Шмидт О. Ю., Абстрактная теория групп, 2-е изд., ГТТИ, 1933.

Курош А. Г., Теория групп, Гостехиздат, 1944.

По теории полей:

Hasse H., Höhere Algebra I, II u. Aufgabensammlung zur höheren Algebra, Sammlung Götschen, 1926/27.

Haupt O., Einführung in die Algebra I, II, Leipzig, 1929.

По классической алгебре:

Perron O., Algebra I, II, 1927.

По линейной алгебре:

Böcher M., Introduction to Higher Algebra, New York, 1908 (русский перевод: М. Бохер, Введение в высшую алгебру, Москва, ГТТИ, 1933).

Dickson L. E., Modern Algebraic Theories, Chicago, 1926.

Schreier O. u. Sperner E., Einführung in die analytische Geometrie und Algebra, B. I, Leipzig — Berlin, 1931 (русский перевод: О. Шрейер и Г. Шпернер, Введение в линейную алгебру в геометрическом изложении, т. I, ОНТИ, 1934).

Schreier O. u. Sperner E., Vorlesungen über Matrizen, Leipzig — Berlin, 1932 (русский перевод: О. Шрейер и Е. Шпернер, Теория матриц, ОНТИ, 1936).

Дальнейшим руководящим принципом служило требование, чтобы, по возможности, каждая отдельная часть книги была понятна сама по себе, независимо от других. Тот, кто хочет познакомиться с общей теорией идеалов или с теорией алгебр, не должен предварительно изучать теорию Галуа, и обратно; и того, кто желает узнать что-нибудь из теории исключения или линейной алгебры, не должны отпугивать сложные понятия теории идеалов.

Поэтому мы остановились на следующем распределении материала. Первые три главы на минимальном количестве страниц содержат необходимый подготовительный материал для всех дальнейших глав: основные понятия, относящиеся к: 1) множествам, 2) группам и 3) кольцам, идеалам и полям. Следующие главы, до десятой включительно, посвящены, главным образом, теории полей и опираются, в первую очередь, на основоположную работу Штейница из *Crelles Journal*¹⁾. Далее следуют по возможности независимые друг от друга разделы, посвященные теории модулей, колец и идеалов, с приложениями к теории исключения, элементарным делителям, алгебрам и представлениям групп.

Теорию алгебраических функций и теорию непрерывных групп пришлось опустить, поскольку для должного построения обеих этих теорий потребовалось бы привлечение трансцендентных понятий и методов. Мы опустили также теорию инвариантов из-за обширности её материала. Предполагается знакомство читателя с определителями, которые, впрочем, будут употребляться весьма редко.

Для дальнейшей ориентировки мы отошлём читателя к оглавлению и прежде всего к «схеме зависимости глав», в которой точно указано, какие из предшествующих глав необходимы для понимания каждой отдельной главы.

Менее существенный, равно как и более трудный дополнительный материал напечатан мелким шрифтом.

Восьмую, девятую и десятую главы можно при первом чтении опустить.

Задачи, вкрапленные в текст, выбраны большей частью так, что на них можно проверить, понят ли предыдущий текст. Они содержат также примеры и дополнения, на которые в последующем тексте делаются иногда ссылки. Решение этих задач большей частью не требует применения искусственных приёмов; в случае же надобности последние указываются в прямых скобках.

Источники. Предлагаемая книга частично возникла из записей лекций, причём были использованы:

¹⁾ См. *J. reine u. angew. Math.*, 137 (1910), 167—309. Эта работа вышла также отдельной книгой: Steinitz E., *Algebraische Theorie der Körper. Neu herausgegeben, mit Erläuterungen und einem Anhang «Abriß der Galoischen Theorie» versehen von R. Baer und H. Hasse*, Berlin, 1930.

курс лекций Артина по алгебре (Гамбург, летний семестр 1926 г.); семинар по теории идеалов, проведённый Артином, Блашке, Шрайером и автором (Гамбург, зимний семестр 1926/27 уч. г.); два курса лекций Э. Нётер, оба по теории групп и алгебр (Гёттинген, зимний семестр 1924/25 уч. г. и зимний семестр 1927/28 уч. г.)¹⁾.

Многие новые доказательства и варианты доказательств, встречающиеся в этой книге, имеют своим источником упомянутые лекции и семинар, хотя бы этот источник и не был прямо указан.

¹⁾ Обработка последнего из названных курсов лекций Э. Нётер появилась в *Math. Zeitschrift*, 30 (1929), 641—692.

ГЛАВА ПЕРВАЯ. ЧИСЛА И МНОЖЕСТВА.

В этой книге мы будем опираться на некоторые логические и общематематические понятия, в частности, на понятие множества, с которыми начинающий математик мог не часто встречаться. Поэтому мы предположим дальнейшему изложению краткую главу, посвящённую этим понятиям. При этом мы не будем вдаваться в трудности, связанные с вопросами обоснования¹⁾: мы будем всюду стоять на «наивной точке зрения», конечно, избегая определений, содержащих порочный круг и приводящих к парадоксам. Подготовленный читатель может, ознакомившись лишь со смыслом символов $\in$, $\subset$, $\supset$, $\cap$, $\cup$ и $\{\dots\}$, пропустить остальное содержание этой главы.

§ 1. Множества.

Мы мыслим, в качестве отправного пункта всех математических рассуждений, какие-либо доступные представлению объекты, например, числовые символы, буквы или их комбинации. Свойство, которым либо обладает, либо не обладает каждый отдельный из этих объектов, определяет *множество* или *класс*; *элементы этого множества* суть те объекты, которые обладают данным свойством. Запись

$$a \in \mathfrak{M}$$

означает: a есть элемент множества $\mathfrak{M}$. Говорят также, пользуясь наглядно-геометрическим представлением: a лежит в $\mathfrak{M}$. Множество, не содержащее ни одного элемента, называется *пустым*.

Мы считаем дозволенным рассматривать сами последовательности и множества чисел (или букв и т. п.) снова как объекты и элементы множеств (как говорят иногда, — множеств второй ступени). Эти множества второй ступени могут, в свою очередь, служить элементами множеств более высокой ступени, и т. д. Мы, однако, остережёмся от употребления таких понятий, как «множество всех множеств» и т. п., так как подобные понятия могут приводить (и действительно приводили) к противоречиям; напротив, мы всегда будем образовать

¹⁾ См. по этому поводу А. Fraenkel, *Einleitung in die Mengenlehre*, 3-е изд. (Berlin, 1928).

вать новые множества лишь из объектов заранее очерченной категории (к которой вновь определяемые множества ещё не принадлежат).

Если все элементы множества $\mathcal{N}$ являются одновременно элементами множества $\mathcal{M}$, то $\mathcal{N}$ называется *подмножеством* или *частью* множества $\mathcal{M}$; пишут:

$$\mathcal{N} \subseteq \mathcal{M}.$$

$\mathcal{M}$ называется тогда *надмножеством* или *объемлющим множеством* множества $\mathcal{N}$; пишут:

$$\mathcal{M} \supseteq \mathcal{N}.$$

Из $\mathcal{A} \subseteq \mathcal{B}$ и $\mathcal{B} \subseteq \mathcal{C}$ следует $\mathcal{A} \subseteq \mathcal{C}$.

Пустое множество содержится в каждом множестве.

Если одновременно все элементы множества $\mathcal{M}$ содержатся в $\mathcal{N}$ и все элементы множества $\mathcal{N}$ содержатся в $\mathcal{M}$, то множества $\mathcal{M}$ и $\mathcal{N}$ называют *равными*; пишут:

$$\mathcal{M} = \mathcal{N}.$$

Таким образом, равенство множеств $\mathcal{M}$ и $\mathcal{N}$ означает совместное выполнение соотношений

$$\mathcal{M} \subseteq \mathcal{N}, \quad \mathcal{N} \subseteq \mathcal{M}.$$

Или иначе: два множества равны, если они содержат одни и те же элементы.

Если $\mathcal{N} \subseteq \mathcal{M}$, но $\mathcal{N}$ не равно $\mathcal{M}$, то $\mathcal{N}$ называют *собственным подмножеством* множества $\mathcal{M}$, а $\mathcal{M}$ — *собственным объемлющим множеством* множества $\mathcal{N}$ и пишут:

$$\mathcal{N} \subset \mathcal{M}, \quad \mathcal{M} \supset \mathcal{N}.$$

Таким образом, запись $\mathcal{N} \subset \mathcal{M}$ означает, что все элементы множества $\mathcal{N}$ лежат в $\mathcal{M}$, причём в $\mathcal{M}$ существует по меньшей мере один элемент, не лежащий в $\mathcal{N}$.

Пусть теперь $\mathcal{A}$ и $\mathcal{B}$ — произвольные множества. Множество $\mathcal{D}$, состоящее из всех тех и только тех элементов, которые принадлежат и $\mathcal{A}$, и $\mathcal{B}$, называется *пересечением* множеств $\mathcal{A}$ и $\mathcal{B}$; пишут:

$$\mathcal{D} = [\mathcal{A}, \mathcal{B}] = \mathcal{A} \cap \mathcal{B}.$$

$\mathcal{D}$ содержится и в $\mathcal{A}$, и в $\mathcal{B}$, причём каждое множество, обладающее этим свойством, содержится в $\mathcal{D}$.

Множество $\mathcal{B}$, состоящее из всех тех и только тех элементов, каждый из которых принадлежит по крайней мере одному из множеств $\mathcal{A}$, $\mathcal{B}$, называется *объединением* множеств $\mathcal{A}$ и $\mathcal{B}$; пишут:

$$\mathcal{B} = \mathcal{A} \cup \mathcal{B}.$$

$\mathcal{B}$ содержит и $\mathcal{A}$, и $\mathcal{B}$, причём каждое множество, обладающее этим свойством, содержит также $\mathcal{B}$.

Таким же образом определяют пересечение и объединение любого множества Σ множеств $\mathcal{A}, \mathcal{B}, \dots$. Для записи пересечения

(т. е. множества элементов, лежащих во всех множествах $\mathcal{A}, \mathcal{B}, \dots$ множества Σ) пользуются символом $\mathcal{D}(\Sigma)$, либо $[\mathcal{A}, \mathcal{B}, \dots]$.

Два множества называются *взаимно простыми*, если их пересечение пусто, т. е. если нет ни одного элемента, общего обоим множествам.

Если множество задано перечнем его элементов, например: множество $\mathcal{M}$ состоит из элементов a, b, c , то пишут:

$$\mathcal{M} = \{a, b, c\}.$$

Этот способ записи оправдывается тем, что, по определению равенства множеств, множество вполне определяется заданием его элементов; свойством, выделяющим элементы множества $\mathcal{M}$, является: быть тождественным с a , или b , или c .

§ 2. Отображения. Мощности.

Если каждому элементу a множества $\mathcal{M}$ по какому-либо правилу поставлен в соответствие единственный (вообще говоря, новый) объект $\varphi(a)$, то это сопоставление называется *функцией*, а множество $\mathcal{M}$ — *областью определения* этой функции. Множество $\mathcal{N}$ всех значений функции $\varphi(a)$ называется *областью значений* функции. Такое сопоставление, при котором каждому элементу множества $\mathcal{M}$ ставится в соответствие точно один элемент множества $\mathcal{N}$, и притом каждый элемент множества $\mathcal{N}$ используется хотя бы один раз, называется также (однозначным) *отображением* множества $\mathcal{M}$ на множество $\mathcal{N}$. Элемент $\varphi(a)$ называется тогда *образом* элемента a , элемент же a — *прообразом* элемента $\varphi(a)$. Образ $\varphi(a)$ однозначно определяется заданием a , но обратное — не обязательно. Слово «отображение» будет на протяжении всей книги употребляться только для обозначения этих однозначных отображений.

Если каждый элемент множества $\mathcal{M}$ служит образом только одного элемента множества $\mathcal{N}$, то отображение называется *взаимно однозначным*. Тогда существует «обратное» отображение, относящее каждому элементу b из $\mathcal{N}$ тот элемент из $\mathcal{M}$, образом которого служит b .

Два множества $\mathcal{M}, \mathcal{N}$, каждое из которых можно однозначно отобразить на другое, называются *равномощными*; пишут:

$$\mathcal{M} \sim \mathcal{N}.$$

О равномощных множествах говорят также, что они имеют «одинаковую мощность».

Примеры. Если мы каждому натуральному числу n поставим в соответствие число 0 или 1, смотря по тому, чётно или нечётно n , то получим отображение множества натуральных чисел на множество $\{0, 1\}$. Это отображение не взаимно однозначно. Поставив в соответствие каждому натуральному числу n число $2n$, мы полу-

чим взаимно однозначное отображение множества всех натуральных чисел на множество всех чётных натуральных чисел. Таким образом, множество всех натуральных чисел равномощно с множеством всех чётных натуральных чисел.

Задача. Доказать следующие три свойства символа $\sim$:

1. $M \sim M$.

2. Из $M \sim B$ следует $B \sim M$.

3. Из $M \sim B$ и $B \sim C$ следует $M \sim C$.

Множество вполне может быть равномощным с собственным объемлющим множеством. Это показывает как второй из приведенных выше примеров, так и следующий пример: если поставить в соответствие каждому натуральному числу n число $n - 1$, то множество натуральных чисел взаимно однозначно отобразится на множество, содержащее кроме натуральных чисел ещё число нуль. Однако, как будет показано в § 4, ничего подобного не может иметь места для «конечных» множеств.

§ 3. Натуральный ряд.

Мы будем предполагать известным множество натуральных чисел:

1, 2, 3, ...;

точно так же будут предполагаться известными и следующие основные свойства этого множества (аксиомы Пеано):

I. 1 есть натуральное число.

II. В множестве натуральных чисел для каждого числа ¹⁾ a имеется одно определённое последующее a^+ .

III. Всегда

$$a^+ \neq 1,$$

т. е. никакое число не имеет своим последующим числом единицу.

IV. Из $a^+ = b^+$ следует $a = b$, т. е. каждое число либо вовсе не является последующим ни для какого числа, либо служит последующим точно для одного числа.

V. «Принцип полной индукции»: каждое множество натуральных чисел, которое содержит число 1 и которое вместе с каждым содержащимся в нём числом a содержит и его последующее число a^+ , совпадает со всем множеством натуральных чисел.

На свойстве V основывается метод доказательства с помощью *полной индукции*: для того чтобы доказать, что некоторым свойством E обладают все числа, доказывают это свойство для числа 1, а затем — для любого n^+ при «предположении индукции», что n уже обладает свойством E . В силу V, множество чисел, обладающих свойством E , должно содержать тогда все числа.

¹⁾ «Число» будет пока означать лишь натуральное число.

Сумма двух чисел. Каждой паре чисел x, y можно единственным образом поставить в соответствие натуральное число, обозначаемое $x + y$, так, чтобы выполнялись условия ¹⁾:

- (1) $x + 1 = x^+$ для каждого x ,
 (2) $x + y^+ = (x + y)^+$ для каждого x и каждого y .

В силу этого определения мы можем в дальнейшем вместо a^+ писать также $a + 1$.

Сложение, определённое условиями (1) и (2), обладает следующими свойствами:

- (3) $(a + b) + c = a + (b + c)$ («закон ассоциативности сложения»);
 (4) $a + b = b + a$ («закон коммутативности сложения»);
 (5) Из $a + b = a + c$ следует $b = c$.

Произведение двух чисел. Каждой паре чисел x, y можно единственным образом поставить в соответствие натуральное число, обозначаемое $x \cdot y$ или xy , так, чтобы выполнялись условия:

- (6) $x \cdot 1 = x$,
 (7) $x \cdot y^+ = x \cdot y + x$ для каждого x и каждого y .

Умножение, определённое условиями (6) и (7), обладает следующими свойствами:

- (8) $a \cdot b \cdot c = a \cdot bc$ («закон ассоциативности умножения»);
 (9) $a \cdot b = b \cdot a$ («закон коммутативности умножения»);
 (10) $a \cdot (b + c) = a \cdot b + a \cdot c$ («закон дистрибутивности»);
 (11) Из $a \cdot b = a \cdot c$ следует $b = c$.

. Больше и меньше. Если $a = b + u$, то пишут $a > b$, или также $b < a$. Доказывается, что:

- (12) Любые два числа a, b связаны одним и только одним из соотношений

$$a < b, a = b, a > b.$$

- (13) Из $a < b$ и $b < c$ следует $a < c$.
 (14) Из $a < b$ следует $a + c < b + c$.
 (15) Из $a < b$ следует $ac < bc$.

Решение u уравнения $a = b + u$ при $a > b$ (единственное в силу (5)) обозначается через $a - b$. Вместо « $a < b$ или $a = b$ » пишут кратко $a \leq b$. Соответственный смысл имеет запись $a \geq b$.

¹⁾ Доказательство этого и последующих предложений настоящего параграфа читатель найдёт, например, в книге И. В. Арнольд, Теоретическая арифметика, гл. 2, Москва, Учпедгиз, 1938. Ред.

Далее, имеет место следующая важная теорема:

В каждом непустом множестве натуральных чисел имеется наименьшее число, т. е. такое, которое меньше всех остальных чисел этого множества.

На этой теореме основана вторая форма полной индукции: для того чтобы доказать, что некоторым свойством E обладают все числа, доказывают это свойство для произвольного числа n при «предположении индукции», что им уже обладают все числа $< n$. (Тогда, в частности, это свойство имеет место для $n = 1$, поскольку совсем нет чисел < 1 , так что здесь «предположение индукции» отпадает ¹⁾). Доказательство по индукции, разумеется, должно быть так построено, чтобы оно охватывало случай $n = 1$, ибо иначе оно было бы недостаточным.) Тогда свойством E должны обладать все числа. Действительно, в противном случае множество чисел, не обладающих свойством E , было бы не пусто. Наименьший элемент n этого множества был бы числом, не обладающим свойством E , тогда как все числа $< n$ свойством E обладают, в противоречие с доказанным.

Наряду с «доказательством методом полной индукции», в обеих его формах, существует ещё «определение (или построение) методом полной индукции». Пусть мы хотим каждому натуральному числу x отнести новый объект $\varphi(x)$, причём заранее указана система «рекуррентных определяющих соотношений», которые должны связывать значение $\varphi(n)$ для каждого n с предшествующими значениями $\varphi(m)$ ($m < n$). При этом предполагается, что эти соотношения единственным образом определяют значение $\varphi(n)$, как только все $\varphi(m)$ ($m < n$) даны и сами уже удовлетворяют заданным соотношениям ²⁾. Простейшим является случай, когда для $m = n^+$ значение $\varphi(n^+)$ выражается через $\varphi(n)$, а для $m = 1$ значение $\varphi(1)$ непосредственно задано. Примерами могут служить соотношения (1), (2), соответственно (6), (7), которыми выше были определены суммы и произведения.

¹⁾ Высказывание «все A обладают свойством B » в тех случаях, когда никаких A вообще нет, будет рассматриваться как верное. Точно так же будет рассматриваться как верное утверждение «из E следует F » (где E и F суть свойства, которыми могут обладать или не обладать некоторые объекты x), если нет ни одного x , обладающего свойством E . Всё это вполне согласуется со сделанным уже выше замечанием, что пустое множество содержится в каждом множестве.

Целесообразность этого — в разговорной речи отнюдь не обычного — словоупотребления явствует, например, из того, что лишь при нём высказывание «из E следует F » может быть без всяких исключений превращено в «из не- F следует не- E ». Отрицание высказывания «из E следует (всегда) F » означает: существует x , для которого E верно, а F неверно.

²⁾ Это предположение включает в себя, что $\varphi(1)$ вполне определяется самими соотношениями, так как нет чисел, которые предшествовали бы числу 1.

Мы утверждаем теперь: при указанных предположениях существует одна и только одна функция $\varphi(x)$, значения которой удовлетворяют заданным соотношениям.

Доказательство. Будем понимать под отрезком $(1, n)$ натурального ряда совокупность всех чисел, не превосходящих n . Мы утверждаем теперь прежде всего: на каждом отрезке $(1, n)$ существует одна и только одна функция $\varphi_n(x)$, определённая для чисел x этого отрезка и удовлетворяющая заданным соотношениям. А именно, это утверждение верно для отрезка $(1, 1)$, равно как и для каждого отрезка $(1, n^+)$, коль скоро оно верно для отрезка $(1, n)$. Действительно, в силу рекуррентных соотношений как значение $\varphi(1)$, так и значение $\varphi(n^+)$ по предшествующим значениям $\varphi(m) = \varphi_n(m)$ ($m \leq n$) однозначно определены. Таким образом, наше утверждение верно для каждого отрезка $(1, n)$. Мы получаем, следовательно, ряд функций $\varphi_n(x)$. Каждая функция $\varphi_n(x)$ определена на отрезке $(1, n)$ и тем самым также на каждом меньшем отрезке $(1, m)$; но там она также удовлетворяет определяющим соотношениям и потому совпадает с функцией $\varphi_m(x)$. Таким образом, любые две функции $\varphi_n(x)$, $\varphi_m(x)$ совпадают для всех значений x , для которых они обе определены.

Искомая же функция $\varphi(x)$ должна быть определена для всех отрезков $(1, n)$; удовлетворяя определяющим соотношениям, она должна для всякого n совпадать на $(1, n)$ с $\varphi_n(x)$. Такая функция действительно существует, и притом только одна: её значение $\varphi(x)$ для каждого x есть общее значение всех тех $\varphi_n(x)$, которые определены для этого числа x . Тем самым теорема доказана.

«Построением методом полной индукции» мы будем пользоваться весьма часто.

Задача 1. Пусть свойство E , во-первых, имеет место для $n=3$ и, во-вторых, имея место для $n \geq 3$, имеет также место для $n+1$. Доказать, что E имеет место для всех чисел ≥ 3 .

Присоединением символов $-a$ (отрицательные целые числа) и 0 (нуль) можно дополнить натуральный ряд до области *целых чисел*. Для того чтобы было удобнее распространить смысл знаков $+$, $\cdot$, $<$ на эту более широкую область, целесообразно представить целые числа парами натуральных чисел, а именно:

натуральное число a с помощью $(a+b, b)$,

нуль с помощью (b, b) ,

отрицательное число $-a$ с помощью $(b, a+b)$,

где b , каждый раз, — произвольное натуральное число.

Каждое целое число может быть представлено многими парами (a, b) ; однако каждой парой (a, b) определяется одно и только одно целое число, а именно:

натуральное число $a-b$, если $a > b$,

число 0, если $a = b$.

отрицательное число $-(b-a)$, если $a < b$.

Теперь вводим следующие определения:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc),$$

$$(a, b) < (c, d) \text{ или } (c, d) > (a, b), \text{ если } a + d < b + c,$$

и без труда проверяем: во-первых, что эти определения не зависят от выбора пар в левой части, лишь бы только числа, определяемые этими парами, оставались одни и те же; во-вторых, что выполнены правила (3), (4), (5), (8), (9), (10), (12), (13), (14), равно как и (15) для $c > 0$; в-третьих, что в расширенной области уравнение $a + x = b$ всегда имеет решение, и притом единственное (это решение будет снова обозначаться через $b - a$); и в-четвертых, что $ab = 0$ тогда и только тогда, когда $a = 0$ или $b = 0$ ¹⁾.

Задача 2. Провести доказательства.

Задача 3. То же, что и в задаче 1, но с заменой 3 на 0.

Из элементарных свойств целых чисел мы привели здесь лишь те, которые играют важную роль для дальнейшего. По поводу определения дробей, а также свойств делимости целых чисел, см. гл. 3.

§ 4. Конечные и счётные множества.

Множество, равномощное с отрезком натурального ряда (т. е. с множеством натуральных чисел, не превосходящих некоторого натурального числа n), называется *конечным*. Пустое множество также называется конечным²⁾.

Проще говоря: множество называется конечным, если его элементы могут быть снабжены номерами от 1 до n так, чтобы различные элементы получили различные номера, и все номера от 1 до n были использованы. В соответствии с этим элементы конечного множества $\mathcal{A}$ можно обозначать через $a_1, \dots, a_n$:

$$\mathcal{A} = \{a_1, \dots, a_n\}.$$

Задача 1. Доказать методом полной индукции по n , что каждое подмножество конечного множества $\mathcal{A} = \{a_1, \dots, a_n\}$ в свою очередь также конечно.

Каждое множество, не являющееся конечным, называется *бесконечным*. Например, множество всех целых чисел, как это сейчас будет показано, — бесконечно.

¹⁾ Несколько отличающееся от изложенного введение отрицательных чисел и нуля см. в книге И. В. Арнольд, Теоретическая арифметика, гл. 2.

²⁾ По поводу других определений понятия конечного множества см. A. Tarski, Sur les ensembles finis, Fundamenta Mathematicae, 6 (1924), 45—95.

Основная теорема о конечных множествах (называемая также «основной теоремой арифметики») гласит:

Конечное множество не может быть равномощно ни с каким собственным объемлющим множеством.

Доказательство. Пусть, в противоречие с утверждением теоремы, существует отображение некоторого конечного множества $\mathfrak{M}$ на собственное объемлющее множество $\mathfrak{D}$. Пусть $a_1, \dots, a_n$ — элементы множества $\mathfrak{M}$, а $\varphi(a_1), \dots, \varphi(a_n)$ — их образы; между этими образами должны содержаться как все элементы $a_1, \dots, a_n$, так и, кроме того, по меньшей мере ещё один элемент; обозначим его через a_{n+1} .

При $n=1$ абсурдность этого ясна: единственный элемент a_1 не может иметь двух отличных друг от друга образов a_1, a_2 .

Пусть, таким образом, невозможность отображения φ , обладающего указанными свойствами, уже доказана для значения $n-1$; докажем её для значения n .

Мы можем принять, что $\varphi(a_n) = a_{n+1}$; действительно, если бы это не имело места, так что

$$\varphi(a_n) = a' \quad (a' \neq a_{n+1}),$$

то a_{n+1} имело бы другой прообраз a_i :

$$\varphi(a_i) = a_{n+1},$$

и мы могли бы вместо отображения φ построить другое, которое элементу a_n относит a_{n+1} , элементу a_i относит a' , а в остальном совпадает с φ .

Теперь подмножество $\mathfrak{M}' = \{a_1, \dots, a_{n-1}\}$ будет отображаться функцией φ на множество $\varphi(\mathfrak{M}')$, получающееся из $\varphi(\mathfrak{M}) = \mathfrak{D}$ отображением элемента $\varphi(a_n) = a_{n+1}$. Следовательно, $\varphi(\mathfrak{M}')$ содержит $a_1, \dots, a_n$, являясь тем самым собственным надмножеством множества $\mathfrak{M}'$ и вместе с тем взаимно однозначным образом этого множества. Однако по предположению индукции это невозможно.

Из этой теоремы вытекает прежде всего, что множество никогда не может быть равномощным с двумя различными отрезками натурального ряда; действительно, тогда эти отрезки были бы равномощны друг с другом, в то время как они суть конечные множества, и одно какое-то из них необходимо является собственным объемлющим множеством для другого. Таким образом, конечное множество $\mathfrak{M}$ равномощно с одним и только одним отрезком $(1, n)$ натурального ряда. Однозначно определяемое этим число n называется *числом элементов* множества $\mathfrak{M}$ и может служить мерой его мощности.

Во-вторых, из доказанной теоремы следует, что никакой отрезок натурального ряда не может быть равномощен со всем натуральным рядом. Таким образом, натуральный ряд бесконечен. Каждое множество, равномощное с натуральным рядом, называется *счётно бесконечным*. В соответствии с этим элементы счётно бесконечного

множества можно так перенумеровать, чтобы каждое натуральное число было использовано в качестве номера точно один раз.

Конечные и счётно бесконечные множества называются *счётными*.

Задача 2. Доказать, что число элементов объединения двух взаимно простых конечных множеств равно сумме чисел элементов объединяемых множеств. [Полная индукция с помощью рекуррентных формул (1), (2) § 3.]

Задача 3. Доказать, что число элементов объединения r попарно взаимно простых множеств, составленных каждое из s элементов, равно rs . [Полная индукция с помощью рекуррентных формул (6), (7), § 3.]

Задача 4. Доказать, что каждое подмножество натурального ряда счётно. Вывести отсюда, что множество тогда и только тогда счётно, если его элементы можно перенумеровать натуральными числами так, чтобы различные элементы получили различные номера.

Пример несчётного множества. Множество всех счётно бесконечных последовательностей натуральных чисел не счётно. Что оно не конечно — легко видеть. Если бы оно было счётно бесконечно, то каждая последовательность имела бы номер и каждой номеру i соответствовала бы некоторая последовательность; обозначим её

$$a_{i1}, a_{i2}, \dots$$

Построим теперь последовательность

$$a_{11} + 1, a_{22} + 1, \dots$$

Она также должна иметь номер, скажем, j . Тогда

$$a_{j1} = a_{11} + 1, a_{j2} = a_{22} + 1 \text{ и т. д.,}$$

в частности,

$$a_{jj} = a_{jj} + 1,$$

что, однако, противоречиво.

Задача 5. Доказать, что множество всех целых чисел (положительных, отрицательных и нуля) счётно бесконечно. Точно так же счётно бесконечно множество всех чётных чисел.

Задача 6. Доказать, что множество всех вещественных чисел (т. е. всех бесконечных десятичных дробей) не счётно. [Способ доказательства аналогичен применённому в рассмотренном выше примере.]

Задача 7. Доказать, что мощность счётно бесконечного множества не изменяется от прибавления к нему конечного или счётно бесконечного множества новых элементов.

Объединение счётного множества счётных множеств снова счётно.

Доказательство. Пусть множества будут $M_1, M_2, \dots$; элементы множества M_i пусть будут $m_{i1}, m_{i2}, \dots$.

Существует лишь конечное множество элементов m_{ik} с $i+k=2$, точно так же лишь конечное множество с $i+k=3$, и т. д. Перенумеруем сначала те элементы, для которых $i+k=2$ (скажем, в порядке возрастания i), затем, начиная с ближайшего следующего номера, перенумеруем те элементы, для которых $i+k=3$, и т. д. Тогда каждый элемент m_{ik} получит, в конце концов, некоторый номер, причём разные элементы получат разные номера. Тем самым утверждение доказано.

Задача 8. Доказать, что множество всех несократимых дробей $\frac{\pm a}{b}$ (a и b — взаимно простые натуральные числа) счётно бесконечно.

§ 5. Разбиения на классы.

Знак равенства подчиняется следующим законам:

$$a = a.$$

Из $a = b$ следует $b = a$.

Из $a = b$ и $b = c$ следует $a = c$.

То же выражают словами: соотношение $a = b$ *рефлексивно, симметрично и транзитивно*. Если теперь между элементами какого-либо множества определено некоторое соотношение $a \sim b$ (причём для каждой пары элементов a, b либо $a \sim b$, либо $a \not\sim b$) и если это соотношение удовлетворяет тем же аксиомам:

$$1) a \sim a;$$

$$2) \text{ из } a \sim b \text{ следует } b \sim a;$$

$$3) \text{ из } a \sim b \text{ и } b \sim c \text{ следует } a \sim c,$$

то его называют *соотношением эквивалентности* или просто *эквивалентностью*. Так, например, введённое в § 2 для множеств $M, N, \dots$ соотношение $M \sim N$ (M равномощно с N) удовлетворяет указанным аксиомам. Конгруэнтность треугольников есть соотношение такого же рода. Третий пример: назовём два целых числа эквивалентными, если их разность делится на 2; очевидно, приведённые выше аксиомы будут выполнены.

Если теперь дано какое-либо соотношение эквивалентности, то мы можем все элементы, эквивалентные любому фиксированному элементу a , объединить в *класс* R_a . Тогда все элементы одного класса будут эквивалентны друг другу, ибо из $a \sim b$ и $a \sim c$ следует, в силу 2) и 3), что $b \sim c$, и все элементы, эквивалентные какому-нибудь одному элементу из данного класса, будут лежать в том же классе, ибо из $a \sim b$ и $b \sim c$ следует $a \sim c$. Тем самым класс вполне определяется любым своим элементом: исходя, вместо a , от любого элемента b класса R_a , мы получим тот же самый класс: $R_b = R_a$.

Мы можем поэтому каждый элемент b данного класса выбрать в качестве *представителя* этого класса.

Если же мы возьмём элемент b , не принадлежащий к данному классу (т. е. не эквивалентный элементу a), то $\mathfrak{R}_a$ и $\mathfrak{R}_b$ не смогут иметь ни одного общего элемента; действительно, из $c \sim a$ и $c \sim b$ следовало бы $a \sim b$, т. е. $b \in \mathfrak{R}_a$. Таким образом, в этом случае классы $\mathfrak{R}_a$ и $\mathfrak{R}_b$ взаимно просты.

Классы целиком покрывают заданное множество, так как каждый элемент a лежит в некотором классе, а именно, в $\mathfrak{R}_a$. Таким образом, заданное множество *распадается на попарно взаимно простые классы*. В нашем последнем примере это — класс чётных и класс нечётных чисел.

Как мы видели, $\mathfrak{R}_a = \mathfrak{R}_b$ тогда и только тогда, когда $a \sim b$. Таким образом, введением классов вместо элементов мы можем заменить соотношение эквивалентности $a \sim b$ соотношением равенства $\mathfrak{R}_a = \mathfrak{R}_b$.

Обратно, если дано разбиение множества $\mathfrak{M}$ на попарно взаимно простые классы, то можно положить по определению: $a \sim b$, если a и b принадлежат одному и тому же классу. Соотношение $a \sim b$ будет тогда очевидным образом удовлетворять аксиомам 1)–3).

ГЛАВА ВТОРАЯ.

ГРУППЫ.

Содержание: Изучение фундаментальных для всей книги теоретико-групповых понятий: группы, подгруппы, изоморфизма, гомоморфизма, нормального делителя, факторгруппы.

§ 6. Понятие группы.

Определение. Непустое множество $\mathfrak{G}$ элементов произвольной природы (например, чисел, отображений, преобразований) называется *группой*, если выполнены следующие четыре условия:

1) Задан *закон композиции*, по которому каждой паре элементов a, b множества $\mathfrak{G}$ ставится в соответствие некоторый третий элемент того же множества, называемый большей частью *произведением* элементов a и b и обозначаемый ab или $a \cdot b$. (Произведение может зависеть от порядка следования множителей: равенство $ab = ba$ не обязано выполняться.)

2) *Закон ассоциативности*: Для каждых трёх элементов a, b, c множества $\mathfrak{G}$ имеет место равенство

$$ab \cdot c = a \cdot bc.$$

3) В $\mathfrak{G}$ существует (по меньшей мере) одна (левая) *единица* e , т. е. элемент, обладающий тем свойством, что

$$ea = a \text{ для всех } a \text{ из } \mathfrak{G}.$$

4) Для каждого a из $\mathfrak{G}$ существует в $\mathfrak{G}$ (по меньшей мере) один (левый) *обратный элемент* a^{-1} , т. е. элемент, обладающий тем свойством, что

$$a^{-1}a = e.$$

Группа называется *абелевой*, или *коммутативной*, если, кроме того, всегда $ab = ba$ (*закон коммутативности*).

Примеры. Если элементами группы служат числа, а законом композиции — обыкновенное умножение, то, прежде всего, нуль не может содержаться в группе, так как для нуля не существует обратного числа. Все рациональные числа, отличные от нуля, образуют

уже группу (единицей её служит число 1); точно так же группу образуют числа 1 и -1 , равно как и само число 1.

Но в понятии группы название закона композиции роли не играет: групповой композицией может быть также сложение чисел, лишь бы только были выполнены требования 1) — 4). В этом случае следует, конечно, отказаться от наименования элемента, составленного из a и b , «произведением» и вместо «произведение $a \cdot b$ » в формулировке свойств 1) — 4) читать всюду «сумма $a + b$ ». Единицей будет теперь число 0, ибо $0 + a = a$ для всех чисел a . Точно так же обратным для a будет число $-a$, ибо $-a + a = 0$. Закон ассоциативности сложения

$$a + (b + c) = (a + b) + c$$

всегда выполнен для чисел. Таким образом, множество чисел тогда и только тогда является группой относительно сложения, если оно вместе с каждым двумя числами a и b содержит также их сумму и, кроме того, содержит нуль и вместе с каждым числом a — также противоположное число $-a$. Такое числовое множество называют также *числовым модулем*. Так, например, модуль образуют все рациональные числа, равно как и все целые числа, все чётные числа, и, наконец, уже одно число 0.

Примером группы, элементы которой не являются числами, может служить совокупность всех поворотов плоскости или пространства вокруг некоторой неподвижной точки. Композиция поворотов состоит в их последовательном выполнении: если мы сделаем сначала поворот B , а затем A , то того же результата (т. е. тех же окончательных положений всех точек пространства) можно будет достичь также некоторым одним поворотом; его и называют $A \cdot B$ или AB . Точное алгебраическое определение поворотов и закона их композиции будет дано позже (в главе 15); здесь же мы вводим группу поворотов пространства, основываясь лишь на наглядно-геометрических представлениях, в качестве первого примера группы, элементы которой не являются числами. Одновременно, группа пространственных поворотов представляет собою и первый пример некоммутативной группы, ибо, как весьма легко усмотреть из геометрических соображений, отнюдь не безразлично, производится ли сначала поворот A , а затем B , либо, наоборот, сначала B и потом A . Выполнение закона ассоциативности будет следовать дальше как частный случай из закона ассоциативности для любых преобразований. Единицей группы поворотов служит поворот на угол 0, оставляющий каждую точку на месте. Поворотом, обратным к заданному, является противоположный поворот, возвращающий все точки на прежние места.

Группа поворотов подходит как частный случай под общее понятие *группы преобразований*. Под *преобразованием* или *подстановкой* множества M понимается взаимно однозначное отображение этого множества на себя, т. е. такое соответствие s , при котором каждому

элементу a из $\mathfrak{M}$ отвечает некоторый образ $s(a)$, причём каждый элемент из $\mathfrak{M}$ служит образом точно для одного a . Вместо $s(a)$ пишут также sa . Элементы множества $\mathfrak{M}$ называются *объектами* преобразования s . Слово «преобразование» употребляется большей частью для бесконечных множеств, а слово «подстановка» — для конечных.

Если $\mathfrak{M}$ — конечное множество и его элементы снабжены номерами $1, 2, \dots, n$, то можно каждую подстановку полностью описать с помощью схемы, в которой под номером k каждого элемента записан номер $s(k)$ образа этого элемента; например,

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

есть та подстановка цифр $1, 2, 3, 4$, которая переводит 1 в 2 , 2 в 4 , 3 в 3 и 4 в 1 .

Под *произведением* st двух преобразований s, t понимается преобразование, получающееся, если сначала выполнить преобразование t , а затем подвергнуть образы преобразованию s ¹⁾, т. е.

$$st(a) = s(t(a));$$

например, для $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, $t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ произведение

$$st = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}; \text{ точно так же } ts = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Закон ассоциативности.

$$(rs)t = r(st)$$

доказывается для преобразований следующим образом: Применяя преобразования, стоящие в обеих частях, к произвольному объекту a , получаем:

$$(rs)t(a) = (rs)(t(a)) = r(s(t(a))),$$

$$r(st)(a) = r(st(a)) = r(s(t(a))),$$

т. е. в обоих случаях приходим к одному и тому же результату.

Тождество, или *тождественное преобразование*, есть такое отображение I , которое переводит каждый объект сам в себя:

$$I(a) = a.$$

¹⁾ Порядок записи перемножаемых преобразований есть дело соглашения. Часто принимают обратный порядок; st означает тогда: сначала s , затем t . В этом случае целесообразно записывать символы преобразований справа от объектов преобразований: as вместо $s(a)$.

Тождественное преобразование, очевидно, обладает характеристическим свойством единицы группы: $Is = s$ для каждого преобразования s .

Обратное преобразование для преобразования s есть такое отображение, которое переводит $s(a)$ в a , т. е. возвращает элементы, подвергнутые преобразованию s , в их исходные положения, отменяя тем самым преобразование s . Обозначая это обратное преобразование через s^{-1} , будем иметь, таким образом, для каждого объекта a

$$s^{-1}s(a) = a;$$

тем самым

$$s^{-1}s = I.$$

Из доказанного следует, что совокупность подстановок множества M удовлетворяет всем требованиям 1) — 4). Тем самым эти подстановки образуют группу. Группа всех подстановок конечного множества, состоящего из n элементов, называется *симметрической группой* $1)$ n -ной степени S_n .

Далее, мы заключаем также, что группой является каждое множество G преобразований некоторого множества M , коль скоро оно а) вместе с каждым двумя преобразованиями содержит их произведение; б) вместе с каждым преобразованием содержит также обратное к нему; в) содержит тождество. Если это множество не пусто, то требование в) даже излишне, так как, если s — любое преобразование из G , то в G содержится, в силу б), также s^{-1} , а потому, в силу а), — также $s^{-1}s = I$.

Вернёмся теперь к общей теории групп.

Вместо $ab \cdot c$ или $a \cdot bc$ пишут кратко abc .

Из 3) и 4) следует:

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1},$$

откуда, умножая слева на элемент, обратный к a^{-1} , получаем:

$$eaa^{-1} = e$$

или

$$aa^{-1} = e;$$

таким образом, каждый левый обратный элемент является, вместе с тем, и правым обратным. Одновременно мы видим, что a в свою очередь есть обратный элемент для a^{-1} . Далее имеем:

$$ae = aa^{-1}a = ea = a;$$

таким образом, левая единица является, вместе с тем, и правой.

1) Выбор этого названия объясняется тем, что функции от $x_1, \dots, x_n$, не меняющиеся при всех перестановках переменных, т. е. при всех подстановках из указанной группы, суть «симметрические функции».

Теперь получается и возможность (двустороннего) деления:

5) Каждое из уравнений $ax = b$ и $ya = b$, где a и b — произвольные элементы из $\mathfrak{G}$, обладает решением в $\mathfrak{G}$.

Решениями служат $x = a^{-1}b$ и $y = ba^{-1}$; действительно,

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$

$$(ba^{-1})a = b(a^{-1}a) = be = b.$$

Так же легко доказывается однозначность деления:

6) Из $ax = ax'$, равно как и из $xa = x'a$, следует $x = x'$.

Действительно, если $ax = ax'$, то, умножая обе части слева на a^{-1} , получаем: $x = x'$. Аналогично доказывается вторая часть утверждения.

Отсюда, в частности, следует единственность единицы (как решения уравнения $xa = a$) и единственность обратного элемента (как решения уравнения $xa = e$). Мы будем часто обозначать (единственную) единицу через 1.

Возможность деления, т. е. предложение 5), может, в качестве постулата, заменить постулаты 3) и 4). Действительно, предположим, что 1), 2) и 5) выполнены, и докажем сначала выполнение свойства 3). Выберем какой-нибудь элемент c и будем понимать под e решение уравнения $xc = c$, так что

$$ec = c.$$

Пусть теперь a — произвольный элемент и x — решение уравнения

$$cx = a.$$

Тогда

$$ea = ecx = cx = a,$$

чем 3) и доказано. Свойство же 4) есть непосредственное следствие разрешимости уравнения $xa = e$.

Тем самым мы можем всюду, вместо 1), 2), 3) и 4), использовать в качестве равносильной системы групповых постулатов также 1), 2) и 5).

Если $\mathfrak{G}$ — конечное множество, то вместо 5) можно также принять в качестве постулата свойство 6). Иными словами, вместо выполнимости деления достаточно предполагать (кроме постулатов 1) и 2)) лишь его однозначность.

Доказательство. Пусть a — произвольный элемент из $\mathfrak{G}$. Поставим в соответствие каждому элементу x элемент ax . В силу 6) это соответствие будет взаимно однозначным, т. е. $\mathfrak{G}$ взаимно однозначно отобразится на подмножество, состоящее из всех произведений ax . Но так как $\mathfrak{G}$, по предположению, есть конечное множество, то оно не может быть взаимно однозначно отображено на собственное подмножество. Таким образом, совокупность элементов ax должна совпадать с $\mathfrak{G}$, так что каждый элемент b из $\mathfrak{G}$ может

быть записан в виде $b = ax$, что и утверждается первым из требований 5). Аналогично докажем разрешимость уравнения $b = xa$. Следовательно, 5) вытекает из 6).

Число элементов конечной группы называется *порядком* этой группы.

Дальнейшие правила оперирования. Обратный элемент для произведения вычисляется по следующему правилу:

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Действительно,

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}ab) = b^{-1}b = e.$$

Для абелевых групп часто целесообразно записывать групповую композицию аддитивно, т. е. писать $a + b$ вместо $a \cdot b$. Группа называется тогда *аддитивной группой* или *модулем* (обобщение определённых выше числовых модулей). В этом случае единица группы обозначается символом 0, ибо она, совершенно так же, как нуль в области целых чисел, характеризуется свойством

$$0 + a = a.$$

Аналогично, элемент модуля, обратный к a , записывается в виде $-a$.

Вместо $a + (-b)$ пишут кратко $a - b$, так как этот элемент служит решением уравнения $x + b = a$:

$$(a - b) + b = a + (-b + b) = a + 0 = a.$$

Задача 1. Эвклидовы движения и зеркальные отражения пространства (т. е. те преобразования, при которых сохраняются взаимные расстояния всех пар точек) образуют бесконечную некоммутативную группу.

Задача 2. Доказать, что элементы e, a с законом композиции

$$ee = e, \quad ea = a, \quad ae = a, \quad aa = e$$

образуют (абелеву) группу.

Замечание. Закон групповой композиции можно задать с помощью «групповой таблицы», т. е. таблицы с двойным входом, в которой для каждого двух элементов на пересечении соответствующих строки и столбца помещено произведение этих элементов. Например, для группы предшествующего примера групповой таблицей будет

	e	a
e	e	a
a	a	e

Задача 3. Написать групповую таблицу для группы всех подстановок трёх цифр.

Сложные произведения (суммы); степени. Подобно тому как вместо $ab \cdot c$ мы стали кратко писать abc , определим теперь *сложное произведение* нескольких множителей:

$$\prod_{v=1}^n a_v = \prod_1^n a_v = a_1 a_2 \dots a_n.$$

А именно, при заданных элементах $a_1, \dots, a_N$ определяем рекуррентно (для $n < N$):

$$\left\{ \begin{array}{l} \prod_1^1 a_v = a_1, \\ \prod_1^{n+1} a_v = \left(\prod_1^n a_v \right) \cdot a_{n+1}^1. \end{array} \right.$$

В частности $\prod_1^3 a_v$ есть наше старое $a_1 a_2 a_3$, тогда как $\prod_1^4 a_v = a_1 a_2 a_3 a_4 = (a_1 a_2 a_3) a_4$, и т. д.

Докажем теперь, пользуясь лишь законом ассоциативности, следующее правило:

$$(1) \quad \prod_{\mu=1}^m a_{\mu} \cdot \prod_{v=1}^n a_{m+v} = \prod_{v=1}^{m+n} a_v;$$

словами: *произведение двух сложных произведений равно сложному произведению всех входящих в них сомножителей, взятых в том же порядке.* Так, например, равенство

$$(ab)(cd) = abcd$$

есть частный случай правила (1).

Формула (1) очевидна для $n=1$ (по определению символа $\prod$). Если она уже доказана для некоторого значения n , то для следующего значения $n+1$ имеем:

$$\begin{aligned} \prod_1^m a_{\mu} \cdot \prod_{v=1}^{n+1} a_{m+v} &= \prod_1^m a_{\mu} \left(\prod_1^n a_{m+v} \cdot a_{m+n+1} \right) = \\ &= \left(\prod_1^m a_{\mu} \cdot \prod_1^n a_{m+v} \right) a_{m+n+1} = \\ &= \left(\prod_1^{m+n} a_{\mu} \right) a_{m+n+1} = \prod_1^{m+n+1} a_v. \end{aligned}$$

Тем самым формула (1) доказана.

1) Разумеется, букву v , обозначающую переменный индекс, можно заменить любой другой буквой, не изменяя произведения.

Замечание. Вместо $\prod_1^n a_{m+}$ пишут также $\prod_{m+1}^{m+n} a_v$. Иногда также, если это удобно, полагают $\prod_1^0 a_v = e$.

Произведение n одинаковых сомножителей называется *степенью*:

$$a^n = \prod_1^n a \quad (\text{в частности, } a^1 = a, a^2 = aa \text{ и т. д.}).$$

Из доказанной теоремы следует:

$$(2) \quad a^n \cdot a^m = a^{n+m}.$$

Далее имеет место равенство

$$(3) \quad (a^m)^n = a^{mn}.$$

Доказательство (методом полной индукции) предоставляем читателю.

Доказанные до сих пор правила (1), (2), (3) опирались лишь на закон ассоциативности и потому могут в дальнейшем применяться во всех тех областях, в которых определены произведения и выполнен закон ассоциативности (как, например, в области натуральных чисел), даже когда эти области вовсе не являются группами.

Если умножение, кроме того, коммутативно (абелевы группы), то можно дополнительно доказать, что значение сложного произведения не зависит от порядка следования сомножителей; точнее: *если φ — любое взаимно однозначное отображение отрезка $(1, n)$ натурального ряда на самого себя, то*

$$\prod_{v=1}^n a_{\varphi(v)} = \prod_{v=1}^n a_v.$$

Доказательство. Для $n=1$ утверждение очевидно. Предположим, что оно верно для $n-1$, и будем доказывать его для n . Пусть k — число, отображающееся на n : $\varphi(k) = n$. Имеем:

$$\prod_1^n a_{\varphi(v)} = \prod_1^{k-1} a_{\varphi(v)} \cdot a_{\varphi(k)} \cdot \prod_1^{n-k} a_{\varphi(k+v)} = \prod_{v=1}^{k-1} a_{\varphi(v)} \cdot \prod_{v=1}^{n-k} a_{\varphi(k+v)} \cdot a_{\varphi(k)}.$$

Обозначая теперь через ψ отображение отрезка $(1, n-1)$ на себя, определяемое условиями

$$\psi(v) = \varphi(v) \quad (v < k),$$

$$\psi(v) = \varphi(v+1) \quad (v \geq k),$$

получаем:

$$\prod_1^n a_{\varphi(v)} = \prod_1^{k-1} a_{\psi(v)} \prod_1^{n-k} a_{\psi(k-1+v)} \cdot a_n = \prod_1^{n-1} a_{\psi(v)} \cdot a_n,$$

¹⁾ В случае $k=1$ отпадает первый множитель, в случае $k=n$ — второй; но это не нарушает доказательства.

что, по предположению индукции,

$$= \prod_1^{n-1} a_i \cdot a_n = \prod_1^n a_i.$$

Из доказанного правила следует, что в случае абелевых групп мы вправе употреблять запись вида

$$\prod_{1 \leq i < k \leq n} a_{ik},$$

или

$$\prod_{i < k} a_{ik} \quad (i = 1, \dots, n; k = 1, \dots, n),$$

означающую, что множество всех пар индексов i, k , удовлетворяющих условиям $1 \leq i < k \leq n$, перенумеровано каким-нибудь (безразлично—каким) способом, и затем образовано произведение.

В любой группе можно определить нулевую и отрицательные степени произвольного элемента a обычными формулами

$$a^0 = 1, \\ a^{-n} = (a^{-1})^n.$$

Без труда доказывается, что правила (2), (3) сохраняют силу для произвольных целочисленных показателей степеней.

В аддитивной группе вместо $\prod_1^n a_i$, разумеется, пишут $\sum_1^n a_i$, и вместо a^n , соответственно, $n \cdot a$. В аддитивной группе целых чисел последнее определение согласуется с данным ранее определением произведения двух целых чисел. Всё доказанное для произведений переносится теперь на суммы.

Правило (3), записанное аддитивно, имеет вид закона ассоциативности:

$$n \cdot ma = nm \cdot a,$$

тогда как (2) — вид «закона дистрибутивности»:

$$ma + na = (m + n)a.$$

К этим двум законам присоединяется теперь ещё один закон дистрибутивности:

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

[мультипликативно: $(ab)^m = a^m b^m$], имеющий место, однако, лишь для абелевых групп. Для положительных m он доказывается снова по индукции. А именно, для $m = 1$ справедливость его очевидна. Предположим теперь, что $m(a + b) = ma + mb$ для заданного m . Тогда

$$\begin{aligned} (m + 1)(a + b) &= m(a + b) + (a + b) = \\ &= ma + mb + a + b = \\ &= (ma + a) + (mb + b) = \\ &= (m + 1)a + (m + 1)b. \end{aligned}$$

Как видим, при доказательстве использована перестановочность mb и a . Для $m=0$ утверждение также очевидно, а для отрицательных m достаточно лишь применить определение отрицательных степеней, чтобы вновь вернуться к случаю положительных m .

Задача 5. Доказать для абелевых групп, что

$$\prod_{\nu=1}^n \prod_{\mu=1}^m a_{\mu\nu} = \prod_{\mu=1}^m \prod_{\nu=1}^n a_{\mu\nu}.$$

Задача 6. Точно так же, что

$$\prod_{\nu=1}^n \prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^n \prod_{\nu=\mu}^n a_{\mu\nu}.$$

Задача 7. Порядок симметрической группы $\mathfrak{S}_n$ равен $n! = \prod_{\nu=1}^n \nu$.

[Полная индукция по n .]

§ 7. Подгруппы.

Для того чтобы непустое подмножество $\mathfrak{g}$ группы $\mathfrak{G}$ с тем же законом композиции для элементов из $\mathfrak{g}$, что и в $\mathfrak{G}$, было само группой, необходимо и достаточно, чтобы оно удовлетворяло требованиям 1) — 4) § 6. Требование 1) означает, что если a и b лежат в $\mathfrak{g}$, то и ab должно лежать в $\mathfrak{g}$. Требование 2) выполняется для $\mathfrak{g}$ само собой, ибо оно выполнено даже для $\mathfrak{G}$. Требования 3) и 4) означают, что в $\mathfrak{g}$ должна содержаться единица и что $\mathfrak{g}$ вместе с a содержит также обратный элемент a^{-1} . Первое из этих двух последних требований излишне, так как, если a — любой элемент из $\mathfrak{g}$, то в $\mathfrak{g}$ лежит также a^{-1} , а значит, и произведение $aa^{-1} = e$. Тем самым доказано следующее предложение:

Для того чтобы непустое подмножество $\mathfrak{g}$ заданной группы $\mathfrak{G}$ было подгруппой этой группы, т. е. группой с тем же законом композиции, необходимо и достаточно выполнение следующих условий:

- 1) $\mathfrak{g}$ содержит вместе с каждым двумя элементами a, b также их произведение ab ;
- 2) $\mathfrak{g}$ содержит вместе с каждым элементом a также обратный элемент a^{-1} .

Если, в частности, $\mathfrak{g}$ конечно, то второе из этих требований даже излишне; действительно, в этом случае требования 3) и 4) могут быть заменены требованием 6), а последнее во всяком случае выполняется в $\mathfrak{g}$, ибо оно выполнено даже в $\mathfrak{G}$.

Условия 1) и 2) можно объединить в одно: $\mathfrak{g}$ должно вместе с a и b содержать также ab^{-1} . Действительно, тогда $\mathfrak{g}$ вместе с a содержит также $aa^{-1} = e$ и $ea^{-1} = a^{-1}$, а потому, вместе с a и b , — также b^{-1} и $a(b^{-1})^{-1} = ab$.

Если (в абелевой группе) групповые соотношения записываются аддитивно, то подгруппа характеризуется тем, что она вместе с a и b содержит также $a + b$ и вместе с a — также $-a$. Оба эти требования можно заменить единственным требованием, чтобы вместе с a и b в подгруппе содержался также $a - b$.

Примеры подгрупп:

Каждая группа имеет в качестве подгруппы единичную группу $\mathcal{E}$, состоящую лишь из единицы.

Важнейшей подгруппой симметрической группы n -й степени $\mathcal{S}_n$ является *знакопеременная группа* $\mathcal{A}_n$, состоящая из тех подстановок, которые, будучи применены к переменным $x_1, \dots, x_n$, преобразуют функцию

$$(1) \quad \Delta = \prod_{i < k} (x_i - x_k)$$

саму в себя. Эти подстановки называются *чётными*, остальные — *нечётными*. Нечётные подстановки меняют знак функции Δ на обратный. Каждая *транспозиция* (т. е. подстановка, меняющая местами две цифры) является нечётной подстановкой. Произведение двух чётных или двух нечётных подстановок есть чётная подстановка; произведение чётной и нечётной подстановок есть нечётная подстановка. Из первого свойства вытекает, что $\mathcal{A}_n$ есть группа. Так как фиксированная транспозиция при перемножении с чётной подстановкой даёт нечётную и наоборот, то чётных подстановок существует столько же, сколько и нечётных, и, следовательно, подстановок каждого вида имеется $\frac{n!}{2}$ (см. § 6, задача 7).

Для целей удобного описания подгрупп симметрической группы $\mathcal{S}_n$ пользуются известным способом разложения подстановок на *циклы*.

Будем обозначать через $(pqrs)$ циклическую подстановку, переводящую p в q , q в r , r в s и s в p , а все остальные объекты оставляющую на месте. Легко видеть, что каждая подстановка однозначно (с точностью до порядка следования множителей) представима в виде произведения подобных циклических подстановок или «циклов»:

$$(ikl\dots)(pq\dots)\dots,$$

причём никакие два цикла не имеют общего элемента. Сомножители этого произведения перестановочны. Цикл, состоящий из одного элемента, например (1), представляет тождественную подстановку. Разумеется,

$$(1254) = (2541) = \dots$$

Пользуясь этими обозначениями, мы можем представить $3! = 6$ подстановок группы $\mathcal{S}_3$ следующим образом:

$$(1), (12), (13), (23), (123), (132).$$

Подгруппы все легко определяются. Это суть (кроме самой $\mathcal{S}_3$):

$$\begin{aligned} \mathcal{A}_3: & (1), (123), (132); \\ \mathcal{S}_2: & (1), (12); \\ \mathcal{S}_2': & (1), (13); \\ \mathcal{S}_2'': & (1), (23); \\ \mathcal{E}: & (1). \end{aligned}$$

Пусть $a, b, \dots$ — любые элементы группы $\mathfrak{G}$. Кроме $\mathfrak{G}$ могут существовать и другие подгруппы группы $\mathfrak{G}$, содержащие элементы $a, b, \dots$. Пересечение $\mathfrak{H}$ всех этих подгрупп будет снова группой. Её называют группой, порождённой элементами $a, b, \dots$. Она во всяком случае содержит все произведения их степеней, как, например, $a^{-1}a^{-1}bab^{-1} \dots$ (составленные из конечного числа сомножителей, с повторениями или без). Но эти произведения степеней уже сами образуют группу, содержащую $a, b, \dots$ и таким образом охватывающую группу $\mathfrak{H}$. Следовательно, эта группа совпадает с $\mathfrak{H}$. Тем самым доказано следующее предложение:

Группа, порождённая элементами $a, b, \dots$, состоит из всевозможных конечных произведений степеней этих элементов.

В частности, один единственный элемент a порождает группу всех степеней $a^{\pm n}$ (включая $a^0 = e$). Так как

$$a^n a^m = a^{n+m} = a^m a^n,$$

то эта группа абелева.

Группу, состоящую из всех степеней одного элемента, называют *циклической*.

Имеются две возможности. Либо все степени a^h попарно различны; тогда циклическая группа

$$\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$$

бесконечна. Либо для каких-то двух показателей h и k , $h > k$, имеет место равенство

$$a^h = a^k.$$

Тогда

$$a^{h-k} = e \quad (h - k > 0).$$

Пусть в этом случае n — наименьший положительный показатель, для которого $a^n = e$. Тогда степени $a^0, a^1, a^2, \dots, a^{n-1}$ все попарно различны, так как из равенства

$$a^h = a^k \quad (0 \leq k < h < n)$$

следовало бы

$$a^{h-k} = e \quad (0 < h - k < n),$$

в противоречие с предположением относительно n .

Представляя каждое целое число m в виде

$$m = qn + r \quad (0 \leq r < n),$$

будем иметь:

$$a^m = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = a^r.$$

Таким образом, уже в ряде $a^0, a^1, \dots, a^{n-1}$ встречаются все степени a . Тем самым рассматриваемая циклическая группа имеет точно n элементов, именно

$$a^0, a^1, a^2, \dots, a^{n-1}.$$

Число n — порядок циклической группы, порождённой элементом a , — называется *порядком элемента a* . Если все степени элемента a различны, то a называют *элементом бесконечного порядка*.

Примеры. Целые числа

$$\dots, -2, -1, 0, 1, 2, \dots$$

образуют бесконечную циклическую группу по сложению. Выписанные выше группы $\mathbb{S}_2, \mathbb{A}_3$ суть циклические группы порядков 2, 3.

Задача 1. В абелевой группе произведение элемента a порядка m на элемент b порядка n , где m и n — взаимно простые числа, есть элемент порядка mn .

Задача 2. Существуют циклические группы подстановок произвольного порядка.

Задача 3. Доказать индукцией по n , что $n-1$ транспозиций $(12), (13), \dots, (1n)$, где $n > 1$, порождают симметрическую группу $\mathbb{S}_n$.

Задача 4. Точно так же $n-2$ трёхчленных циклов $(123), (124), \dots, (12n)$, где $n > 2$, порождают знакопеременную группу $\mathbb{A}_n$.

Определим теперь все подгруппы циклической группы. Пусть $\mathbb{G}$ — циклическая группа, порождённая элементом a , и $\mathfrak{g}$ — подгруппа, состоящая не только из единицы. Если $\mathfrak{g}$ содержит элемент a^{-m} с отрицательным показателем, то также и обратный элемент a^m лежит в $\mathfrak{g}$. Пусть теперь a^m — элемент подгруппы $\mathfrak{g}$, имеющий наименьший положительный показатель. Докажем, что все элементы подгруппы $\mathfrak{g}$ суть степени элемента a^m . Действительно, пусть a^s — произвольный элемент из $\mathfrak{g}$. Мы можем снова положить

$$s = qm + r \quad (0 \leq r < m).$$

Тогда $a^s (a^m)^{-q} = a^{s-mq} = a^r$ есть элемент из $\mathfrak{g}$ с $r < m$. Отсюда, в силу выбора числа m , следует, что $r = 0$, и тем самым $s = qm$ и $a^s = (a^m)^q$. Таким образом, все элементы подгруппы $\mathfrak{g}$ суть степени элемента a^m .

Если a — элемент конечного порядка n , $a^n = e$, то, так как $a^n = e$ лежит в $\mathfrak{g}$, n должно делиться на m : $n = qm$. Подгруппа $\mathfrak{g}$ состоит тогда из элементов $a^m, a^{2m}, \dots, a^{qm} = e$ и имеет порядок q . Если же a — элемент бесконечного порядка, то и подгруппа $\mathfrak{g}$, будучи составлена из элементов $e, a^{\pm m}, a^{\pm 2m}, \dots$, имеет бесконечный порядок. Тем самым доказано следующее предложение:

Подгруппа циклической группы сама циклическа. Она состоит либо только из единицы, либо из всех степеней элемента a^m , имеющего наименьший возможный положительный показатель m (где a — элемент, порождающий всю исходную циклическую группу); иначе говоря: она состоит из m -х степеней элементов исходной группы. При этом для циклической группы бесконечного порядка m произвольно, тогда как для циклической группы конечного порядка n число m должно быть делителем n . В этом случае

подгруппа имеет порядок $q = \frac{n}{m}$. Каждому такому числу t соответствует одна и только одна подгруппа $\{a^m\}$ циклической группы $\{a\}$.

§ 8. Операции над комплексами. Смежные классы.

Под *комплексом* в теории групп понимают произвольное множество элементов группы $\mathfrak{G}$.

Под *произведением* gh двух комплексов g и h понимают множество всех произведений gh , где g берётся из g , а h — из h . Если в произведении gh один из комплексов, например g , состоит лишь из одного элемента g , то вместо gh пишут просто gh .

Очевидно,

$$g(hf) = (gh)f.$$

Таким образом, в сложных произведениях комплексов скобки можно опускать [ср. § 6, (1)].

Если комплекс g является группой, то имеем

$$gg = g.$$

Пусть g и h — подгруппы группы $\mathfrak{G}$. Рассмотрим, при каких условиях произведение gh снова является группой. Совокупностью обратных элементов к элементам из gh служит hg , так как обратным к gh является $h^{-1}g^{-1}$. Таким образом, если gh — группа, то должно выполняться условие

$$(1) \quad hg = gh.$$

т. е. g должна быть перестановочна с h . Но это условие и достаточно; действительно, если оно выполнено, то gh вместе с каждым элементом gh содержит также обратный элемент $h^{-1}g^{-1}$ и, кроме того, вместе с каждым двумя элементами — также их произведение, ибо

$$ghgh = gghh = gh.$$

Итак, произведение двух подгрупп g и h группы $\mathfrak{G}$ тогда и только тогда является снова подгруппой этой группы, если подгруппы g и h перестановочны. Разумеется, для этого не требуется, чтобы каждый элемент из g был перестановочен с каждым элементом из h . Если условие перестановочности (1) выполнено, то произведение gh есть группа, порождённая подгруппами g и h .

В абелевой группе условие (1) всегда выполнено. Если абелева группа записана аддитивно, так что g и h суть подмодули некоторого модуля, то вместо gh пишут (g, h) , обозначение же $g + h$ резервируется для исследуемого позже специального случая «прямой суммы».

Пусть g — подгруппа и a — элемент группы $\mathfrak{G}$. Комплекс ag называют *левым смежным классом*, а комплекс ga — *правым смеж-*

ным классом группы $\mathfrak{G}$ по подгруппе g . Если a лежит в g , то $ag = g$; таким образом, всегда одним из левых (равно как и одним из правых) смежных классов по подгруппе g служит сама эта подгруппа.

В дальнейшем будут рассматриваться большей частью левые смежные классы, но все результаты будут в равной мере справедливы и для правых смежных классов.

Два смежных класса ag , bg могут совпадать и без того, чтобы $a = b$. А именно, всякий раз, как $a^{-1}b$ лежит в g , имеем:

$$bg = aa^{-1}bg = a(a^{-1}bg) = ag.$$

Два различных смежных класса не имеют ни одного общего элемента. Действительно, если смежные классы ag и bg имеют общий элемент, скажем,

$$ag_1 = bg_2,$$

то отсюда следует, что

$$g_1 g_2^{-1} = a^{-1}b,$$

так что $a^{-1}b$ лежит в g ; но тогда, по предыдущему, ag и bg совпадают.

Каждый элемент a принадлежит к некоторому смежному классу, а именно, к классу ag , так как последний заведомо содержит элемент $ag = a$. При этом, по только что доказанному, элемент a принадлежит лишь к одному смежному классу. Мы можем поэтому рассматривать каждый элемент a в качестве *представителя* содержащего его смежного класса ag .

В силу всего сказанного, смежные классы образуют *разбиение* группы $\mathfrak{G}$ на классы. Каждый элемент принадлежит одному и только одному классу¹⁾.

Каждые два смежных класса равноможны, так как соответствием $ag \rightarrow bg$ устанавливается взаимно однозначное отображение ag на bg .

За исключением самой подгруппы g , смежные классы по ней не являются группами, так как группа должна содержать единицу.

Число различных смежных классов группы $\mathfrak{G}$ по подгруппе g называется *индексом* g в $\mathfrak{G}$. Индекс может быть конечным или бесконечным.

¹⁾ В литературе часто встречается введенная Галуа запись:

$$\mathfrak{G} = a_1g + a_2g + \dots,$$

которая должна означать, что классы $a_i g$ попарно взаимно просты и в совокупности исчерпывают всю группу $\mathfrak{G}$. Мы не будем пользоваться этим способом записи, так как резервируем знак $+$ для вводимых дальше прямых сумм.

Пусть N — порядок группы $\mathfrak{G}$ (предполагаемый конечным), n — порядок подгруппы g и j — индекс g в $\mathfrak{G}$. Тогда имеет место соотношение

$$(2) \quad N = jn.$$

Действительно, $\mathfrak{G}$ разбивается на j классов, в каждом из которых содержится по n элементов¹⁾.

Из соотношения (2) можно в случае конечных групп определить индекс j :

$$j = \frac{N}{n}.$$

Следствие. Порядок подгруппы конечной группы есть делитель порядка всей группы.

Беря, в частности, в качестве подгруппы циклическую группу, порождённую некоторым элементом s , получаем:

Порядок элемента конечной группы есть делитель порядка группы.

Из этого предложения в качестве непосредственного следствия вытекает, что в группе, состоящей из n элементов, для каждого элемента a имеет место равенство $a^n = e$.

Может случиться, что все левые смежные классы ag служат одновременно правыми смежными классами. Если это имеет место, то тот левый смежный класс, в котором лежит произвольно заданный элемент a , должен совпадать с правым смежным классом, содержащим a , т. е. для каждого a должно быть

$$(3) \quad ag = ga.$$

Подгруппу g , обладающую свойством (3), т. е. перестановочную с каждым элементом a из $\mathfrak{G}$, называют нормальным делителем²⁾ или *инвариантной подгруппой* группы $\mathfrak{G}$.

Если g — нормальный делитель, то произведение двух смежных классов есть снова смежный класс:

$$ag \cdot bg = a \cdot gb \cdot g = abgg = abg.$$

Задача 1. Определить правые и левые смежные классы для подгрупп группы $\mathfrak{S}_3$. Какие из этих подгрупп являются нормальными делителями?

¹⁾ Это соотношение остаётся в силе и в случае бесконечного N ; но для точного определения его смысла в этом случае нужно ввести понятие произведения кардинальных чисел, чего мы здесь не делали.

²⁾ Название расшифровывается следующим образом: делитель означает здесь подгруппу, а слово «нормальный» должно выражать отличительное свойство $ag = ga$.

Задача 2. Показать, что для произвольной подгруппы элементы, обратные к элементам левого смежного класса, образуют правый смежный класс. Вывести отсюда, далее, что индекс может быть определён также, как число правых смежных классов.

Задача 3. Показать, что каждая подгруппа индекса 2 является нормальным делителем. Пример: знакопеременная группа в симметрической группе.

Задача 4. Подгруппа абелевой группы всегда является нормальным делителем.

Задача 5. Элементы группы, перестановочные с каждым её элементом, образуют в группе нормальный делитель («центр» группы).

Задача 6. Если $\mathfrak{G}$ — циклическая группа, порождённая элементом a , и g — отличная от $\mathfrak{G}$ подгруппа, порождённая степенью a^m с минимальным положительным m (см. § 7), то 1, a , a^2 , ..., a^{m-1} суть представители всех смежных классов, а m есть индекс g в $\mathfrak{G}$.

Задача 7. Если произведение любых двух левых смежных классов группы $\mathfrak{G}$ по подгруппе g есть снова левый смежный класс, то g есть нормальный делитель в $\mathfrak{G}$.

§ 9. Изоморфизмы и автоморфизмы.

Пусть даны два множества $\mathfrak{M}$, $\overline{\mathfrak{M}}$, в каждом из которых определены некоторые соотношения между элементами. Например, множества $\mathfrak{M}$, $\overline{\mathfrak{M}}$ могут быть группами, а соотношениями — служить равенства $a \cdot b = c$, существующие в силу наличия групповой операции; либо, скажем, множества упорядочены и рассматриваемые соотношения суть неравенства $a > b$.

Если эти множества можно так взаимно однозначно отобразить одно на другое, чтобы определённые в них соотношения при отображении не нарушились, т. е. если каждому элементу a из $\mathfrak{M}$ можно взаимно однозначно отнести элемент $\bar{a}$ из $\overline{\mathfrak{M}}$ так, чтобы соотношения, существующие между любыми элементами $a, b, \dots$ из $\mathfrak{M}$, имели место и между соответствующими элементами $\bar{a}, \bar{b}, \dots$, и обратно, — то эти множества называют *изоморфными* (относительно рассматриваемых соотношений); пишут $\mathfrak{M} \cong \overline{\mathfrak{M}}$. Само же это взаимно однозначное соответствие между элементами множеств $\mathfrak{M}$ и $\overline{\mathfrak{M}}$, сохраняющее определённые в них соотношения, называют *изоморфизмом*.

Так, можно говорить об *изоморфных группах*, об изоморфно упорядоченных или *подобно упорядоченных* множествах, и т. д. Таким образом, изоморфизм двух групп есть такое взаимно однозначное отображение $a \rightarrow \bar{a}$, при котором из $ab = c$ следует $\bar{a}\bar{b} = \bar{c}$ (и обратно), т. е. при котором произведению ab всегда отвечает произведение $\bar{a}\bar{b}$.

Подобно тому как в общей теории множеств равномошные множества считаются равнозначными, так и подобные множества в теории порядковых типов и изоморфные группы в теории групп рассматриваются как несущественно различные. Все понятия и теоремы, которые могут быть определены и доказаны на основании одних лишь заданных соотношений между элементами некоторого множества, непосредственно переносятся на всякое изоморфное ему множество. Например, множество, в котором определено произведение элементов и которое изоморфно некоторой группе, само является группой, причём единица, обратные элементы и подгруппы переходят при изоморфизме снова в единицу, обратные элементы и подгруппы.

Если, в частности, оба множества M , $\bar{M}$ совпадают, т. е. рассматриваемое взаимно однозначное соответствие относит каждому элементу a элемент $\bar{a}$ того же множества с сохранением соотношений, то это соответствие называется *автоморфизмом*.

Например, если M — множество всех целых чисел, а основное соотношение есть соотношение порядка $a < b$, то соответствие

$$a \rightarrow a + 1$$

есть автоморфизм, так как при этом соответствии множество всех целых чисел взаимно однозначно отображается на себя, и из $a < b$ следует $a + 1 < b + 1$ и обратно.

Автоморфизмы множества в известной степени выражают его свойства симметрии. Действительно, что, например, представляет собой симметрия геометрической фигуры? Она означает, что при некоторых преобразованиях (отражениях, вращениях и т. п.) фигура переходит в себя, причём некоторые соотношения (расстояния, углы, взаимное расположение) сохраняются в силе, или, в нашей терминологии, что фигура допускает некоторые автоморфизмы по отношению к её метрическим свойствам.

Очевидно, произведение двух автоморфизмов (в смысле произведения преобразований по § 6), равно как и преобразование, обратное к автоморфизму, снова есть автоморфизм. Отсюда, по § 6, следует, что автоморфизмы произвольного множества (с произвольными соотношениями между его элементами) составляют группу преобразований: *группу автоморфизмов* этого множества.

В частности, автоморфизмы группы, в свою очередь, образуют группу. Некоторые из этих автоморфизмов мы рассмотрим сейчас подробнее.

Для каждого фиксированного элемента группы a соответствие, переводящее x в

(1)

$$\bar{x} = axa^{-1}.$$

есть автоморфизм. Действительно, во-первых, уравнение (1) однозначно разрешимо относительно x :

$$x = a^{-1}\bar{a};$$

таким образом, соответствие взаимно однозначно. Во-вторых,

$$\overline{xy} = axa^{-1} \cdot aya^{-1} = a(xy)a^{-1} = \overline{xy};$$

таким образом, соответствие — изоморфное.

Элемент axa^{-1} называют *элементом, полученным из x трансформированием с помощью a* ; элементы x , axa^{-1} называют *сопряжёнными элементами* группы. Автоморфизмы $x \rightarrow axa^{-1}$, порождённые элементами a , называют *внутренними автоморфизмами* группы. Все остальные автоморфизмы (в случае, если таковые существуют) называются *внешними автоморфизмами*.

При внутреннем автоморфизме $x \rightarrow axa^{-1}$ произвольная подгруппа g переходит в подгруппу aga^{-1} , называемую *сопряжённой с g* .

Если подгруппа g совпадает со всеми с ней сопряжёнными:

$$(2) \quad aga^{-1} = g \text{ для каждого } a,$$

то это означает не что иное, как то, что группа g перестановочна с каждым элементом a :

$$ag = ga,$$

и тем самым g является нормальным делителем (§ 8). Итак:

Подгруппы, инвариантные относительно всех внутренних автоморфизмов, суть нормальные делители.

Этой теоремой и объясняется наименование нормального делителя «инвариантной подгруппой».

Требование (2) может быть заменено несколько более слабым:

$$(3) \quad aga^{-1} \subseteq g.$$

Действительно, если (3) имеет место для всех a , то оно имеет место и для a^{-1} :

$$a^{-1}ga \subseteq g,$$

откуда

$$(4) \quad g \subseteq aga^{-1};$$

но из (3) и (4) следует (2). Таким образом:

Подгруппа есть нормальный делитель, если она вместе с каждым элементом b содержит также все сопряжённые с ним элементы aba^{-1} .

Задача 1. Абелевы группы не имеют никаких внутренних автоморфизмов, кроме тождественного. Показать, что группа

$$e, a, b, c$$

с единицей e и определяющими соотношениями

$$a^2 = b^2 = c^2 = e,$$

$$ab = ba = c,$$

$$bc = cb = a,$$

$$ca = ac = b,$$

не имеет никаких внутренних автоморфизмов, кроме тождественного, но обладает пятью внешними автоморфизмами.

Задача 2. В группах подстановок элемент aba^{-1} , полученный из b трансформированием с помощью a , можно вычислить, представив b в виде произведения циклов (§ 7) и подвергнув цифры в этих циклах подстановке a . Дать доказательство. Основываясь на этой теореме, вычислить aba^{-1} для случая

$$b = (12)(345), \quad a = (2345).$$

$ba^{-1} = (k_1, k_2) \quad aba^{-1} = b = (12)(345),$
 $= (k_1, k_2) = (k_1, k_2)$
 $(b = (mn) \dots \quad a^{-1} = (k_1, k_2, \dots, k_m)$
 $a = (k_1, k_2, \dots, k_n)$

Задача 3. Доказать, что симметрическая группа S_3 не имеет ни одного внешнего автоморфизма и имеет шесть внутренних.

Задача 4. Симметрическая группа S_4 , кроме самой себя и единичной подгруппы, имеет ещё лишь следующие нормальные делители:

а) знакопеременную группу A_4 ,

б) «четверную группу Клейна» V_4 , состоящую из подстановок

$$(1), (12)(34), (13)(24), (14)(23).$$

Последняя группа абелева и изоморфна группе, абстрактно определённой в задаче 1.

Задача 5. Если $\mathfrak{g}$ — нормальный делитель в $\mathfrak{G}$ и $\mathfrak{H}$ — «промежуточная группа»:

$$\mathfrak{g} \subseteq \mathfrak{H} \subseteq \mathfrak{G},$$

то $\mathfrak{g}$ будет также нормальным делителем в $\mathfrak{H}$.

Задача 6. Все бесконечные циклические группы изоморфны аддитивной группе целых чисел.

Задача 7. Элементы x группы $\mathfrak{G}$, перестановочные с элементом a , т. е. такие, что

$$xa = ax,$$

образуют группу — *нормализатор* элемента a . Эта группа содержит в качестве нормального делителя циклическую подгруппу, порождённую элементом a . Число элементов, сопряжённых с a , равно индексу нормализатора элемента a в $\mathfrak{G}$.

Задача 8. Элементы группы $\mathfrak{G}$ можно разбить на классы сопряжённых элементов. Число элементов класса, в случае конечности

группы $\mathcal{G}$, есть делитель порядка этой группы. Единичный элемент, равно как и каждый элемент центра (§ 8, задача 5), образует сам по себе класс.

Задача 9. Если в группе порядка p^n , где p — простое число, a_λ означает число классов с p^λ элементами, в частности, a_0 — число элементов центра, то

$$p^n = a_0 + a_1 p + a_2 p^2 + \dots$$

Вывести из этого равенства, что центр группы порядка p^n не может состоять из одной лишь единицы.

§ 10. Гомоморфизмы. Нормальные делители. Факторгруппы.

Если в двух множествах $\mathcal{M}$, $\overline{\mathcal{M}}$ определены некоторые соотношения между элементами и если каждому элементу a из $\mathcal{M}$ поставлен в соответствие один и только один элемент $\bar{a}$ из $\overline{\mathcal{M}}$ так, что:

1) каждый элемент $\bar{a}$ из $\overline{\mathcal{M}}$ является образом по меньшей мере одного элемента из $\mathcal{M}$,

2) все соотношения между элементами из $\mathcal{M}$ выполняются и для соответствующих им элементов из $\overline{\mathcal{M}}$, —

то это соответствие называется *гомоморфизмом*. $\overline{\mathcal{M}}$ называется тогда *гомоморфным образом* множества $\mathcal{M}$ или, кратко, *гомоморфным* с $\mathcal{M}$; пишут: $\mathcal{M} \sim \overline{\mathcal{M}}$.

Если $\overline{\mathcal{M}} \subseteq \mathcal{M}$, так что гомоморфизм есть отображение $\mathcal{M}$ в себя, то он называется *эндоморфизмом*.

Если соответствие взаимно однозначно, и гомоморфизм имеет место и в обратном направлении, то этот гомоморфизм есть *изоморфизм*.

Элементы множества $\mathcal{M}$, имеющие при гомоморфном отображении один и тот же образ $\bar{a}$ в $\overline{\mathcal{M}}$, можно объединить в один класс. Каждый элемент a принадлежит одному и только одному классу; таким образом, множество $\mathcal{M}$ разбивается на классы, находящиеся во взаимно однозначном соответствии с элементами множества $\overline{\mathcal{M}}$.

Примеры. Если мы поставим в соответствие каждому элементу группы единицу, то получим гомоморфизм этой группы с единичной группой. Точно так же получится гомоморфизм, если каждой подстановке из некоторой группы подстановок поставить в соответствие число $+1$ или -1 , смотря по тому, чётна или нечётна эта подстановка; гомоморфным образом будет служить мультипликативная группа чисел $+1$ и -1 .

Ставя в соответствие каждому целому числу m степень a^m элемента a некоторой группы, мы получим гомоморфизм аддитивной группы целых чисел с циклической группой, порождённой элементом a , ибо сумме $m+n$ будет соответствовать произведение $a^{m+n} = a^m a^n$. Если a — элемент бесконечного порядка, то этот гомоморфизм будет изоморфизмом.

Исследуем теперь специально гомоморфизмы групп.

Если в некотором множестве $\mathfrak{G}$ определены произведения $\overline{ab}$ (т. е. соотношения вида $\overline{ab} = \overline{c}$) и если некоторая группа $\mathfrak{G}$ гомоморфно отображается на $\mathfrak{G}$, то $\mathfrak{G}$ есть также группа. Коротко: гомоморфный образ группы есть снова группа.

Доказательство. Прежде всего, любые три заданных элемента $\overline{a}$, $\overline{b}$, $\overline{c}$ из $\mathfrak{G}$ служат образами некоторых элементов из $\mathfrak{G}$, например, элементов a , b , c . Из

$$ab \cdot c = a \cdot bc$$

следует тогда:

$$\overline{ab} \cdot \overline{c} = \overline{a} \cdot \overline{bc}.$$

Далее, из

$$ae = a \quad \text{для всех } a$$

следует

$$\overline{ae} = \overline{a} \quad \text{для всех } \overline{a}$$

и из

$$ba = e \quad (b = a^{-1})$$

следует

$$\overline{ba} = \overline{e}.$$

Таким образом, в $\mathfrak{G}$ существует единица $\overline{e}$ и обратный элемент для каждого $\overline{a}$. Следовательно, $\mathfrak{G}$ есть группа. Вместе с тем мы доказали, что при гомоморфизме единица и обратный элемент переходят снова в единицу и обратный элемент.

Исследуем теперь подробнее разбиение на классы, порождаемое гомоморфным отображением $\mathfrak{G} \rightarrow \mathfrak{G}$. При этом мы установим весьма важную взаимно однозначную связь между гомоморфизмами и нормальными делителями.

Класс e группы $\mathfrak{G}$, которому при гомоморфизме $\mathfrak{G} \sim \mathfrak{G}$ отвечает единица $\overline{e}$ группы $\mathfrak{G}$, является нормальным делителем в $\mathfrak{G}$, а остальные классы суть смежные классы по этому нормальному делителю.

Доказательство. Прежде всего, e есть группа. Действительно, если a и b при гомоморфизме оба переходят в $\overline{e}$, то ab

переходит в $\bar{e}^2 = \bar{e}$; таким образом, e вместе с каждым двумя элементами содержит и их произведение. Далее, a^{-1} переходит в $\bar{e}^{-1} = \bar{e}$, так что e содержит также обратные для всех своих элементов.

Элементы каждого левого смежного класса ae переходят все в один и тот же элемент $\bar{ae} = \bar{a}$. Пусть, обратно, a' переходит в $\bar{a}$. Рассмотрим элемент x , удовлетворяющий уравнению

$$ax = a'.$$

Тогда

$$\bar{ax} = \bar{a},$$

$$\bar{x} = \bar{e}.$$

Следовательно, x лежит в e и, значит, $a' — в ae$.

Таким образом, класс в $\mathfrak{G}$, соответствующий элементу $\bar{a}$, есть как раз левый смежный класс ae .

Но таким же точно образом можно показать, что классом, соответствующим элементу $\bar{a}$, должен быть правый смежный класс ea . Следовательно, правые и левые смежные классы совпадают:

$$ae = ea,$$

и, значит, e есть нормальный делитель. Тем самым всё доказано.

До сих пор мы исходили от заданного гомоморфизма и с необходимостью пришли к нормальному делителю. Теперь мы обратим постановку вопроса: Пусть задан нормальный делитель $\mathfrak{g}$ группы $\mathfrak{G}$. Можно ли образовать гомоморфную $\mathfrak{G}$ группу $\mathfrak{G}/\mathfrak{g}$ так, чтобы смежными классам группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$ отвечали как раз элементы группы $\mathfrak{G}/\mathfrak{g}$?

Чтобы добиться этого, проще всего выбрать в качестве элементов группы $\mathfrak{G}/\mathfrak{g}$, которую мы хотим построить, сами смежные классы по подгруппе $\mathfrak{g}$. Как мы видели в § 8, произведение двух смежных классов по нормальному делителю $\mathfrak{g}$ само является смежным классом, причём, если a лежит в смежном классе $a\mathfrak{g}$, а b — в смежном классе $b\mathfrak{g}$, то ab принадлежит смежному классу-произведению $ab\mathfrak{g} = a\mathfrak{g} \cdot b\mathfrak{g}$. Тем самым смежные классы образуют множество, гомоморфное с $\mathfrak{G}$, и, следовательно, группу, гомоморфную группе $\mathfrak{G}$. Эту группу называют факторгруппой группы $\mathfrak{G}$ по $\mathfrak{g}$ и обозначают символом

$$\mathfrak{G}/\mathfrak{g}.$$

Порядком группы $\mathfrak{G}/\mathfrak{g}$ служит индекс подгруппы $\mathfrak{g}$ в $\mathfrak{G}$.

Мы видим теперь принципиальную важность нормальных делителей: они дают возможность строить новые группы, гомоморфные заданной группе.

Если группа $\mathfrak{G}$ гомоморфно отображена на некоторую группу $\overline{\mathfrak{G}}$, то, как мы уже видели, элементам группы $\overline{\mathfrak{G}}$ соответствуют (взаимно однозначно) смежные классы по некоторому нормальному делителю e в $\mathfrak{G}$. Это соответствие есть, очевидно, изоморфизм. В самом деле, если ae, be — два смежных класса, то abe есть их произведение; соответствующие элементы в $\overline{\mathfrak{G}}$ суть $\bar{a}, \bar{b}, \bar{ab}$, и вследствие гомоморфизма, действительно,

$$\overline{ab} = \bar{a} \cdot \bar{b}.$$

Таким образом, мы имеем:

$$\mathfrak{G}/e \cong \overline{\mathfrak{G}}.$$

Тем самым установлена теорема о гомоморфизмах групп:

Каждая группа $\overline{\mathfrak{G}}$, на которую гомоморфно отображается $\mathfrak{G}$, изоморфна некоторой факторгруппе $\mathfrak{G}/e$; при этом e есть тот нормальный делитель группы $\mathfrak{G}$, элементам которого соответствует единица в $\overline{\mathfrak{G}}$. Обратно, $\mathfrak{G}$ гомоморфно отображается на каждую свою факторгруппу $\mathfrak{G}/e$ (где e — нормальный делитель).

Задача 1. Тривиальными факторгруппами каждой группы $\mathfrak{G}$ являются: $\mathfrak{G}/\mathfrak{G} \cong \mathfrak{G}$ и $\mathfrak{G}/\mathfrak{G} \cong \mathfrak{E}$.

Задача 2. Факторгруппа $\mathfrak{S}_n/\mathfrak{A}_n$ симметрической группы по знаку переменной есть циклическая группа второго порядка.

Задача 3. Факторгруппа $\mathfrak{S}_4/\mathfrak{V}_4$ симметрической группы четвертой степени по четверной группе Клейна (§ 9, задача 4) изоморфна с $\mathfrak{S}_3$.

Задача 4. Элементы $aba^{-1}b^{-1}$ группы $\mathfrak{G}$ и всевозможные их конечные произведения образуют подгруппу, называемую *коммутантом* группы $\mathfrak{G}$. Она является нормальным делителем, а факторгруппа по ней абелева. Каждый нормальный делитель, факторгруппа по которому абелева, содержит коммутант.

Задача 5. Множество всех элементов, перестановочных с подгруппой $\mathfrak{g}$, представляет собою подгруппу $\mathfrak{h}$, в которой $\mathfrak{g}$ является нормальным делителем. Её называют *нормализатором* подгруппы $\mathfrak{g}$. Индекс $\mathfrak{h}$ в $\mathfrak{G}$ равен числу подгрупп группы $\mathfrak{G}$, сопряжённых с $\mathfrak{g}$.

Задача 6. Если $\mathfrak{G}$ — циклическая группа, a — элемент, порождающий $\mathfrak{G}$, и $\mathfrak{g}$ — подгруппа индекса m , то $\mathfrak{G}/\mathfrak{g}$ есть циклическая группа порядка m (см. § 8, задача 6).

В абелевой группе каждая подгруппа является нормальным делителем (см. § 8, задача 4). Если групповая композиция записывается в виде сложения, то группы и их подгруппы, как уже упоминалось, называют *модулями*. Смежные классы $a + \mathfrak{M}$ (где $\mathfrak{M}$ есть модуль) называют *классами вычетов* по $\mathfrak{M}$ или *классами вычетов по модулю $\mathfrak{M}$* , а факторгруппа $\mathfrak{G}/\mathfrak{M}$ называется *фактормодулем $\mathfrak{G}$ по $\mathfrak{M}$* .

Два элемента a, b лежат в одном классе вычетов, если их разность лежит в $\mathfrak{M}$. Такие два элемента называют *сравнимыми по модулю $\mathfrak{M}$* ; пишут:

$$a \equiv b \pmod{\mathfrak{M}}$$

или, короче,

$$a \equiv b \pmod{\mathfrak{M}}.$$

Для соответствующих при гомоморфизме элементов $\bar{a}, \bar{b}$ фактормодуля имеем тогда:

$$\bar{a} = \bar{b}.$$

И обратно, из $\bar{a} = \bar{b}$ следует всегда $a \equiv b \pmod{\mathfrak{M}}$.

Например, в области целых чисел кратные натурального числа m образуют модуль; в соответствии с этим, если разность $a - b$ делится на m , будем писать:

$$a \equiv b \pmod{m}.$$

Классы вычетов могут быть представлены числами $0, 1, 2, \dots, m-1$, а фактормодуль есть циклическая группа порядка m .

Задача 7. Каждая циклическая группа порядка m изоморфна фактормодулю модуля целых чисел по целому числу m .

ГЛАВА ТРЕТЬЯ.

КОЛЬЦА И ПОЛЯ.

Содержание: Определение понятий кольца, области целостности, поля. Общие методы образования из колец других колец (соотв. полей). Теоремы о разложении на простые множители в областях целостности.

Понятия, вводимые в этой главе, используются на протяжении всей книги.

§ 11. Кольца.

В алгебре и арифметике оперируют величинами различной природы; это могут быть целые, рациональные, вещественные, комплексные или алгебраические числа, либо полиномы или рациональные функции n переменных и т. д. Позже мы познакомимся ещё с величинами совершенно другой природы: гиперкомплексными числами, классами вычетов и т. п., с которыми можно оперировать так же или почти так же, как с числами. Поэтому желательно объединить все эти области величин одним общим понятием и исследовать законы операций в этих областях в общем виде.

Под *системой с двойной композицией* понимают множество элементов $a, b, \dots$, в котором для каждого двух элементов a, b однозначно определены сумма $a + b$ и произведение $a \cdot b$, принадлежащие тому же множеству.

Система с двойной композицией называется *кольцом*, если операции над элементами системы подчиняются следующим законам:

I. Законы сложения.

- a) Закон ассоциативности: $a + (b + c) = (a + b) + c$.
- b) Закон коммутативности: $a + b = b + a$.
- c) Разрешимость¹⁾ уравнения $a + x = b$ для всех a и b .

II. Закон умножения.

- a) Закон ассоциативности: $a \cdot bc = ab \cdot c$.

¹⁾ Однозначная разрешимость не постулируется, а получается дальше как следствие.

III. Законы дистрибутивности:

$$a) a \cdot (b + c) = ab + ac.$$

$$b) (b + c) \cdot a = ba + ca.$$

Дополнение. Если для умножения имеет место также закон коммутативности:

$$II. b) a \cdot b = b \cdot a,$$

то кольцо называется *коммутативным*. На первых порах мы будем иметь дело главным образом с коммутативными кольцами.

К законам сложения. Законы I a), b), c) в совокупности означают, что элементы кольца образуют относительно сложения абелеву группу¹⁾. Таким образом, мы можем все доказанные ранее теоремы об абелевых группах перенести на кольца: существует (и притом только один) нуль 0, т. е. элемент, обладающий следующим свойством:

$$a + 0 = a \text{ для всех } a;$$

далее, для каждого элемента a существует *противоположный элемент* $-a$, со свойством:

$$-a + a = 0.$$

Затем, уравнение $a + x = b$ не только разрешимо, но и однозначно разрешимо: единственным его решением является

$$x = -a + b;$$

мы будем обозначать его также $b - a$. Так как, в силу формулы

$$a - b = a + (-b),$$

каждая разность может быть преобразована в сумму, то в этом смысле и для разностей имеют место те же правила перестановки действий, что и для сумм, например,

$$(a - b) - c = (a - c) - b,$$

и т. д. Наконец, $-(-a) = a$ и $a - a = 0$.

К законам ассоциативности. Как мы видели в гл. 2, § 6, основываясь на законе ассоциативности умножения, можно определить сложные произведения

$$\prod_1^n a_i = a_1 a_2 \dots a_n$$

и доказать основное их свойство

$$\prod_1^m a_i \cdot \prod_{i=1}^n a_{m+i} = \prod_1^{m+n} a_i.$$

¹⁾ Эту группу называют *аддитивной группой кольца*.

Подобным же образом можно определить суммы

$$\sum_1^n a_v = a_1 + a_2 + \dots + a_n$$

и доказать основное их свойство

$$\sum_1^m a_\mu + \sum_{\nu=1}^n a_{m+\nu} = \sum_1^{m+n} a_\nu.$$

Кроме того, в силу Ib), можно в сумме произвольным образом переставлять слагаемые, и то же имеет место в коммутативных кольцах для произведений.

К законам дистрибутивности. В случае, когда имеет место закон коммутативности умножения, III b) является, конечно, следствием III a).

Из III a) непосредственно следует полной индукцией по n :

$$a(b_1 + b_2 + \dots + b_n) = ab_1 + ab_2 + \dots + ab_n,$$

и точно так же из III b):

$$(a_1 + a_2 + \dots + a_n)b = a_1b + a_2b + \dots + a_nb.$$

Совместное применение обоих правил даёт обычное правило перемножения сумм:

$$\begin{aligned} (a_1 + \dots + a_n)(b_1 + \dots + b_m) &= \\ &= a_1b_1 + \dots + a_1b_m + \\ &\quad + \dots + a_nb_1 + \dots + a_nb_m = \\ &= \sum_{i=1}^n \sum_{k=1}^m a_ib_k. \end{aligned}$$

Законы дистрибутивности имеют место также для вычитания, например,

$$a(b - c) = ab - ac,$$

как это следует из равенства

$$a(b - c) + ac = a(b - c + c) = ab.$$

В частности,

$$a \cdot 0 = a(a - a) = a \cdot a - a \cdot a = 0,$$

или: если один из сомножителей равен нулю, то произведение равно нулю. Ниже мы увидим на примерах, что обратное может и не иметь места: может случиться, что

$$a \cdot b = 0, \quad a \neq 0, \quad b \neq 0.$$

В этом случае a и b называют *делителями нуля*, и притом a — левым, а b — правым делителем нуля. (В коммутативных кольцах оба эти понятия совпадают.) Целесообразно и сам нуль считать делителем нуля. Таким образом, a называется левым делителем нуля, если существует такое $b \neq 0$, что $ab = 0$ ¹⁾.

Если в кольце нет делителей нуля, кроме самого нуля, т. е. если из $ab = 0$ всегда следует, что $a = 0$ или $b = 0$, то такое кольцо называют *кольцом без делителей нуля*. Если кольцо, к тому же, коммутативно, то его называют тогда также *областью целостности*.

Примеры. Все упомянутые в начале этого параграфа примеры (кольцо целых чисел, рациональных чисел и т. д.) суть примеры колец без делителей нуля. Кольцо непрерывных функций, определённых в интервале $(-1, +1)$, содержит делители нуля; действительно, положив

$$f = f(x) = \max(0, x),$$

$$g = g(x) = \max(0, -x),$$

будем иметь: $f \neq 0$ ²⁾, $g \neq 0$, $fg = 0$.

Задача 1. Числовые пары (a_1, a_2) (где a_1, a_2 , скажем, — рациональные числа) со сложением и умножением, определёнными формулами

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2),$$

образуют кольцо с делителями нуля.

Задача 2. Равенство $ax = ay$ можно сократить на a в случае, если a не есть левый делитель нуля. (В частности, в области целостности можно сокращать на каждое $a \neq 0$.)

Задача 3. Построить, исходя из любой абелевой группы, кольцо, имеющее эту группу своей аддитивной группой и обладающее тем свойством, что произведение любых двух его элементов равно нулю.

Единица. Если кольцо обладает некоторой левой единицей e :

$$ex = x \text{ для всех } x,$$

и одновременно — некоторой правой единицей e' :

$$xe' = x \text{ для всех } x,$$

то обе они должны совпадать, так как

$$e = ee' = e'.$$

¹⁾ В предположении, что в данном кольце вообще существуют элементы $\neq 0$.

²⁾ $f \neq 0$ означает: f есть функция, не равная тождественно нулю, но отнюдь не означает, что f вообще нигде не принимает значения 0.

Точно так же тогда каждая правая единица, равно как и каждая левая единица равна e . В этом случае e называют просто единицей и говорят, что данное кольцо есть *кольцо с единицей*. Мы будем часто обозначать единицу символом 1, но при этом надо помнить, что его следует отличать от числа 1.

Все целые числа образуют кольцо S с единицей, одни чётные числа — кольцо без единицы. Существуют также кольца, в которых имеются одна или несколько правых единиц, но нет ни одной левой единицы, или наоборот.

Обратный элемент. Пусть a — произвольный элемент кольца с единицей e . Под *левым обратным* к a понимают элемент $a_{(l)}^{-1}$, обладающий тем свойством, что

$$a_{(l)}^{-1}a = e$$

и под *правым обратным* к a — элемент $a_{(r)}^{-1}$ со свойством

$$aa_{(r)}^{-1} = e.$$

Если элемент a обладает как некоторым левым, так и некоторым правым обратным, то они снова равны между собой; действительно,

$$a_{(l)}^{-1} = a_{(l)}^{-1}(aa_{(r)}^{-1}) = (a_{(l)}^{-1}a)a_{(r)}^{-1} = a_{(r)}^{-1}.$$

Поэтому им равен также каждый правый и каждый левый обратный к a . В этом случае говорят: a *обладает обратным элементом*, и обозначают обратный элемент через a^{-1} .

Степени и кратные. Мы видели уже в гл. 2, что, основываясь на законе ассоциативности, можно определить степени a^n (где n — произвольное натуральное число) для всякого элемента a кольца, причём эти степени подчиняются обычным правилам:

$$(1) \quad \begin{cases} a^n \cdot a^m = a^{n+m}, \\ (a^n)^m = a^{nm}, \\ (a^h)^n = a^{hn}, \end{cases}$$

последнее — для коммутативных колец.

Если в кольце есть единица и a обладает обратным элементом, то можно ввести также нулевую и отрицательные степени элемента a (§ 6); при этом правила (1) сохраняют силу.

Подобным же образом можно определить в аддитивной группе кратные

$$n \cdot a \quad (= a + a + \dots + a, \text{ с } n \text{ слагаемыми}),$$

¹⁾ В работе Р. Бэра, *Bull. Amer. Math. Soc.* 48 (1942), 630—638, указаны некоторые условия для существования в кольце единицы и обратных элементов, а также связь этих понятий с делителями нуля. *Ред.*

причём будем иметь:

$$(2) \quad \begin{cases} na + ma = (n + m)a, \\ n \cdot ma = nm \cdot a, \\ n(a + b) = na + nb, \\ n \cdot ab = na \cdot b = a \cdot nb. \end{cases}$$

Если положить

$$(-n) \cdot a = -na,$$

то правила (2) будут верны для всех целых n и m (положительных, отрицательных и равных нулю).

Мы предостерегаем от понимания выражения $n \cdot a$ как настоящего произведения двух элементов кольца, ибо n , вообще говоря, есть вовсе не элемент кольца, а нечто извне привнесённое: целое число. Но если кольцо обладает единицей e , то na можно записать в виде настоящего произведения, а именно:

$$na = n \cdot ea = ne \cdot a.$$

Задача 4. Левый делитель нуля не может обладать левым обратным, а правый делитель нуля — правым обратным элементом. В частности, нуль не обладает ни левым, ни правым обратным элементом, если только исключить тот тривиальный случай, когда кольцо состоит из одного лишь элемента 0, который тогда есть одновременно и единица и собственный обратный элемент («нулевое кольцо»).

Задача 5. Доказать для произвольных коммутативных колец полной индукцией по n биномиальную теорему:

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + b^n,$$

где $\binom{n}{k}$ означает целое число

$$\frac{n(n-1)\dots(n-k+1)}{1 \cdot 2 \dots k} = \frac{n!}{(n-k)! k!}.$$

Задача 6. В кольце, состоящем из n элементов, для каждого a имеет место равенство

$$n \cdot a = 0.$$

[См. § 8, где было доказано соотношение $a^n = e$.]

Задача 7. Если a перестановочно с b , т. е. если $ab = ba$, то a перестановочно также с $-b$, nb и b^{-1} . Если a перестановочно с b и с c , то также с $b + c$ и bc .

Тело. Кольцо называется *телом*, если

а) оно содержит по меньшей мере один элемент, отличный от нуля, и

b) уравнения

$$(3) \quad \begin{cases} ax = b, \\ ya = b \end{cases}$$

разрешимы при всяком $a \neq 0$.

Если такое кольцо, кроме того, коммутативно, то оно называется *полем*¹⁾ или *областью рациональности*. Совершенно так же, как в случае групп (гл. 2), из а) и б) вытекает:

с) существование левой единицы e . А именно, разрешим для какого-либо $a \neq 0$ уравнение $xa = a$ и обозначим решение через e . Если тогда b произвольно, и x — решение уравнения $ax = b$, то получим:

$$eb = eax = ax = b.$$

Аналогичным образом устанавливается существование правой единицы, а значит, существование единицы вообще.

Далее, из с) непосредственно следует

д) существование левого обратного элемента a^{-1} для каждого $a \neq 0$ и точно так же существование правого обратного элемента, следовательно, существование обратного элемента вообще.

Как и для групп, можно, далее, показать, что, обратно, из с) и d) следует б).

Задача 8. Провести доказательства.

Тело не имеет делителей нуля. Действительно, из $ab = 0$, $a \neq 0$ непосредственно следует, путём умножения слева на a^{-1} , что $b = 0$.

Уравнения (3) разрешимы однозначно. Действительно, из существования двух решений x, x' , скажем, первого уравнения следовало бы, что

$$ax = ax',$$

откуда, умножая слева на a^{-1} , мы получили бы

$$x = x'.$$

Разумеется, решения уравнений (3) суть:

$$x = a^{-1}b,$$

$$y = ba^{-1}.$$

В коммутативном случае $a^{-1}b = ba^{-1}$; вместо этого пишут также $\frac{b}{a}$.

Элементы тела, отличные от нуля, образуют по умножению группу: мультипликативную группу тела.

¹⁾ Некоторые авторы называют все тела полями и различают тогда коммутативные и некоммутативные поля.

Таким образом, тело объединяет в себе две группы: мультипликативную и аддитивную. Эти группы связаны друг с другом законом дистрибутивности.

Пример 1. Рациональные числа, вещественные числа, комплексные числа образуют поля.

Пример 2. Следующее построение даёт поле, состоящее из двух лишь элементов 0 и 1. Элементы поля перемножаются как числа 0 и 1. Элемент 0 служит нулём относительно сложения:

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1;$$

наконец, полагаем $1 + 1 = 0$. Сложение совпадает с законом композиции в циклической группе второго порядка (§ 7); таким образом, законы сложения здесь удовлетворяются. Справедливы и законы умножения, поскольку они имеют место для обычных чисел 0 и 1. Первый закон дистрибутивности доказываем путём рассмотрения всех возможных случаев: там, где входит нуль, он тривиален; остаётся, таким образом, проверить равенство

$$1 \cdot (1 + 1) = 1 \cdot 1 + 1 \cdot 1,$$

но оно сводится к равенству

$$0 = 0.$$

Наконец, уравнение $1 \cdot x = a$ разрешимо для всякого a : решением служит $x = a$.

Задача 9. Построить поле, составленное из трёх элементов. [Рассмотреть сначала, каково может быть строение его аддитивной и мультипликативной групп.]

Задача 10. Область целостности, состоящая из конечного числа элементов, есть поле. (Ср. соответствующую теорему теории групп в гл. 2, § 6.)

§ 12. Гомоморфизм и изоморфизм.

Пусть $\mathfrak{S}$ и $\bar{\mathfrak{S}}$ — системы с двойной композицией, и пусть $\mathfrak{S}$ отображена на $\bar{\mathfrak{S}}$ так, что каждому a из $\mathfrak{S}$ соответствует одно и только одно $\bar{a}$ из $\bar{\mathfrak{S}}$ и, обратно, каждое $\bar{a}$ из $\bar{\mathfrak{S}}$ соответствует по меньшей мере одному a из $\mathfrak{S}$. Это отображение называется *гомоморфизмом*, если из $a \rightarrow \bar{a}$ и $b \rightarrow \bar{b}$ всегда следует

$$a + b \rightarrow \bar{a} + \bar{b}$$

и

$$a \cdot b \rightarrow \bar{a} \cdot \bar{b}.$$

$\bar{\mathfrak{S}}$ называется тогда *гомоморфным образом* системы $\mathfrak{S}$. Пишем: $\mathfrak{S} \sim \bar{\mathfrak{S}}$.

Если отображение, кроме того, взаимно однозначно, т. е. каждое $\bar{a}$ соответствует только одному a , то такое отображение называется *изоморфизмом*. Пишем: $\mathfrak{S} \cong \bar{\mathfrak{S}}$. Системы $\mathfrak{S}$, $\bar{\mathfrak{S}}$ называют тогда *изоморфными*. Соотношение $\mathfrak{S} \cong \bar{\mathfrak{S}}$ рефлексивно, транзитивно и, поскольку отображение, обратное к изоморфизму, есть снова изоморфизм, — также симметрично.

Гомоморфный образ кольца есть снова кольцо.

Доказательство. Пусть $\mathfrak{R}$ — кольцо, $\bar{\mathfrak{R}}$ — система с двойной композицией и $\mathfrak{R} \sim \bar{\mathfrak{R}}$. Нам нужно показать, что $\bar{\mathfrak{R}}$ также есть кольцо. Доказательство проводится, как и для групп (§ 10), следующим образом.

Если $\bar{a}$, $\bar{b}$, $\bar{c}$ — любые три элемента из $\bar{\mathfrak{R}}$, и мы хотим доказать выполнение, например, закона дистрибутивности $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$, то берём какие-либо три прообраза a , b , c , соответственно, для элементов $\bar{a}$, $\bar{b}$, $\bar{c}$. Так как $\mathfrak{R}$ — кольцо, то $a(b + c) = ab + ac$, а отсюда, в силу гомоморфности, следует, что и $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$. Так же поступаем и для установления всех законов ассоциативности, коммутативности и дистрибутивности. Для доказательства разрешимости уравнения $\bar{a} + \bar{x} = \bar{b}$ снова берём прообразы a , b , разрешаем уравнение $a + x = b$ и тогда, в силу гомоморфности, имеем $\bar{a} + \bar{x} = \bar{b}$.

Нуль 0 кольца $\mathfrak{R}$ и противоположному элементу $-a$ для каждого a соответствуют при гомоморфизме снова нуль и противоположный элемент в $\bar{\mathfrak{R}}$. Если $\mathfrak{R}$ имеет единицу e , то ей соответствует единица в $\bar{\mathfrak{R}}$.

Доказательство — такое же, как и для аналогичного предложения теории групп:

$$\text{из } a + 0 = a \quad \text{следует} \quad \bar{a} + \bar{0} = \bar{a};$$

$$\text{из } -a + a = 0 \quad \text{следует} \quad (-\bar{a}) + \bar{a} = \bar{0};$$

$$\text{из } ae = a \quad \text{следует} \quad \bar{a}\bar{e} = \bar{a}.$$

Очевидно, если $\mathfrak{R}$ коммутативно, то и $\bar{\mathfrak{R}}$ коммутативно.

Гомоморфный образ $\bar{\mathfrak{R}}$ области целостности $\mathfrak{R}$, как мы ниже увидим, может уже не быть областью целостности; точно так же $\bar{\mathfrak{R}}$ может быть, а $\mathfrak{R}$ — не быть областью целостности. Однако, если отображение изоморфно, то, разумеется, все алгебраические свойства кольца $\mathfrak{R}$ переносятся и на $\bar{\mathfrak{R}}$. Отсюда следует:

Изоморфный образ области целостности (поля) есть снова область целостности (поле).

Следующая теорема, выглядящая почти тривиальной, будет, однако, играть в дальнейшем важную роль:

Пусть $\mathfrak{R}$ и $\mathfrak{S}'$ — два непересекающихся кольца. Если $\mathfrak{S}'$ содержит подкольцо $\mathfrak{R}'$, изоморфное кольцу $\mathfrak{R}$, то существует также кольцо $\mathfrak{S} \cong \mathfrak{S}'$, содержащее $\mathfrak{R}$ как подкольцо.

Доказательство. Удалим из $\mathfrak{S}'$ элементы подкольца $\mathfrak{R}'$, заменив их соответствующими им в силу изоморфизма элементами из $\mathfrak{R}$. Затем определим суммы и произведения незамещённых и замещённых элементов так, чтобы они в точности соответствовали суммам и произведениям из $\mathfrak{S}'$. (Если, например, до замены $a'b' = c'$ и если a' заменяется на a , тогда как b' и c' заменой не затрагиваются, то полагаем по определению: $ab' = c'$.) Этим способом, из $\mathfrak{S}'$ получается кольцо $\mathfrak{S} \cong \mathfrak{S}'$, действительно содержащее $\mathfrak{R}$.

§ 13. Отношения.

Если коммутативное кольцо $\mathfrak{R}$ вложено в тело Ω , то в Ω можно образовать из элементов кольца $\mathfrak{R}$ отношения

$$\frac{a}{b} = ab^{-1} = b^{-1}a \quad (b \neq 0)^1).$$

Они подчиняются следующим законам:

$$(1) \quad \begin{cases} \frac{a}{b} = \frac{c}{d} \text{ тогда и только тогда, если } ad = bc; \\ \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}; \\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \end{cases}$$

Для доказательства замечаем, что во всех случаях умножение обеих частей на bd даёт один и тот же результат и что из $bdx = bdy$ следует $x = y$.

Легко доказать, что отношения $\frac{a}{b}$ образуют поле P ; его называют полем отношений коммутативного кольца $\mathfrak{R}$. Далее, из формул (1) видно, что мы будем знать, как сравнивать, складывать и перемножать дроби, коль скоро можем производить эти операции с их числителями и знаменателями, т. е. с элементами кольца $\mathfrak{R}$. Иными словами, структура поля отношений P вполне определяется структурой кольца $\mathfrak{R}$, или: поля отношений изоморфных колец изоморфны. В частности, любые два поля отношений одного и того же кольца изоморфны, или: поле отношений P с точностью до изоморфизма однозначно определяется кольцом $\mathfrak{R}$, если только для этого кольца вообще существует поле отношений.

Поставим теперь вопрос: какие коммутативные кольца обладают полем отношений? Или, что сводится к тому же: какие вообще коммутативные кольца могут быть вложены в поле?

¹⁾ Из $ab = ba$, умножением слева и справа на b^{-1} , получаем $ab^{-1} = b^{-1}a$.

Для того чтобы кольцо $\mathfrak{R}$ могло быть вложено в тело (в частности, в поле), необходимо, прежде всего, чтобы в $\mathfrak{R}$ не было делителей нуля, так как тело (поле) делителей нуля содержать не может. Для коммутативного случая это условие также и достаточно: каждая область целостности $\mathfrak{R}$ может быть вложена в поле¹⁾.

Доказательство. Мы можем исключить из рассмотрения тот тривиальный случай, когда $\mathfrak{R}$ состоит из одного лишь нуля. Рассмотрим множество всех пар элементов (a, b) , где $b \neq 0$. Этим парам будут далее сопоставлены дроби $\frac{a}{b}$.

Положим $(a, b) \sim (c, d)$, если $ad = bc$. [Ср. первую из приведённых выше формул (1).] Определённое таким образом соотношение $\sim$, очевидно, рефлексивно и симметрично; оно также транзитивно, так как из

$$(a, b) \sim (c, d), \quad (c, d) \sim (e, f)$$

вытекает

$$ad = bc, \quad cf = de,$$

следовательно,

$$adf = bcf = bde,$$

откуда, так как $d \neq 0$ и $\mathfrak{R}$ коммутативно и не содержит делителей нуля, получаем:

$$af = be,$$

т. е.

$$(a, b) \sim (e, f).$$

Таким образом, соотношение $\sim$ обладает всеми свойствами эквивалентности; тем самым, согласно § 5 гл. 1, оно определяет для пар разбиение на классы, при котором эквивалентные пары причисляются к одному и тому же классу. Будем обозначать класс, в котором лежит (a, b) , символом $\frac{a}{b}$. В силу этого определения, $\frac{a}{b} = \frac{c}{d}$ тогда и только тогда, когда $(a, b) \sim (c, d)$, т. е. когда $ad = bc$.

В соответствии с формулами (1), мы определим теперь суммы и произведения новых символов $\frac{a}{b}$ формулами

$$(2) \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$(3) \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Определения эти законны. Действительно, во-первых, $bd \neq 0$, если $b \neq 0$ и $d \neq 0$, так что символы $\frac{ad + bc}{bd}$ и $\frac{ac}{bd}$ допустимы. Во-вторых,

¹⁾ Для некоммутативных колец без делителей нуля такая теорема не имеет места; см. А. И. Мальцев, *Math. Ann.* 113 (1936), 686 — 691.

правые части формул (2) и (3) не зависят от выбора представителей (a, b) и (c, d) классов $\frac{a}{b}$ и $\frac{c}{d}$; в самом деле, заменив в (2) a и b через a' и b' , где

$$ab' = ba',$$

будем иметь:

$$adb' = a'db,$$

$$adb' + bcb' = a'db + b'cb,$$

$$(ad + bc)b'd = (a'd + b'c)bd,$$

и, значит,

$$\frac{ad + bc}{bd} = \frac{a'd + b'c}{b'd};$$

точно так же,

$$cb' = ba',$$

$$acb'd = a'cbd,$$

и, значит,

$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

Аналогичный результат получим, заменяя (c, d) на (c', d') , где $cd' = dc'$.

Легко убедиться в том, что все свойства тела выполнены. Так, например, закон ассоциативности сложения получается следующим образом:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf};$$

$$\left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf};$$

аналогично проверяются и все остальные законы.

Построенное тело, очевидно, коммутативно. Для того чтобы оно содержало кольцо $\mathfrak{R}$, нужно отождествить некоторые дроби с элементами из $\mathfrak{R}$. Это достигается следующим образом.

Отнесём элементу c все дроби $\frac{cb}{b}$, где $b \neq 0$. Эти дроби совпадают друг с другом:

$$\frac{cb}{b} = \frac{cb'}{b'}, \text{ так как } (cb)b' = b(cb').$$

Таким образом, каждому элементу c будет отнесена одна дробь. Но различным элементам c, c' будут соответствовать и различные дроби. Действительно, из

$$\frac{cb}{b} = \frac{c'b'}{b'}$$

следует

$$cb'b' = bc'b',$$

или, так как на $b \neq 0$, $b' \neq 0$ можно сократить:

$$c = c'.$$

Таким образом, элементам кольца $\mathfrak{R}$ взаимно однозначно соответствуют некоторые определённые дроби.

Если элементы c_1, c_2, c_3 кольца $\mathfrak{R}$ связаны соотношением $c_1 + c_2 = c_3$ или $c_1 c_2 = c_3$, то отсюда для произвольных $b_1 \neq 0$, $b_2 \neq 0$ и $b_3 = b_1 b_2$ следует:

$$\frac{c_1 b_1}{b_1} + \frac{c_2 b_2}{b_2} = \frac{c_1 b_1 b_2 + c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3},$$

соответственно,

$$\frac{c_1 b_1}{b_1} \cdot \frac{c_2 b_2}{b_2} = \frac{c_1 c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3}.$$

Таким образом, дроби $\frac{c_i b_i}{b_i}$, соответствующие элементам c_i кольца $\mathfrak{R}$, складываются и перемножаются точно так же, как сами элементы c , и тем самым образуют область, изоморфную кольцу $\mathfrak{R}$. На этом основании мы можем заменить дроби $\frac{cb}{b}$ соответствующими элементами c (см. конец § 12). Этим и будет достигнуто вложение кольца $\mathfrak{R}$ в поле.

Итак, мы доказали существование объемлющего поля для каждой области целостности.

Построение отношений есть первое вспомогательное средство для образования из одного кольца новых колец (в частных случаях — полей). Этим способом порождается, например, из кольца $\mathcal{C}$ обыкновенных целых чисел поле Γ рациональных чисел.

Задача. Показать, что каждое коммутативное кольцо $\mathfrak{R}$ (безразлично — с делителями нуля или без) может быть вложено в некоторое «кольцо отношений», состоящее из всех дробей $\frac{a}{b}$, где b пробегает все не делители нуля. Вообще, предоставляя b возможность пробегать любое множество $\mathfrak{M}$ не делителей нуля, содержащее вместе с каждым двумя элементами b_1, b_2 также их произведение $b_1 b_2$, мы получим некоторое кольцо отношений $\mathfrak{R}_{\mathfrak{M}}$.

§ 14. Векторные пространства и алгебры.

Пусть $\mathfrak{R}$ — кольцо с единицей; элементы его будем обозначать греческими буквами $\alpha, \beta, \dots$. Пусть, далее, $\mathfrak{G}$ — аддитивная абелева группа; её элементы будем обозначать латинскими буквами $u, v, \dots$

Модуль $\mathfrak{G}$ называется *n-членным модулем линейных форм* или *n-мерным векторным пространством* относительно $\mathfrak{R}$, если в $\mathfrak{G}$,

кроме сложения, определено также умножение на элементы из $\mathfrak{R}$, обладающее следующими свойствами:

1) Произведение αu элемента u из $\mathfrak{G}$ на элемент α из $\mathfrak{R}$ всегда принадлежит к $\mathfrak{G}$.

$$2) \alpha(u + v) = \alpha u + \alpha v.$$

$$3) (\alpha + \beta)u = \alpha u + \beta u.$$

$$4) (\alpha\beta)u = \alpha(\beta u).$$

5) Все элементы из $\mathfrak{G}$ однозначно представимы в виде линейных форм $\alpha_1 u_1 + \dots + \alpha_n u_n$ относительно n фиксированных «базисных элементов» $u_1, \dots, u_n$.

Из 2) и 4) следует:

$$(1) \quad \beta(\alpha_1 u_1 + \dots + \alpha_n u_n) = (\beta \alpha_1) u_1 + \dots + (\beta \alpha_n) u_n.$$

Полагая, в частности, $\beta = 1$ и $\alpha_1 u_1 + \dots + \alpha_n u_n = u$, получаем:

$$(2) \quad 1 \cdot u = u.$$

Далее, из 3) следует:

$$(3) \quad \begin{cases} (\alpha_1 u_1 + \dots + \alpha_n u_n) + (\beta_1 u_1 + \dots + \beta_n u_n) = \\ = (\alpha_1 + \beta_1) u_1 + \dots + (\alpha_n + \beta_n) u_n. \end{cases}$$

Каждый элемент $u = \alpha_1 u_1 + \dots + \alpha_n u_n$ векторного пространства однозначно представляется системой $(\alpha_1, \dots, \alpha_n)$ из n элементов кольца $\mathfrak{R}$, называемых *компонентами* элемента u (относительно базиса $u_1, \dots, u_n$). Обратно, всякая такая система служит системой компонент для некоторого u из $\mathfrak{G}$. Число n базисных элементов или компонент называется *размерностью* векторного пространства. Сложение двух элементов из $\mathfrak{G}$ выполняется, согласно (3), путём сложения их компонент; умножение на β выполняется, согласно (1), путём умножения всех компонент на β .

Таким образом, *векторное пространство с точностью до изоморфизма однозначно определяется заданием кольца $\mathfrak{R}$ и размерности n .*

На основании этой теоремы можно, при заданном кольце $\mathfrak{R}$, взять любое векторное пространство данной размерности в качестве модели всех таких пространств. Проще всего понимать под вектором упорядоченную систему из n элементов $\alpha_1, \dots, \alpha_n$ кольца $\mathfrak{R}$. Сумма двух векторов $(\alpha_1, \dots, \alpha_n)$ и $(\beta_1, \dots, \beta_n)$ будет тогда определяться как $(\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$, а произведение $\beta(\alpha_1, \dots, \alpha_n)$ — как $(\beta \alpha_1, \dots, \beta \alpha_n)$. Правила действий 1) — 4) будут при этом автоматически выполняться. Если, далее, положить

$$(1, 0, \dots, 0) = u_1,$$

$$(0, 1, \dots, 0) = u_2,$$

$$\dots\dots\dots$$

$$(0, 0, \dots, 1) = u_n,$$

то будем иметь:

$$(\alpha_1, \dots, \alpha_n) = (\alpha_1, 0, \dots, 0) + (0, \alpha_2, \dots, 0) + \dots \\ \dots + (0, 0, \dots, \alpha_n) = \alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_n u_n,$$

т. е. будет выполнено и требование 5). Таким образом, векторы $(\alpha_1, \dots, \alpha_n)$ действительно образуют n -мерное векторное пространство в смысле нашего определения.

Векторное пространство $\mathfrak{G}$ будет кольцом, если определено ещё умножение элементов $u, v, \dots$ друг на друга. От этого умножения мы потребуем, кроме закона ассоциативности и обоих законов дистрибутивности, выполнения ещё следующего свойства:

$$(4) \quad (\alpha u) v = u (\alpha v) = \alpha (uv) \quad \text{для всех } \alpha \in \mathfrak{R}.$$

Если все эти свойства выполнены, то кольцо $\mathfrak{G}$ называют *гиперкомплексной системой* или *алгеброй* ранга n над кольцом $\mathfrak{R}$. При этом $\mathfrak{R}$ большей частью предполагается полем, в чём, однако, нет безусловной необходимости. Как можно эффективно задать алгебру — мы вскоре увидим.

Из (4) следует прежде всего:

$$(\alpha u) (\beta v) = (\alpha \beta) (uv)$$

и далее

$$(5) \quad \left(\sum_j \alpha_j u_j \right) \left(\sum_k \beta_k u_k \right) = \sum_j \sum_k \alpha_j \beta_k (u_j u_k).$$

Поэтому мы сможем вычислить все произведения uv , как только будут известны все произведения $u_j u_k$. При этом последние, конечно, должны быть снова линейными комбинациями базисных элементов $u_1, \dots, u_n$:

$$(6) \quad u_j u_k = \sum_i \gamma_{jk}^i u_i.$$

n^2 констант γ_{jk}^i , вполне определяющих, в силу (5) и (6), умножение в рассматриваемой алгебре, называются *структурными константами* этой алгебры.

Если заданы кольцо $\mathfrak{R}$, векторное пространство $\mathfrak{G}$ над $\mathfrak{R}$ и система структурных констант γ_{jk}^i , то умножение, определённое формулами (5) и (6), во всяком случае дистрибутивно относительно сложения. Если $\mathfrak{R}$ коммутативно, то выполнено также свойство (4). Лишь закон ассоциативности умножения не выполняется автоматически. Для произвольных сумм

$$u = \sum_j \alpha_j u_j, \quad v = \sum_k \beta_k u_k, \quad w = \sum_i \gamma_i u_i$$

он имеет место тогда и только тогда, если он выполняется для произведений $u_j u_k u_i$ базисных элементов, т. е. если

$$(7) \quad u_j (u_k u_i) = (u_j u_k) u_i.$$

Формула (7) является дополнительным условием, налагаемым на структурные константы γ_{jk}^i . Если это условие выполнено, то формулы (1), (3), (5), (6) полностью определяют операции в алгебре над кольцом $\mathfrak{A}$.

Если $\mathfrak{A}$ коммутативно и умножение базисных элементов u_j также коммутативно: $u_j u_k = u_k u_j$, то $\mathfrak{G}$ есть коммутативное кольцо. Если $\mathfrak{G}$ содержит единицу e , то кратные ae образуют в $\mathfrak{G}$ кольцо, изоморфное кольцу $\mathfrak{A}$; их можно поэтому отождествлять с элементами α из $\mathfrak{A}$.

Если алгебра $\mathfrak{G}$ — тело, то $\mathfrak{G}$ называется также *алгеброй с делением*.

Пример 1. *Определение обыкновенных комплексных чисел.*

Возьмём в качестве $\mathfrak{A}$ поле вещественных чисел и, обозначая через e и i базисные элементы двумерного векторного пространства $\mathfrak{G}$, положим в основу следующую таблицу умножения:

$$e \cdot e = e, \quad e \cdot i = i,$$

$$i \cdot e = i, \quad i \cdot i = -e.$$

Умножение базисных элементов ассоциативно и коммутативно; поэтому $\mathfrak{G}$ будет коммутативным кольцом с единицей e . Кратные ae можно отождествить с вещественными числами α . Поэтому вместо $ae + bi$ мы будем писать $\alpha + bi$. Так как $(a - bi)(a + bi) = a^2 + b^2 > 0$ (за исключением случая $a = b = 0$), то каждый отличный от нуля элемент $\alpha + bi$ имеет обратный, а именно $(a^2 + b^2)^{-1}(\alpha - bi)$. Таким образом, кольцо $\mathfrak{G}$ есть поле — поле комплексных чисел.

К аналогичному результату мы придём, взяв в качестве $\mathfrak{A}$ поле рациональных чисел. Получающаяся таким способом система $\mathfrak{G}$ называется *гауссовским числовым полем*. Если в качестве $\mathfrak{A}$ взять кольцо целых рациональных чисел, то $\mathfrak{G}$ будет *кольцом целых гауссовских чисел* $\alpha + bi$.

Пример 2. *Система кватернионов.*

Пусть снова $\mathfrak{A}$ — поле вещественных или рациональных чисел, а $\mathfrak{G}$ — четырёхмерное векторное пространство с базисными элементами e, j, k, l . Умножение, определяемое правилами

$$ee = e, \quad jj = kk = ll = -e,$$

$$ej = je = j, \quad ek = ke = k, \quad el = le = l,$$

$$jk = l, \quad kj = -l,$$

$$kl = j, \quad lk = -j,$$

$$lj = k, \quad jl = -k,$$

ассоциативно, но не коммутативно. Мы получаем таким образом некоммутативное кольцо с единицей e . Кратные ae будем отождествлять с числами a . Элементы

$$a + bj + ck + dl$$

называются *кватернионами*. Так как

$$(a - bj - ck - dl)(a + bj + ck + dl) = a^2 + b^2 + c^2 + d^2,$$

то каждый отличный от нуля кватернион $a + bj + ck + dl$ имеет обратный, равный

$$(a^2 + b^2 + c^2 + d^2)^{-1}(a - bj - ck - dl).$$

Таким образом, система кватернионов есть тело — *тело кватернионов*.

Пример 3. Групповое кольцо конечной группы.

Если мы возьмём в качестве базисных элементов векторного пространства $\mathfrak{R}_g$ элементы конечной группы g и определим умножение базисных элементов в соответствии с их умножением в группе g , то закон ассоциативности (7) будет выполняться автоматически. Получающаяся таким способом алгебра $\mathfrak{R}_g$ называется *групповым кольцом группы g над $\mathfrak{R}$* .

Задача 1. Если определить матрицу n -го порядка как систему n^2 элементов α_{jk} кольца $\mathfrak{R}$ ($j = 1, \dots, n$; $k = 1, \dots, n$), а сумму (σ_{jk}) и произведение (π_{jk}) двух матриц (α_{jk}) , (β_{jk}) — обычным способом формулами

$$\sigma_{jk} = \alpha_{jk} + \beta_{jk},$$

$$\pi_{jl} = \sum_{k=1}^n \alpha_{jk} \beta_{kl},$$

то матрицы n -го порядка будут составлять алгебру ранга n^2 над $\mathfrak{R}$.

Задача 2. Комплексные матрицы второго порядка

$$\begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}$$

образуют алгебру, изоморфную телу кватернионов. (Доказательство этого факта даёт попутно простейшее доказательство ассоциативности умножения кватернионов.)

Само собой напрашивается обобщение алгебр на системы бесконечного ранга. Рассматриваем бесконечное множество базисных элементов $u_1, u_2, \dots$, для которых определено умножение, удовлетворяющее условиям (6) и (7). Элементами же обобщённой алгебры

Считаем только конечные суммы $\sum a_{ji}$. Все результаты этого параграфа переносятся и на такие «алгебры с бесконечным базисом».

Простейшим примером такой алгебры может служить кольцо полиномов $\mathfrak{R}[x]$, которое будет определено в следующем параграфе.

§ 15. Кольца полиномов.

Пусть $\mathfrak{R}$ — кольцо с единицей и g — бесконечная циклическая группа, образованная степенями некоторого элемента x . Выделим из группы g элементы x^v с $v \geq 0$. Произведение двух таких элементов в силу равенства

$$x^p \cdot x^v = x^{p+v}$$

есть снова элемент того же рода. Эти элементы $x^0, x^1, x^2, \dots$ будут теперь служить базисными элементами алгебры с бесконечным базисом.

Элементами этой алгебры являются все конечные суммы

$$\sum a_v x^v.$$

Они называются *полиномами от x над $\mathfrak{R}$* . Их совокупность называется *областью полиномов $\mathfrak{R}[x]$* . Образующий элемент x называется *неизвестной* этой области полиномов; a_v называются *коэффициентами* полинома.

Так как базисные элементы $u_k = x^{k-1}$ области полиномов удовлетворяют условиям (7) предыдущего параграфа, то область полиномов $\mathfrak{R}[x]$ есть кольцо. Сумма и произведение двух полиномов задаются формулами

$$(1) \quad \begin{cases} \sum a_v x^v + \sum b_v x^v = \sum (a_v + b_v) x^v, \\ (\sum a_\lambda x^\lambda)(\sum b_\mu x^\mu) = \sum c_v x^v, \end{cases}$$

где

$$(2) \quad c_v = \sum_{\lambda+\mu=v} a_\lambda b_\mu.$$

Степенью полинома, отличного от нуля, называется наибольшее число v , для которого $a_v \neq 0$. Это a_v называется *старшим коэффициентом* полинома.

Полиномы нулевой степени имеют вид $a_0 x^0$. Мы будем отождествлять их с элементами a_0 исходного кольца $\mathfrak{R}$, что допустимо, так как они складываются и перемножаются таким же точно способом и потому образуют систему, изоморфную исходному кольцу $\mathfrak{R}$ (см. конец § 12). Таким образом, кольцо полиномов $\mathfrak{R}[x]$ содержит $\mathfrak{R}$.

Переход от $\mathfrak{R}$ к $\mathfrak{R}[x]$ называют *присоединением* (притом *кольцевым присоединением*) *неизвестной x* . Если $\mathfrak{R}$ коммутативно, то $\mathfrak{R}[x]$ также коммутативно,

Если мы присоединим к кольцу $\mathfrak{R}$ последовательно неизвестные $x_1, \dots, x_n$, образуя таким образом $\mathfrak{R}[x_1][x_2]\dots[x_n]$, то получится кольцо полиномов $\mathfrak{R}[x_1, \dots, x_n]$, состоящее из всех сумм

$$\sum a_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Мы будем считать, что в таком полиноме можно всюду менять порядок следования множителей $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$. Таким образом, кольцо полиномов $\mathfrak{R}[x_1][x_2]\dots[x_n]$ будет отождествляться с кольцом полиномов, получающимся путём перестановки неизвестных, например, с $\mathfrak{R}[x_2][x_1]\dots[x_n]$. Это отождествление допустимо, так как перестановка неизвестных x_i не оказывает никакого влияния на определение суммы и произведения. $\mathfrak{R}[x_1, \dots, x_n]$ называют *кольцом полиномов от n неизвестных $x_1, \dots, x_n$* .

Если, в частности, $\mathfrak{R}$ есть кольцо целых чисел, то получаем так называемые *целочисленные полиномы*.

Замена неизвестного произвольными элементами кольца. Пусть $f(x) = \sum a_\nu x^\nu$ — полином над $\mathfrak{R}$ и α — элемент (из $\mathfrak{R}$ или из более широкого кольца), перестановочный со всеми элементами из $\mathfrak{R}$. Мы можем в выражении для $f(x)$ заменить всюду x на α ; в результате получим значение $f(\alpha) = \sum a_\nu \alpha^\nu$. Если $g(x)$ — другой полином и $g(\alpha)$ — его значение для $x = \alpha$, то сумма и произведение

$$f(x) + g(x) = s(x), \quad f(x)g(x) = p(x)$$

имеют при $x = \alpha$ значения

$$f(\alpha) + g(\alpha) = s(\alpha), \quad f(\alpha)g(\alpha) = p(\alpha).$$

Действительно, для суммы это очевидно, для произведения же вычисление проводится на основании формулы (2) следующим образом:

$$\begin{aligned} p(\alpha) &= \sum c_\nu \alpha^\nu = \sum_\nu \sum_{\lambda + \mu = \nu} a_\lambda b_\mu \alpha^\nu = \sum_\lambda \sum_\mu a_\lambda b_\mu \alpha^{\lambda + \mu} = \\ &= (\sum a_\lambda \alpha^\lambda) (\sum b_\mu \alpha^\mu) = f(\alpha)g(\alpha). \end{aligned}$$

Тем самым доказано, что все соотношения между полиномами $f(x)$, $g(x), \dots$, основывающиеся на сложении и умножении, остаются в силе при замене x любым элементом α , перестановочным со всеми элементами кольца $\mathfrak{R}$.

Соответствующая теорема верна и для полиномов от нескольких неизвестных. В частности, если $\mathfrak{R}$ коммутативно, то можно в полиномах $f(x_1, \dots, x_n)$ заменять неизвестные любыми элементами из $\mathfrak{R}$ (или из некоторого коммутативного расширения кольца $\mathfrak{R}$). Основываясь на этой возможности замены, полиномы называют также *целыми рациональными функциями от переменных $x_1, \dots, x_n$* .

Для целочисленных полиномов без постоянного члена имеется ещё дальнейшая возможность замены x величиной из любого кольца, независимо от того, содержит ли оно целые числа или нет.

Если $\mathfrak{R}$ есть область целостности, то $\mathfrak{R}[x]$ также есть область целостности.

Доказательство. Если $f(x) \neq 0$, $g(x) \neq 0$ и a_α — старший (отличный от нуля) коэффициент полинома $f(x)$, а b_β — старший коэффициент полинома $g(x)$, то $a_\alpha b_\beta \neq 0$ будет коэффициентом при $x^{\alpha+\beta}$ в $f(x)g(x)$; поэтому $f(x)g(x) \neq 0$. Таким образом, $\mathfrak{R}[x]$ не содержит делителей нуля.

Попутно мы получили также следующее:

Дополнение. Если $\mathfrak{R}$ — область целостности, то степень произведения $f(x)g(x)$ равна сумме степеней сомножителей $f(x)$ и $g(x)$.

Из доказанной теоремы методом полной индукции непосредственно следует:

Если $\mathfrak{R}$ есть область целостности, то также $\mathfrak{R}[x_1, \dots, x_n]$ есть область целостности.

Под степенью члена $a_{\alpha_1 \dots \alpha_r} x_1^{\alpha_1} \dots x_r^{\alpha_r}$ понимают сумму показателей $\sum \alpha_i$. Под степенью полинома, отличного от нуля, понимают наибольшую из степеней его членов, отличных от нуля. Полином называется *однородным*, или *формой*, если все его члены имеют одну и ту же степень. Произведения однородных полиномов суть снова однородные полиномы, и если $\mathfrak{R}$ — область целостности, то степень произведения равна сумме степеней сомножителей.

Неоднородные полиномы можно записывать (однозначным образом) в виде сумм однородных форм различных степеней. Если перемножить два таких полинома f , g , имеющих, соответственно, степени m , n , то произведение содержащихся в них однородных форм высших степеней будет, в случае, когда $\mathfrak{R}$ — область целостности, отличной от нуля формой степени $m+n$. Все остальные однородные формы, входящие в состав произведения fg , будут иметь низшие степени, поэтому степень произведения fg будет равна $m+n$. Тем самым сформулированное выше предложение о степени произведения («Дополнение») имеет место также для полиномов от любого числа неизвестных.

Алгоритм деления. Пусть $\mathfrak{R}$ — кольцо с единицей 1, далее,

$$g(x) = \sum c_\nu x^\nu$$

— полином со старшим коэффициентом $c_n = 1$ и

$$f(x) = \sum a_\nu x^\nu$$

— произвольный полином степени $m \geq n$. Старший коэффициент a_m можно обратить в нуль, вычитая из f некоторый полином, крат-

ный g , а именно — полином $a_m x^{m-ng}$. Если степень разности всё ещё будет $\geq n$, то, снова вычитая некоторый полином, кратный g , можно опять обратить старший коэффициент в нуль. Продолжая этот процесс, мы дойдём, наконец, до момента, когда степень остатка станет меньше n , и получим:

$$(3) \quad f - qg = r,$$

где r имеет степень, меньшую чем g , или равно нулю. Этот процесс называют *алгоритмом деления*.

Если, в частности, $\mathfrak{R}$ — поле и $g \neq 0$, то предположение $c_n = 1$ излишне, ибо, в случае необходимости, можно умножить g на c_n^{-1} и добиться таким образом, чтобы старший коэффициент стал равным единице.

Задача. Пусть $x, y, \dots$ — бесконечное множество символов. Можно и в этом случае рассматривать совокупность всех $\mathfrak{R}$ -полиномов от этих неизвестных, причём, однако, каждый отдельный полином должен содержать лишь конечное их число. Доказать, что и так определённая область есть одновременно с $\mathfrak{R}$ кольцо или, соответственно, область целостности.

§ 16. Идеалы. Факторкольца.

Пусть $\mathfrak{o}$ — кольцо. Для того, чтобы некоторое его подмножество тоже было кольцом (*подкольцом* кольца $\mathfrak{o}$), необходимо и достаточно, чтобы это подмножество

- 1) было подгруппой аддитивной группы кольца, иными словами, вместе с a и b содержало бы также $a - b$ ¹⁾ (*свойство модуля*), и
- 2) вместе с a и b содержало бы также ab .

Среди подколец особую роль, аналогичную роли нормальных делителей в теории групп, играют так называемые *идеалы*.

Непустое подмножество $\mathfrak{m}$ кольца $\mathfrak{o}$ называется *идеалом*, и притом *правым идеалом*, если

- 1) из $a \in \mathfrak{m}$ и $b \in \mathfrak{m}$ следует $a - b \in \mathfrak{m}$ (свойство модуля),
- 2) из $a \in \mathfrak{m}$ следует $ar \in \mathfrak{m}$ для всякого r из $\mathfrak{o}$; словами: модуль $\mathfrak{m}$ должен вместе с каждым a содержать также все его «правые кратные» $a \cdot r$.

Точно так же, модуль $\mathfrak{m}$ называется *левым идеалом*, если из $a \in \mathfrak{m}$ следует $ga \in \mathfrak{m}$ для произвольного r из $\mathfrak{o}$.

Наконец, $\mathfrak{m}$ называется *двусторонним идеалом*, если $\mathfrak{m}$ есть одновременно и левый, и правый идеал.

Для коммутативных колец все три понятия совпадают, и говорят просто об *идеалах*. На протяжении этого параграфа мы будем предполагать $\mathfrak{o}$ коммутативным кольцом. Идеалы мы будем всегда обозначать строчными готическими буквами.

¹⁾ Отсюда уже следует, что это множество содержит также нуль и все суммы $a + b$; см. § 7.

Примеры идеалов:

1. Нулевой идеал, состоящий из одного элемента 0.
2. Единичный идеал $\mathfrak{o}$, содержащий все элементы кольца.
3. Идеал (a) , порождённый одним элементом a , т. е. образованный всеми выражениями вида

$$ra + na \quad (r \in \mathfrak{o}, n — \text{целое число}).$$

В том, что это множество действительно является идеалом, — легко убедиться: разность двух выражений указанного вида имеет, очевидно, тот же вид, произвольное же кратное представимо в форме

$$s \cdot (ra + na) = (sr + ns) \cdot a,$$

т. е. имеет вид $r'a$ или $r'a + 0 \cdot a$.

Идеал (a) есть, очевидно, наименьший из идеалов, содержащих a . Действительно, каждый такой идеал должен, во всяком случае, содержать все кратные ra и все суммы $\pm \sum a = na$, а значит, и все суммы $ra + na$. Таким образом, идеал (a) можно также определить как пересечение всех идеалов, содержащих элемент a .

Если кольцо $\mathfrak{o}$ обладает единицей e , то вместо $ra + na$ можно также написать $ra + nea = (r + ne)a = r'a$. Таким образом, в этом случае идеал (a) состоит из всех обыкновенных кратных ra . Так, например, идеал (2) в кольце целых чисел состоит из чётных чисел.

Идеал (a) , порождённый одним элементом a , называется *главным идеалом*. Нулевой идеал (0) всегда есть главный идеал; если $\mathfrak{o}$ обладает единицей e , то единичный идеал $\mathfrak{o}$ также есть главный идеал, а именно, тогда $\mathfrak{o} = (e)$.

4. Точно так же можно определять идеал, порождённый несколькими элементами $a_1, \dots, a_n$, как совокупность всех сумм вида

$$\sum r_i a_i + \sum n_j a_j$$

(соответственно, — вида $\sum r_i a_i$, если $\mathfrak{o}$ обладает единицей), или так же как пересечение всех идеалов из $\mathfrak{o}$, содержащих элементы $a_1, \dots, a_n$. Мы будем обозначать этот идеал символом $(a_1, \dots, a_n)$ и говорить, что $a_1, \dots, a_n$ образуют *базис идеала*.

5. Аналогично можно определить идеал $(\mathfrak{M})$, порождённый бесконечным множеством $\mathfrak{M}$ элементов кольца $\mathfrak{o}$, а именно, как совокупность всех конечных сумм вида

$$\sum r_i a_i + \sum n_j a_j \quad (a_i, a_j \in \mathfrak{M}, r_i \in \mathfrak{o}, n_j — \text{целые числа}).$$

Классы вычетов. Идеал $\mathfrak{m}$ кольца $\mathfrak{o}$, будучи подгруппой аддитивной группы, определяет разбиение кольца $\mathfrak{o}$ на смежные классы или *классы вычетов* по $\mathfrak{m}$. Два элемента a, b называют *сравнимыми по $\mathfrak{m}$* или *сравнимыми по модулю $\mathfrak{m}$* , если они принадлежат одному и тому же классу, т. е. если $a - b \in \mathfrak{m}$. Пишут:

$$a \equiv b \pmod{\mathfrak{m}}$$

или, короче,

$$a \equiv b \ (m).$$

Вместо « a не сравнимо с b » пишут: $a \not\equiv b$.

Если, в частности, m есть главный идеал (m) , то вместо $a \equiv b \ (m)$ можно было бы также писать $a \equiv b \ ((m))$. Но в этом случае берегают пару скобок и пишут просто $a \equiv b \ (m)$.

Таким путём приходят, например, к обыкновенным сравнениям по целому числу («модулю»): $a \equiv b \ (n)$ (читают: a сравнимо с b по модулю n) означает, что $a - b$ принадлежит к (n) , т. е. является кратным числа n .

Действия над сравнениями. Сравнение $a \equiv b$ по идеалу m , очевидно, сохраняет силу, если к обеим частям прибавить один и тот же элемент c или обе части умножить на один и тот же элемент c . Отсюда, далее, следует: если $a \equiv a'$ и $b \equiv b'$, то

$$a + b \equiv a + b' \equiv a' + b',$$

$$ab \equiv ab' \equiv a'b';$$

таким образом, сравнения можно почленно складывать и перемножать.

Обе части сравнения можно также умножить на обыкновенное целое число n . Беря, в частности, $n = -1$, получаем, в комбинации с предшествующим, что сравнения можно почленно вычитать одно из другого.

Таким образом, со сравнениями можно оперировать совершенно так же, как и с равенствами. Нельзя только, вообще говоря, производить сокращение на общий множитель; так, например, в области целых чисел

$$15 \equiv 3 \ (6)$$

и, однако, хотя $3 \not\equiv 0 \ (6)$, нельзя заключить, что $5 \equiv 1 \ (6)$.

Задача 1. Показать, что в кольце целых чисел классы вычетов по идеалу (m) ($m > 0$) можно представить числами $0, 1, \dots, m-1$ и на этом основании обозначить их через $\mathfrak{R}_0, \mathfrak{R}_1, \dots, \mathfrak{R}_{m-1}$.

Задача 2. Какой идеал в кольце целых чисел порождается совокупностью чисел 10 и 13?

Задача 3. Что означает $a \equiv b \ (0)$?

$$a \equiv b \quad a = b$$

Задача 4. Совокупность всех кратных ga элемента a есть идеал ga . Уяснить себе на примере кольца чётных чисел, что этот идеал может не совпадать с главным идеалом (a) .

Задача 5. Определить для некоммутативного кольца правый, левый или, соответственно, двусторонний идеалы, порождённые произвольным множеством элементов кольца.

Задача 6. Какие операции над сравнениями допустимы в некоммутативных кольцах?

Идеалы связаны с понятием гомоморфизма колец таким же образом, как нормальные делители — с понятием гомоморфизма групп. Примем за отправной пункт понятие гомоморфизма.

Гомоморфизм $\varphi \sim \bar{\varphi}$ двух колец порождает разбиение кольца φ на классы: каждый класс $\mathfrak{K}_a$ образован всеми элементами a , имеющими один и тот же образ $\bar{a}$. Но это разбиение на классы можно теперь охарактеризовать точнее следующим образом:

Класс π кольца φ , соответствующий при гомоморфизме $\varphi \sim \bar{\varphi}$ нулю, есть идеал в φ , а остальные классы суть классы вычетов по этому идеалу.

Доказательство. Прежде всего, π есть модуль. Действительно, если a и b переходят при гомоморфизме оба в нуль, то в нуль переходит также $-b$, а значит, и $a - b$; таким образом, $a - b$ также принадлежит классу π .

π есть идеал; действительно, если a переходит в нуль, то ga переходит в $\bar{g} \cdot \bar{0} = \bar{0}$, каково бы ни было g , и, значит, ga тоже принадлежит к π . (В некоммутативном случае π есть даже двусторонний идеал.)

Элементы $a + c$ ($c \in \pi$) класса вычетов по π , представителем которого служит элемент a , переходят в $\bar{a} + \bar{0}$, т. е. в $\bar{a}$, и, таким образом, принадлежат все одному классу $\mathfrak{K}_a$. Обратно, если некоторый элемент b переходит в $\bar{a}$, то $b - a$ переходит в $\bar{a} - \bar{a} = \bar{0}$; таким образом, $b - a \in \pi$ и b лежит в том же классе вычетов, что и a . Тем самым всё доказано.

Итак, каждому гомоморфизму соответствует некоторый идеал.

Обратим теперь эту связь: будем исходить от произвольного идеала π кольца φ и зададимся вопросом: *существует ли гомоморфный образ $\bar{\varphi}$ кольца φ такой, что классы вычетов по идеалу π отображаются как раз в элементы кольца $\bar{\varphi}$?*

Для построения такого кольца мы будем поступать так же, как в § 10 гл. 2: мы примем за элементы конструируемого кольца сами классы вычетов по π , обозначим класс вычетов $a + \pi$ через $\bar{a}$ и попытаемся так определить сложение и умножение, чтобы соответствие $a \rightarrow \bar{a}$ было гомоморфизмом. Итак, мы должны попытаться определить для каждых двух классов вычетов $\bar{a}$, $\bar{b}$ класс-сумму $\bar{a} + \bar{b}$ и класс-произведение $\bar{a} \cdot \bar{b}$ таким образом, чтобы все суммы каждого элемента из $\bar{a}$ с каждым элементом из $\bar{b}$ лежали в классе-сумме, а все произведения — в классе-произведении.

Итак, пусть a — произвольный элемент из $\bar{a}$, b — из $\bar{b}$. Попробуем определить $\bar{a} + \bar{b}$ как класс, в котором лежит $a + b$, и $\bar{a} \cdot \bar{b}$ — как класс, в котором лежит $a \cdot b$. Если $a' \equiv a$ — любой

другой элемент из $\bar{a}$ и $b' \equiv b -$ из $\bar{b}$, то, по предыдущему ¹⁾,

$$a' + b' \equiv a + b,$$

$$a' \cdot b' \equiv a \cdot b;$$

поэтому $a' + b'$ лежит в том же классе вычетов, что и $a + b$, и точно так же $a' \cdot b'$ — в том же, что и $a \cdot b$. Таким образом, наше определение класса-суммы и класса-произведения не зависит от выбора элементов a, b в $\bar{a}, \bar{b}$. Но эти классы $\bar{a} + \bar{b}, \bar{a} \cdot \bar{b}$ действительно обладают требуемыми свойствами, так как каждая сумма $a' + b'$ лежит в классе-сумме $\bar{a} + \bar{b}$ и каждое произведение $a' \cdot b'$ — в классе-произведении $\bar{a} \cdot \bar{b}$.

Каждому элементу a соответствует класс вычетов $\bar{a}$, и это соответствие гомоморфно, так как сумме $a + b$ соответствует сумма $\bar{a} + \bar{b}$ и точно так же произведению ab — произведению $\bar{a}\bar{b}$. Таким образом, классы вычетов образуют кольцо (§ 12). Это кольцо мы будем называть *факторкольцом* $\mathfrak{o}/\mathfrak{m}$ кольца $\mathfrak{o}$ по идеалу $\mathfrak{m}$ или факторкольцом по модулю $\mathfrak{m}$. Посредством указанного соответствия кольцо $\mathfrak{o}$ гомоморфно отображается на $\mathfrak{o}/\mathfrak{m}$. Идеал $\mathfrak{m}$ играет при этом гомоморфизме такую же точно роль, как прежде π : действительно, он совпадает с множеством всех элементов, классом вычетов которых служит нулевой класс.

Мы видим здесь принципиальную важность идеалов: они дают возможность строить кольца, являющиеся гомоморфными образами данного. Элементы такого нового кольца суть классы вычетов по некоторому идеалу: каждому элементу a соответствует класс вычетов $\bar{a}$. Сложение или перемножение двух классов вычетов выполняется путём сложения или перемножения любых двух их представителей. Из $a \equiv b$ следует $\bar{a} = \bar{b}$; таким образом, при переходе к факторкольцу сравнения превращаются в равенства, и оперированию со сравнениями в $\mathfrak{o}$ соответствует оперирование с равенствами в $\mathfrak{o}/\mathfrak{m}$.

Построенными здесь специальными кольцами, являющимися гомоморфными образами кольца $\mathfrak{o}$, — факторкольцами $\mathfrak{o}/\mathfrak{m}$ — исчерпываются по существу все такие кольца. Действительно, если $\mathfrak{o}$ — произвольный гомоморфный образ кольца $\mathfrak{o}$, то, как мы видели, элементам кольца $\mathfrak{o}$ взаимно однозначно соответствуют классы вычетов по некоторому идеалу π в $\mathfrak{o}$. Классу вычетов $\mathfrak{K}_a$ отвечает элемент $\bar{a}$ в $\mathfrak{o}$. Суммой и произведением двух классов вычетов $\mathfrak{K}_a, \mathfrak{K}_b$ служат $\mathfrak{K}_{a+b}$ и $\mathfrak{K}_{ab}$; им соответствуют элементы

$$\overline{a+b} = \bar{a} + \bar{b}$$

и

$$\overline{ab} = \bar{a}\bar{b}.$$

¹⁾ Все сравнения подразумеваются по модулю $\mathfrak{m}$.

Таким образом, соответствие между классами вычетов и элементами из $\bar{v}$ является изоморфизмом. Тем самым доказана теорема о гомоморфизмах колец:

Каждый гомоморфный образ $\bar{v}$ кольца v изоморфен некоторому факторкольцу v/p . При этом p есть идеал, составленный из тех элементов, образом которых v служит нуль. И обратно, каждое факторкольцо v/p является гомоморфным образом кольца v .

Пример. В кольце целых чисел классы вычетов по положительному числу m можно (см. задачу 1) обозначить через $R_0, R_1, \dots, R_{m-1}$, где R_a состоит из тех чисел, которые при делении на m дают остаток a . Сложение и перемножение двух классов вычетов R_a, R_b выполняется путём сложения, соответственно перемножения их представителей a, b и приведения результата к его наименьшему неотрицательному вычету по m .

Задача 7. Факторкольцо v/m может обладать делителями нуля и в том случае, когда v их не имеет. Указать примеры для кольца целых чисел.

Задача 8. Гомоморфизм $v \sim \bar{v}$ тогда и только тогда является изоморфизмом, когда $p = (0)$.

Задача 9. В поле единственными идеалами являются нулевой и единичный. Доказать! Какой вывод можно сделать отсюда относительно возможных гомоморфных отображений поля?

Задача 10. Для некоммутативного кольца гомоморфное отображение связано всегда с двусторонним идеалом, и каждый двусторонний идеал действительно определяет факторкольцо.

Задача 11. Кольцо целых гауссовских чисел $a + bi$ (§ 14, пример 1) изоморфно факторкольцу по идеалу $(x^2 + 1)$ в области целочисленных полиномов от неизвестного x .

§ 17: Делимость. Простые идеалы.

Пусть b — идеал (или, более обще, — модуль) в кольце v . Принадлежность элемента a идеалу b можно записать с помощью сравнения $a \equiv 0 (b)$; в этом случае говорят, что a делится на идеал b . Если все элементы идеала (или модуля) a делятся на b , то говорят, что a делится на b ; но это означает только то, что a есть подмножество идеала b . Пишут:

$$a \equiv 0 (b).$$

b называют делителем идеала a , a — кратным идеала b . Таким образом: делить = содержать, кратное = подмножество. Если, кроме того, $a \neq b$, значит, $a \subset b$, то b называется собственным делителем идеала a и a — собственным кратным идеала b .

Для главных идеалов в коммутативных кольцах с единицей ($a \equiv 0 ((b))$) означает просто, что $a = gb$, и делимость в смысле теории идеалов сводится к обычной делимости элементов.

Начиная отсюда, мы снова будем предполагать все рассматриваемые кольца коммутативными.

Под простым идеалом в $\mathfrak{o}$ понимают идеал $\mathfrak{p}$, факторкольцо по которому является областью целостности, т. е. не содержит делителей нуля.

Таким образом, обозначая классы вычетов по $\mathfrak{p}$, как и прежде, черточками сверху, мы должны иметь:

$$\text{из } \overline{ab} = 0 \text{ и } \overline{a} \neq \overline{0} \text{ следует } \overline{b} = \overline{0}.$$

Или, что то же, для любых элементов a и b кольца $\mathfrak{o}$, из

$$\begin{aligned} ab &\equiv 0 \pmod{\mathfrak{p}}, \\ a &\not\equiv 0 \pmod{\mathfrak{p}} \end{aligned}$$

должно следовать

$$b \equiv 0 \pmod{\mathfrak{p}};$$

словами: произведение должно делиться на идеал $\mathfrak{p}$ только тогда, когда на этот идеал делится один из сомножителей.

Очевидно, единичный идеал — всегда простой, так как предположение $a \not\equiv 0 \pmod{\mathfrak{p}}$ вообще не может быть выполнено. Нулевой идеал является простым тогда и только тогда, когда кольцо $\mathfrak{o}$ само есть область целостности. Другими примерами простых идеалов могут служить, как мы дальше увидим, главные идеалы кольца S целых чисел, порождаемые простыми числами.

Идеал в $\mathfrak{o}$ называется свободным от делителей, если он не содержится ни в каком другом идеале в $\mathfrak{o}$ кроме самого $\mathfrak{o}$, иными словами, если он не обладает собственными делителями, отличными от единичного идеала $\mathfrak{o}$. [Например, упомянутые только что простые главные идеалы (p) в S свободны от делителей.]

Если $\mathfrak{p}$ — кольцо с единицей, то каждый свободный от делителей идеал $\mathfrak{p}$, не совпадающий с $\mathfrak{o}$, является простым, и факторкольцо по нему есть поле. Обратное, если $\mathfrak{o}/\mathfrak{p}$ есть поле, то $\mathfrak{p}$ свободен от делителей.

Доказательство. Будем решать в факторкольце $\mathfrak{o}/\mathfrak{p}$ уравнение $\overline{x}\overline{a} = \overline{b}$, где $\overline{a} \neq \overline{0}$. Пусть, таким образом, $a \not\equiv 0 \pmod{\mathfrak{p}}$ и b произвольно. $\mathfrak{p}$ и a порождают в совокупности идеал, являющийся делителем идеала $\mathfrak{p}$ и притом — даже собственным делителем (поскольку в нём содержится a). Таким образом, идеал, порождаемый идеалом $\mathfrak{p}$ и элементом a , должен совпадать со всем кольцом $\mathfrak{o}$. Поэтому каждый элемент b кольца $\mathfrak{o}$ может быть записан в виде

$$b = p + ra \quad (p \in \mathfrak{p}, r \in \mathfrak{o})$$

(ибо $\mathfrak{o}$ — кольцо с единицей). Отсюда, в силу гомоморфизма кольца $\mathfrak{o}$ факторкольцо $\mathfrak{o}/\mathfrak{p}$, следует, что

$$\overline{b} = \overline{ra},$$

чем уравнение $\overline{x}\overline{a} = \overline{b}$ и решено.

Так как b и a принадлежат оба к идеалу α , то к нему принадлежит и $b - qa = r$. А так как $r < a$, то должно быть $r = 0$, ибо a , по предположению, — наименьшее положительное число идеала α . Таким образом, мы получили, что $b = qa$, т. е. что все числа идеала α кратны числу a . Это означает, что $\alpha = (a)$, т. е. α — главный идеал.

Совершенно так же доказывается следующее предложение:

Если P — поле, то в области полиномов $P[x]$ каждый идеал — главный.

Действительно, мы снова можем принять, что $\alpha \neq (0)$. В качестве a выбираем теперь полином наименьшей степени, содержащийся в идеале α . Так как алгоритм деления существует также и в области полиномов, то каждый полином b из идеала α может быть представлен в виде

$$b = qa + r,$$

где степень r , в случае $r \neq 0$, меньше степени a , и т. д.

Область целостности с единицей, в которой каждый идеал — главный, называется кольцом главных идеалов. Как мы показали, кольцо C целых чисел, равно как и каждое кольцо полиномов $P[x]$ (где P — поле), есть кольцо главных идеалов¹⁾.

Далее, каждое поле тривиальным образом является кольцом главных идеалов. Действительно, если α есть ненулевой идеал поля P , то вместе с каждым $a \neq 0$ он содержит также $a^{-1}a = 1$; таким образом, $\alpha = (1)$ есть единственный идеал, отличный от нулевого. (Ср. § 16, задача 9.)

Применённый выше в двух случаях способ рассуждения может быть обобщён следующим образом. Пусть $\mathfrak{N}$ — область целостности, в которой каждому отличному от нуля элементу a отнесено неотрицательное целое число $g(a)$ так, что удовлетворяются следующие условия:

1. Если $a \neq 0$ и $b \neq 0$, то $g(ab) \geq g(a)$.
2. (Алгоритм деления.) Для каждых двух элементов кольца a и b , где $a \neq 0$, существует представление

$$b = qa + r,$$

в котором либо $r = 0$, либо $g(r) < g(a)$.

В случае $\mathfrak{N} = C$ числом $g(a)$ служит $|a|$, в случае $\mathfrak{N} = P[x]$ — степень полинома a . Область целостности, обладающая указанными свойствами, называется эвклидовым кольцом. То же рассуждение, что и применённое выше в случаях $\mathfrak{N} = C$ и $\mathfrak{N} = P[x]$, приводит теперь сразу к следующей теореме:

В эвклидовом кольце каждый идеал — главный, причём все элементы идеала суть кратные qa порождающего его элемента a .

¹⁾ Элементарное исследование условий, которым должна удовлетворять область целостности для того, чтобы в ней каждый идеал был главным, даёт Н. Hasse, *J. reine u. angew. Math.*, 159 (1928), 3—12.

Применяя эту теорему, в частности, к единичному идеалу, т. е. ко всему кольцу, получаем, что существует такой элемент a , что все элементы кольца являются его кратными qa . В частности, и сам элемент a должен быть представим в этом виде, т. е. должен существовать такой элемент e , что

$$a = ae.$$

Для $b = qa$ получаем тогда:

$$b = qa = qae, \text{ т. е. } b = be.$$

$q = ea$ *область деления, то же эквивалентно*

Тем самым мы доказали, что всякое эвклидово кольцо обладает единицей e , таким образом, является кольцом главных идеалов.

Два отличных от нуля элемента a, b эвклидова кольца (или, вообще, кольца главных идеалов) порождают идеал (a, b) , состоящий из всех выражений вида $ra + sb$. Как и всякий идеал такого кольца, он является главным идеалом, т. е. порождается некоторым элементом d . Таким образом, имеем:

$$\begin{aligned} (1) \quad & d = ra + sb, \\ (2) \quad & \begin{cases} a = gd, \\ b = hd. \end{cases} \end{aligned}$$

В силу (2), d есть общий делитель элементов a и b . В силу же (1), d есть также наибольший общий делитель, т. е. все общие делители элементов a и b суть также делители элемента d . Таким образом, в кольце главных идеалов каждые два элемента a, b обладают наибольшим общим делителем, притом представляемым в виде (1). В частности, это имеет место в кольце целых чисел и в кольце $\mathbb{P}[x]$.

Наибольший общий делитель элементов a, b обозначают обычно символом $d = (a, b)$. Правда, точнее было бы писать $(d) = (a, b)$, ибо элементами a и b однозначно определяется лишь идеал (d) , но не сам элемент d . Если $(a, b) = 1$, то a и b называются взаимно простыми.

Приведённое выше доказательство существования наибольшего общего делителя не даёт ещё никаких средств для его действительного вычисления. В эвклидовых кольцах такое средство предоставляется предложенным ещё Эвклидом ¹⁾ способом последовательного деления (алгоритмом Эвклида, по которому эвклидовы кольца и получили своё наименование).

Пусть даны два элемента кольца a_0, a_1 и пусть, скажем, $g(a_1) \leq g(a_0)$. Тогда полагаем, пользуясь алгоритмом деления,

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 & (g(a_2) < g(a_1)), \\ a_1 &= q_2 a_2 + a_3 & (g(a_3) < g(a_2)) \end{aligned}$$

¹⁾ Эвклид, Начала, книга 7, теоремы 1 и 2.

и продолжаем этот процесс до тех пор, пока не дойдём до деления с остатком нуль:

$$a_{s-1} = q_s a_s.$$

Тогда все элементы $a_0, a_1, a_2, \dots, a_s$ имеют вид $ra_0 + sa_1$. Каждый делитель элемента a_s (и, в частности, сам a_s) является, в силу последнего равенства, также делителем для a_{s-1} , а тогда также для a_{s-2} и так далее, наконец, — также для a_1 и a_0 . Следовательно, a_s есть наибольший общий делитель элементов a_0 и a_1 .

Предшествующие рассмотрения могут быть перекинуты также на некоммукативный случай, если потребовать существования и левого, и правого алгоритма деления:

$$b = qa + r_1 = aq_2 + r_2, \quad g(r_1) < g(a), \quad g(r_2) < g(a).$$

Тогда получается, что в каждом левом идеале имеется элемент a такой, что все элементы идеала являются его левыми кратными qa , и, точно так же, в каждом правом идеале — элемент a такой, что все элементы идеала являются его правыми кратными aq . Двусторонний идеал обладает образующим элементом, характеризующимся тем свойством, что все элементы идеала являются как левыми, так и правыми его кратными. Применяя это, в частности, к единичному идеалу, выводим существование некоторой левой единицы и некоторой правой единицы, а значит — просто единицы.

Наконец, таким же способом, как и выше, доказываем существование левого и правого наибольших общих делителей двух элементов a, b .

Важнейшим примером некоммутативного эвклидова кольца является кольцо полиномов $P[x]$ над некоммутативным телом P .

Задача 1. Соотношение $(a, b) = d$ не нарушается при расширении кольца $\mathfrak{o}$ до любого объемлющего кольца $\bar{\mathfrak{o}}$.

Задача 2. Элементы ε эвклидова кольца, обладающие в этом кольце обратным элементом ε^{-1} , характеризуются равенством $g(\varepsilon) = 1$.

Задача 3. Если числа r и s взаимно просты:

$$(r, s) = 1,$$

то каждый элемент a группы $\mathfrak{G}$, имеющий порядок $r \cdot s$, представим в виде произведения однозначно определённого элемента a^{rs} порядка s и однозначно определённого элемента a^{rs} порядка r .

Задача 4. Циклическая группа порядка n , порождаемая элементом a , порождается также каждой степенью a^r , где $(r, n) = 1$.

Дальнейший пример эвклидова кольца. Рассмотрим кольцо целых гауссовских чисел $a+bi$ (§ 14, пример 1).

Если определить «норму» числа $\alpha = a+bi$ равенством

$$N(\alpha) = (a+bi)(a-bi) = a^2 + b^2,$$

то из определения произведения

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

легко будет следовать равенство

$$(3) \quad N(\alpha\beta) = N(\alpha)N(\beta).$$

Норма $N(\alpha)$ есть обыкновенное целое число и (как сумма двух квадратов) обращается в нуль тогда и только тогда, когда само α равно нулю, в остальных же случаях положительна. Из (3) следует, что произведение $\alpha\beta$ обращается в нуль только тогда, когда обращается в нуль α или β . Таким образом, мы имеем дело с областью целостности.

Согласно § 13, для неё существует поле отношений. Если $\alpha = a + bi \neq 0$, то $\alpha^{-1} = \frac{a-bi}{N(\alpha)}$; таким образом, каждое число из поля отношений можно представить в виде $\frac{a}{n} + \frac{b}{n}i$, где a, b, n — целые числа. Эти «дробные

числа» образуют «поле гауссовских чисел» (§ 14, пример 1). Определение нормы и равенство (3) дословно сохраняются и для элементов этого поля.

Чтобы получить алгоритм деления для целых гауссовских чисел, попытаемся найти для заданных α и $\beta \neq 0$ число $\alpha - \lambda\beta$, имеющее меньшую норму, чем β . Для этой цели найдём сперва дробное число $\lambda' = a' + b'i$, удовлетворяющее уравнению $\alpha - \lambda'\beta = 0$, затем заменим a' и b' ближайшими к ним целыми числами a и b и положим $\lambda = a + bi$, $\lambda' - \lambda = \epsilon$. Тогда будем иметь:

$$\alpha - \lambda\beta = \alpha - \lambda'\beta + \epsilon\beta = \epsilon\beta,$$

$$N(\alpha - \lambda\beta) = N(\epsilon)N(\beta),$$

$$N(\epsilon) = N(\lambda' - \lambda) = (a' - a)^2 + (b' - b)^2 < \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1,$$

$$N(\alpha - \lambda\beta) < N(\beta).$$

Тем самым «алгоритм деления» найден, и установлено, что рассматриваемое кольцо — эвклидово.

Задача 5. Провести такое же исследование для кольца чисел $a + b\tau$, определённого как алгебра над кольцом целых чисел, с базисными элементами 1, τ и определяющим равенством

$$\tau^2 = -\rho - 1.$$

То же для колец, образованных числами $a + b\sqrt{2}$; $a + b\sqrt{-2}$. Почему изложенный метод теряет силу для кольца, образованного числами $a + b\sqrt{-3}$ или $a + b\sqrt{-5}$? Является ли идеал $(2, 1 + \sqrt{-3})$ в первом из названных сейчас колец главным?

Литература. По вопросу о существовании алгоритма Эвклида или его обобщения в произвольных кольцах главных идеалов см. H. Hasse, *J. reine u. angew. Math.*, 159 (1928), 3—12. В каких кольцах алгебраических чисел имеет место алгоритм Эвклида — исследовали O. Perron (*Math. Ann.*, 107 (1932), 489—495), A. Oppenheim (*Math. Ann.*, 109 (1933), 349—352), E. Berg (*Kgl. Fysiogr. Sällskapet's Lund Förhandl.*, 5. No 5), N. Hofreiter (*Mh. Math. Physik*, 42, 397), H. Behrbohm und L. Rédei (*J. reine u. angew. Math.*, 174 (1936), 192—205).

§ 19. Разложение на множители.

В этом параграфе мы будем рассматривать лишь области целостности с единицей. Прежде всего мы обсудим, что в этих областях целесообразно понимать под простыми или неразложимыми элементами. При этом мы будем рассматривать даже если это специально и не оговорено, лишь элементы кольца, отличные от нуля.

В кольце целых чисел обыкновенное простое число всегда можно разложить на множители, и притом даже двумя способами:

$$p = p \cdot 1 = (-p) \cdot (-1).$$

Но одним из этих множителей всегда является делитель единицы, т. е. такое число ε , что в кольце содержится и ε^{-1} ; $(+1$ и -1 суть делители единицы.)

Вообще, если задана область целостности с единицей, то под делителем единицы понимается такой элемент ε , который обладает в этой области обратным элементом ε^{-1} . Очевидно, тогда также ε^{-1} есть делитель единицы.

Каждый элемент a допускает разложение

$$a = a\varepsilon^{-1} \cdot \varepsilon,$$

где ε — любой делитель единицы. Эти разложения мы будем считать тривиальными.

Элемент $p \neq 0$, обладающий лишь тривиальными разложениями (так что из $p = ab$ следует, что a или b есть делитель единицы), называется неразложимым или простым элементом (для целых чисел — также простым числом¹⁾; для полиномов — неприводимым полиномом).

Два элемента, которые, как a и $b = a\varepsilon^{-1}$, отличаются лишь делителем единицы, называются иногда «ассоциированными элементами». Каждый из них служит делителем другого, а для соответствующих главных идеалов имеем:

$$(a) \subseteq (b), \quad (b) \subseteq (a), \quad \text{следовательно,} \quad (b) = (a).$$

Таким образом, два ассоциированных элемента порождают один и тот же главный идеал.

Обратно, если каждый из двух элементов a и b является делителем другого:

$$a = bc, \quad b = ad,$$

то получаем:

$$b = bcd, \quad \text{откуда} \quad 1 = cd, \quad c = d^{-1};$$

тем самым c и d суть делители единицы, и a ассоциировано с b .

Если c есть делитель элемента a , не ассоциированный с b , т. е. $a = cd$, где d — не делитель единицы, то c называется собственным делителем элемента a . В этом случае a не является уже делителем для c , и идеал (c) является собственным делителем идеала (a) . Действительно, если бы a было делителем для c , скажем, $c = ab$, то мы имели бы

$$a = cd = abd,$$

$$1 = bd,$$

т. е. d должно было бы быть делителем единицы.

¹⁾ Чаще всего под простыми числами понимают лишь положительные неразложимые числа $\neq 1$, т. е. числа 2, 3, 5, 7, 11,...

Мы можем теперь определить простой элемент также как отличный от нуля элемент, не имеющий собственных делителей, кроме делителей единицы.

Если в эвклидовом кольце элемент b есть собственный делитель элемента a , то $g(b) < g(a)$.

Доказательство. Деление b на a невыполнимо, так что

$$b = aq + r, \quad \text{где} \quad g(r) < g(a), \quad r \neq 0.$$

Полагая $a = bc$, получаем отсюда:

$$r = b - aq = b(1 - cq),$$

$$g(r) \geq g(b), \quad \text{т. е.} \quad g(b) \leq g(r) < g(a).$$

В эвклидовом кольце каждый отличный от нуля элемент a является произведением простых элементов:

$$a = p_1 p_2 \dots p_r.$$

Доказательство. Мы применим полную индукцию по $g(a)$. Пусть высказанное утверждение верно для всех элементов b с $g(b) < n$ и пусть $g(a) = n$. Если a — простой элемент: $a = p$, то нечего и доказывать. Если же a разложимо: $a = bc$, причём b и c суть собственные делители элемента a , то, по доказанному,

$$g(b) < g(a), \quad g(c) < g(a).$$

Тогда, по предположению индукции, b и c суть произведения простых элементов. А в таком случае и $a = bc$ есть произведение простых элементов.

Впрочем, аналогичная теорема имеет место также для любых колец главных идеалов. Её доказательство основано на следующих леммах:

I. Если в кольце главных идеалов дана последовательность элементов $a_1, a_2, \dots$, из которых каждый следующий является собственным делителем предыдущего, то эта последовательность содержит лишь конечное число членов.

Для случая эвклидовых колец эта лемма тривиальна ввиду доказанного выше утверждения, что в таких кольцах $g(b) < g(a)$, если только b есть собственный делитель для a . Её доказательство для любых колец главных идеалов проходит следующим образом.

Объединение всех идеалов (a_n) есть идеал. Действительно, если элемент a принадлежит к одному из идеалов (a_n) , то это же верно и для всех ga ; если, далее, элементы a и b принадлежат, соответственно, к идеалам (a_μ) и (a_ν) , то разность $a - b$ принадлежит к идеалу (a_λ) , где λ есть больший из индексов μ и ν , т. е. $a - b$ принадлежит к рассматриваемому объединению. Это объединение, являясь идеалом, обладает базисным элементом d , который, принадлежа к объединению, будет делиться, например, на a_n . Тогда a_n

будет последним элементом заданной последовательности. Действительно, если бы существовало a_{n+1} , то мы имели бы

$$a_{n+1} \equiv 0 \pmod{d}, \quad d \equiv 0 \pmod{a_n};$$

т. е. элемент a_{n+1} не был бы собственным делителем для a_n .

II. Если в некоторой области целостности элемент a , отличный от нуля, не представим как произведение простых множителей, то a обладает собственным делителем, который снова не представим как произведение простых множителей.

В самом деле, при наших предположениях элемент a не является простым, т. е. существует разложение

$$a = bc,$$

где b и c — собственные делители элемента a ; при этом хотя бы один из множителей b и c не будет представим в виде произведения простых множителей, так как иначе элемент a был бы произведением простых множителей. Этим лемма доказана.

Повторным применением леммы II получаем, что для всякого элемента, не разложимого на простые множители, существует бесконечная последовательность собственных делителей, каждый из которых есть собственный делитель предыдущего ¹⁾. Так как, однако, по лемме I, кольцо главных идеалов не может обладать такой последовательностью, то этим доказано, что в кольце главных идеалов всякий отличный от нуля элемент является произведением простых множителей.

Следующий пример показывает, что возможность разложения на простые множители, столь очевидная в кольце целых чисел, может уже не иметь места в произвольных областях целостности. Присоединим к области целых чисел величины $2^{\frac{1}{2}}, 2^{\frac{1}{4}}, 2^{\frac{1}{8}}, \dots$ и составим все конечные суммы

$$\sum a_r 2^r,$$

где всякое r имеет вид $\frac{m}{2^n}$. Эти суммы составляют область целостности, в которой

$$2 = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{2}} = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{4}} \cdot 2^{\frac{1}{4}} = \dots;$$

при разложении числа 2 нельзя дойти, следовательно, до конца, т. е. до разложения на простые множители.

Исследуем теперь, как обстоит дело с единственностью разложения элемента a на простые множители $a = p_1 p_2 \dots p_r$, причём будем рассматривать сразу любые кольца главных идеалов.

¹⁾ Детальный анализ этого рассуждения показывает, что здесь используется «аксиома выбора». См. Добавление;

I В кольце главных идеалов каждый неразложимый элемент, не являющийся делителем единицы, порождает свободный от делителей (простой) идеал (факторкольцо по которому есть, таким образом, поле).

Доказательство. Если p — неразложимый элемент, то он не имеет никаких собственных делителей, кроме делителей единицы, и, следовательно (так как каждый идеал — главный), идеал (p) имеет собственным делителем только единичный идеал.

Замечание. Разумеется, разрешимость уравнения $\bar{a}x = \bar{b}$ в факторкольце или сравнения $ax \equiv b \pmod{p}$ в заданном кольце можно вывести также непосредственно из того обстоятельства, что при $a \not\equiv 0 \pmod{p}$ необходимо должно быть $(a, p) = 1$, так что

$$1 = ar + ps,$$

$$b = arh + psb,$$

$$b \equiv arb \pmod{p}.$$

II Основываясь на этом замечании, можно также фактически вычислять в конкретных случаях решения указанных сравнений с помощью алгоритма Эвклида.

В качестве непосредственного следствия получаем:

III Если произведение делится на простой элемент p , то на p должен делиться по крайней мере один из множителей. Действительно, в факторкольце по (p) нет делителей нуля. *в кольце главных идеалов*

Задача 1. Решить сравнение

$$x = -3, -3 + 19, \dots, 6x \equiv 7 \pmod{19}.$$

Задача 2. Определить элемент, обратный к классу вычетов, содержащему число 6, в поле классов вычетов кольца целых чисел по модулю 19. *если $(qr) = k$, то $q = k r^{-1}$*

$$[6 + k \cdot 19] [-3 + h \cdot 19] = [1 + m \cdot 19]$$

Теперь мы в состоянии доказать теорему об однозначности разложения на простые множители в кольцах главных идеалов. *сравнение разрешимо*

Пусть

(1)

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

— два разложения одного и того же элемента a в кольце главных идеалов. Случай, когда a есть делитель единицы, а следовательно, и все p_i и q_j суть делители единицы, можно заранее исключить как тривиальный. Тогда мы можем принять, что p_1 и q_1 — не делители единицы и что все а priori возможные делители единицы среди множителей p_i и q_j включены уже в p_1 и q_1 , так что ни один из оставшихся множителей p_i и q_j не является уже делителем единицы. Мы утверждаем теперь: $r = s$ и p_i совпадают с q_j с точностью до порядка нумерации и до множителей — делителей единицы.

При $r = 1$ утверждение очевидно. Действительно, вследствие неразложимости элемента $a = p_1$ произведение $q_1 \dots q_s$ также может

содержать лишь один множитель $q_1 = p_1$. Мы можем, таким образом, проводить индукцию по r . Так как p_1 делит произведение $q_1 \dots q_r$, то p_1 должен делить один из множителей q_i . Перестановкой этих множителей можно достичь того, чтобы p_1 делил q_1 :

$$(2) \quad q_1 = \varepsilon_1 p_1.$$

Здесь ε_1 должно быть делителем единицы, так как иначе q_1 не был бы простым. Подставив (2) в (1) и сократив на p_1 , получим:

$$(3) \quad p_2 \dots p_r = (\varepsilon_1 q_2) q_3 \dots q_r.$$

Но, по предположению индукции, множители левой и правой частей равенства (3) должны с точностью до порядка следования и делителей единицы совпадать. Так как и p_1 совпадает с q_1 с точностью до делителя единицы ε_1 , то тем самым всё доказано.

Из доказанных теорем следует: элементы эвклидова кольца, как и любого кольца главных идеалов, представимы в виде произведений простых элементов, причём такое представление единственно с точностью до делителей единицы и порядка следования множителей. В частности, это имеет место для целых чисел, для полиномов от одного переменного с коэффициентами из поля и для целых гауссовских чисел.

Задача 3. Целочисленные полиномы $f(x)$ однозначно разложимы по модулю p на неразложимые по модулю p множители для любого простого p .

Задача 4. Найти делители единицы в кольце гауссовских чисел. Разложить в этом кольце числа 2, 3 и 5 на простые множители.

Задача 5. В кольце чисел $a + b\sqrt{-3}$ число 4 обладает двумя существенно различными разложениями на неразложимые множители

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Задача 6. В кольце главных идеалов классы вычетов по модулю a , состоящие из элементов, взаимно простых с a , образуют группу по умножению.

В следующей главе мы увидим, что существуют кольца, не являющиеся кольцами главных идеалов, но где, тем не менее, справедлива теорема об однозначности разложения на простые множители. Для всех таких колец мы докажем теперь следующую теорему:

Если в кольце R каждый элемент однозначно разлагается на простые множители, то каждый неразложимый элемент p порождает простой идеал, а каждый отличный от нуля неразложимый элемент — непростой идеал.

Доказательство. Пусть p — неразложимый элемент. Если теперь $ab \equiv 0 \pmod{p}$, то в разложение ab на простые множители должен входить множитель p . Но это разложение получается путём объединения разложений для a и b ; таким образом, p должен

входить множителем уже в a или b , т. е. должно быть $a \equiv 0 (p)$, либо $b \equiv 0 (p)$. *т. е. p — общий простой идеал.*

Пусть теперь p — разложимый элемент: $p = ab$, где a и b — собственные делители элемента p . Тогда имеем: $ab \equiv 0 (p)$, $a \not\equiv 0 (p)$, $b \not\equiv 0 (p)$, и, значит, идеал (p) — не простой.

Задача 7. Доказать для всех колец с однозначным разложением на простые множители, что для каждой конечной совокупности элементов существуют «наибольший общий делитель» и «наименьшее общее кратное», оба определённые однозначно с точностью до делителей единицы.

в смысле идеалов.

Замечание. Для колец рассматриваемого вида наибольший общий делитель в смысле элементов не всегда есть то же, что наибольший общий делитель в смысле идеалов. Так, например, в области целочисленных полиномов от одного неизвестного x элементы 2 и x не имеют общих делителей, кроме делителей единицы; однако идеал $(2, x)$ не есть единичный идеал. (То, что в этом кольце осуществляется однозначное разложение на простые множители, будет доказано в следующей главе.)

Задача 7. Из только что доказанного Г. следует, что если p — неразложимый, то он образует простой идеал, а тогда легко показать, такой же образ как и с 88/1. А потому можно доказать эту задачу для двух элементов, а потом применить индукцию.

К замечанию Наибольший общий делитель в смысле идеалов и наиб. об. делитель в смысле элементов один и тот же в кольце главных идеалов.

ГЛАВА ЧЕТВЁРТАЯ.

ЦЕЛЫЕ РАЦИОНАЛЬНЫЕ ФУНКЦИИ.

Содержание: элементарные теоремы о полиномах от одного и нескольких неизвестных, с коэффициентами из коммутативного кольца $\mathfrak{o}$ или поля Σ .

§ 20. Дифференцирование.

В этом параграфе будет дано определение производных от целых рациональных функций для произвольных областей полиномов $\mathfrak{o}[x]$, не опирающееся на понятие предельного перехода.

Пусть $f(x) = \sum a_i x^i$ — полином из $\mathfrak{o}[x]$. Образовав в области полиномов $\mathfrak{o}[x, h]$ полином $f(x+h) = \sum a_i (x+h)^i$ и развёртывая его по степеням h , получим:

$$f(x+h) = f(x) + hf_1(x) + h^2 f_2(x) + \dots$$

или

$$f(x+h) \equiv f(x) + h \cdot f_1(x) \pmod{h^2}.$$

Коэффициент $f_1(x)$ при первой степени h (определяемый однозначным образом) называется *производной* полинома $f(x)$ и обозначается через $f'(x)$. Очевидно, $f'(x)$ можно получить также, образовав разность $f(x+h) - f(x)$, разделив её на содержащийся в ней множитель h и положив затем в полученном полиноме $h=0$. Отсюда легко следует, что в случае, когда $\mathfrak{o}$ есть, например, поле вещественных чисел, данное нами определение производной согласуется с её обычным определением как $\lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$. Поэтому мы будем

обозначать производную также символами $\frac{df}{dx}$, или $\frac{d}{dx} f(x)$, или же, если f , кроме x , содержит ещё другие переменные, — символом $\frac{\partial f}{\partial x}$.

Имеют место следующие «правила дифференцирования»:

- (1) $(f+g)' = f' + g'$ (производная суммы),
- (2) $(fg)' = f'g + fg'$ (производная произведения).

Доказательство формулы (1):

$$f(x+h) + g(x+h) \equiv f(x) + hf'(x) + g(x) + hg'(x) \pmod{h^2}.$$

Доказательство формулы (2):

$$\begin{aligned} f(x+h)g(x+h) &\equiv \{f(x) + hf'(x)\} \{g(x) + hg'(x)\} \equiv \\ &\equiv f(x)g(x) + h[f'(x)g(x) + f(x)g'(x)] \pmod{h^2}. \end{aligned}$$

Таким же образом доказывается, что, вообще,

$$(3) \quad (f_1 + \dots + f_n)' = f_1' + \dots + f_n',$$

$$(4) \quad (f_1 f_2 \dots f_n)' = f_1' f_2 \dots f_n + f_1 f_2' \dots f_n + \dots + f_1 f_2 \dots f_n'.$$

Из (4) следует далее:

$$(5) \quad (ax^n)' = nax^{n-1}.$$

Из (3) и (5) получаем:

$$\left(\sum_0^n a_k x^k \right)' = \sum_0^n k a_k x^{k-1}.$$

Последнюю формулу можно было бы принять также за формальное определение производной.

Задача 1. Пусть $F(z_1, \dots, z_m)$ — полином и $F_v = \frac{\partial F}{\partial z_v}$. Доказать формулу

$$\frac{d}{dx} F(f_1(x), \dots, f_m(x)) = \sum_1^m F_v(f_1, \dots, f_m) \frac{df_v}{dx}.$$

Задача 2. Вывести для однородных полиномов r -й степени $f(x_1, \dots, x_n)$ из равенства

$$f(hx_1, \dots, hx_n) = h^r f(x_1, \dots, x_n)$$

тождество Эйлера

$$\sum_v \frac{\partial f}{\partial x_v} x_v = rf.$$

Задача 3. Дать алгебраическое определение производной дробно-рациональной функции $\frac{f(x)}{g(x)}$ с коэффициентами из некоторого поля и доказать известные правила дифференцирования сумм, произведений и частных.

§ 21. Корни.

Пусть $\mathfrak{o}$ — область целостности с единицей.

Элемент α области $\mathfrak{o}$ называется *корнем* полинома $f(x)$ из $\mathfrak{o}[x]$, если $f(\alpha) = 0$. Имеет место следующая теорема:

Если α — корень полинома $f(x)$, то $f(x)$ делится на $x - \alpha$.

существование единицы в кольце нужно
для определения $1 \cdot x - \alpha$

Доказательство. Деление $f(x)$ на $x - \alpha$ даёт:

$$f(x) = q(x) \cdot (x - \alpha) + r, \quad \left(\begin{array}{l} \text{Деление даёт} \\ \text{остаток } r \text{ для ка-} \\ \text{ждого } x \end{array} \right)$$

где r — константа. Полагая $x = \alpha$, получаем:

$$0 = r,$$

и тем самым

$$f(x) = q(x) \cdot (x - \alpha),$$

что и требовалось доказать.

Если $\alpha_1, \dots, \alpha_k$ — различные корни полинома $f(x)$, то $f(x)$ делится на произведение $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)$.

Доказательство. Для случая $k=1$ теорема была только что доказана. Если она уже доказана для $k-1$, то имеем:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_{k-1}) g(x).$$

Подстановка $x = \alpha_k$ даёт:

$$0 = (\alpha_k - \alpha_1) \dots (\alpha_k - \alpha_{k-1}) g(\alpha_k), \quad \left(\begin{array}{l} \text{Здесь } g(\alpha_k) = 0, \\ \text{так как } \alpha_k \text{ — корень } f(x) \end{array} \right)$$

и так как g не содержит делителей нуля, и $\alpha_k \neq \alpha_1, \dots, \alpha_k \neq \alpha_{k-1}$, то отсюда следует, что

$$g(\alpha_k) = 0.$$

Тем самым, в силу предыдущей теоремы,

$$g(x) = (x - \alpha_k) \cdot h(x),$$

и

$$f(x) = (x - \alpha_1) \dots (x - \alpha_{k-1}) (x - \alpha_k) h(x),$$

что и требовалось доказать.

Следствие. Отличный от нуля полином n -й степени имеет в области целостности, самое большее, n корней.

Эта теорема справедлива также в областях целостности без единицы, так как такую область всегда можно вложить в поле (с единицей). Однако, подобная теорема уже не имеет места в кольцах с делителями нуля; так, например, над факторкольцом кольца целых чисел по модулю 16 полином x^2 имеет корни 0, 4, 8, 12, а существуют кольца, в которых тот же полином имеет даже бесконечное множество корней (§ 11, задача 3). Точно так же рассматриваемая теорема неверна и для некоммутативных колец, ибо, например, в теле кватернионов (§ 14, пример 2) полином $x^2 + 1$ имеет корни $\pm i$, $\pm j$, $\pm k$ (и, кроме того, бесконечное множество других).

Если $f(x)$ делится на $(x - \alpha)^k$, но не делится уже на $(x - \alpha)^{k+1}$, то α называют k -кратным корнем полинома $f(x)$. Имеет место следующая теорема:

k -кратный корень полинома $f(x)$ есть по меньшей мере $(k-1)$ -кратный корень производной $f'(x)$.

значения для $n+1$ значений неизвестного, равны; действительно, их разность есть полином степени, не превосходящей n , имеющий $n+1$ корней. Таким образом, существует самое большее один полином степени $\leq n$, принимающий для $n+1$ различных значений неизвестного $\alpha_0, \dots, \alpha_n$ заданные значения $f(\alpha_i)$. Но один такой полином всегда существует, а именно, этим полиномом является

$$(1) \quad f(x) = \sum_{i=0}^n \frac{f(\alpha_i)(x-\alpha_0)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)}{(\alpha_i-\alpha_0)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)}.$$

Итак, существует один и только один полином степени $\leq n$, принимающий при $n+1$ различных значениях неизвестного $\alpha_0, \dots, \alpha_n$ заданные значения $f(\alpha_0), \dots, f(\alpha_n)$, а именно — полином, представленный формулой (1). Формула (1) называется *интерполяционной формулой Лагранжа*; название «интерполяционная» объясняется тем, что эта формула позволяет вычислять значения целой рациональной функции степени n для всех значений аргумента, коль скоро мы знаем её значения для $n+1$ значений аргумента.

Полином с требуемыми свойствами выражается также *интерполяционной формулой Ньютона*

$$(2) \quad \begin{cases} f(x) = \lambda_0 + \lambda_1(x-\alpha_0) + \lambda_2(x-\alpha_0)(x-\alpha_1) + \dots \\ \dots + \lambda_n(x-\alpha_0)(x-\alpha_1)\dots(x-\alpha_{n-1}), \end{cases}$$

где коэффициенты $\lambda_0, \dots, \lambda_n$ последовательно определяются путём подстановки значений $x = \alpha_0, \dots, x = \alpha_n$. Ясно, что мы получим таким способом для каждого λ_i линейное уравнение, в котором коэффициент при этом λ_i имеет значение

$$(\alpha_i - \alpha_0)(\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1}) \neq 0,$$

из остальных же λ в уравнение входят лишь имеющие меньшие индексы.

Вычисление проводится проще всего следующим образом. Полагая сперва в (2) $x = \alpha_0$, получаем:

$$f(\alpha_0) = \lambda_0.$$

Вычитая это из (2) и деля на $x - \alpha_0$, находим:

$$(3) \quad \frac{f(x) - f(\alpha_0)}{x - \alpha_0} = \lambda_1 + \lambda_2(x - \alpha_1) + \dots + \lambda_n(x - \alpha_1)\dots(x - \alpha_{n-1}).$$

Введём для левой части обозначение $f(\alpha_0, x)$. Положив в (3) $x = \alpha_1$, получим:

$$f(\alpha_0, \alpha_1) = \lambda_1.$$

Вычтя это из (3) и разделив результат на $x - \alpha_1$, будем иметь:

$$\frac{f(\alpha_0, x) - f(\alpha_0, \alpha_1)}{x - \alpha_1} = \lambda_2 + \lambda_3(x - \alpha_2) + \dots + \lambda_n(x - \alpha_2)\dots(x - \alpha_{n-1}).$$

Введём для левой части обозначение $f(\alpha_0, \alpha_1, x)$. Положив теперь $x = \alpha_2$, получим:

$$f(\alpha_0, \alpha_1, \alpha_2) = \lambda_2.$$

Этот процесс можно продолжать. Полагая вообще (определение путём полной индукции!)

$$(4) \quad f(\alpha_0, \dots, \alpha_k, x) = \frac{f(\alpha_0, \dots, \alpha_{k-1}, x) - f(\alpha_0, \dots, \alpha_{k-1}, \alpha_k)}{x - \alpha_k},$$

найдем, как выше:

$$f(\alpha_0, \dots, \alpha_{k-1}, x) = \lambda_k + \lambda_{k+1}(x - \alpha_k) + \dots + \lambda_n(x - \alpha_k) \dots (x - \alpha_{n-1}),$$

и

$$(5) \quad f(\alpha_0, \dots, \alpha_k) = \lambda_k.$$

$f(\alpha_0, \dots, \alpha_k)$ называют k -м разностным отношением функции $f(x)$ для значений $\alpha_0, \dots, \alpha_k$ аргумента. Согласно формуле (4), имеем

$$(6) \quad \left\{ \begin{array}{l} f(\alpha_0, \alpha_1) = \frac{f(\alpha_1) - f(\alpha_0)}{\alpha_1 - \alpha_0}, \\ f(\alpha_0, \alpha_1, \alpha_2) = \frac{f(\alpha_0, \alpha_2) - f(\alpha_0, \alpha_1)}{\alpha_2 - \alpha_1}, \\ \dots \dots \dots \\ f(\alpha_0, \dots, \alpha_n) = \frac{f(\alpha_0, \dots, \alpha_{n-2}, \alpha_n) - f(\alpha_0, \dots, \alpha_{n-2}, \alpha_{n-1})}{\alpha_n - \alpha_{n-1}}. \end{array} \right.$$

k -е разностное отношение можно также определить как коэффициент при x^k в том полиноме $\varphi_k(x)$ степени $\leq k$, который при значениях $\alpha_0, \dots, \alpha_k$ аргумента x принимает значения $f(\alpha_0), \dots, f(\alpha_k)$. Действительно, этот полином даётся, согласно интерполяционной формуле Ньютона, равенством

$$\varphi_k(x) = \lambda_0 + \lambda_1(x - \alpha_0) + \dots + \lambda_k(x - \alpha_0) \dots (x - \alpha_{k-1}),$$

где коэффициент при x^k есть как раз $\lambda_k = f(\alpha_0, \dots, \alpha_k)$.

Последнее определение k -го разностного отношения показывает, что это отношение не зависит от порядка следования (т. е. способа нумерации) значений $\alpha_0, \dots, \alpha_k$. Это свойство применяется при практическом вычислении разностных отношений, когда $\alpha_0, \dots, \alpha_n$ суть, скажем, рациональные числа, расположенные в порядке возрастания; а именно, разностные отношения в этом случае образуют последовательно для возрастающих значений α , и вместо (6) применяю формулы

$$(7) \quad f(\alpha_0, \alpha_1, \dots, \alpha_k) = \frac{f(\alpha_1, \dots, \alpha_k) - f(\alpha_0, \dots, \alpha_{k-1})}{\alpha_k - \alpha_0},$$

$$f(\alpha_0, \alpha_1, \dots, \alpha_k) = f(\alpha_1, \dots, \alpha_{k-1}, \alpha_0, \alpha_k) = \frac{f(\alpha_1, \dots, \alpha_{k-1}, \alpha_k) - f(\alpha_1, \dots, \alpha_{k-1}, \alpha_0)}{\alpha_k - \alpha_0}$$

получающиеся из (6) путём перестановки значений α . Тогда можно расположить разностные отношения в следующей схеме:

$$\begin{array}{ccccccc}
 f(\alpha_0) & & & & & & \\
 & f(\alpha_0, \alpha_1) & & & & & \\
 & & f(\alpha_0, \alpha_1, \alpha_2) & & & & \\
 & & & f(\alpha_1, \alpha_2) & & \dots & \\
 & & & & f(\alpha_1, \alpha_2, \alpha_3) & & \\
 & & & & & \dots & \\
 & & & & & & f(\alpha_2, \alpha_3) & \dots & \dots & \\
 & & & & & & & \dots & \dots & \\
 & & & & & & & & \dots &
 \end{array}$$

Каждый следующий столбец образуется согласно формуле (7) путём составления первых разностных отношений для членов предыдущего столбца. Эту схему можно неограниченно продолжать, прибавляя всё новые значения α . Если $f(x)$ — полином n -й степени, то в n -м столбце будет всюду стоять одна и та же постоянная, а именно, коэффициент λ_n при x^n . В $(n+1)$ -м столбце будут в этом случае стоять одни нули.

Арифметические прогрессии высших порядков. Будем теперь предполагать, что наше основное поле содержит в себе поле рациональных чисел и что в качестве значений $\alpha_0, \alpha_1, \alpha_2, \dots$ выбраны последовательные целые числа, скажем, $0, 1, 2, \dots$. Если тогда выписать предложенную выше схему разностных отношений, то разности $\alpha_k - \alpha_0, \alpha_{k+1} - \alpha_1, \dots$, служащие согласно (7) знаменателями разностных отношений, стоящих в $(k+1)$ -м столбце, будут все равны k . Умножая теперь второй столбец на 1, третий — на 2, четвёртый — на $2 \cdot 3$, вообще, $(k+1)$ -й — на $k!$, мы получим вместо схемы разностных отношений *схему разностей*

$$(8) \quad \left\{ \begin{array}{cccc}
 a_0 & & & \\
 & \Delta a_0 & & \\
 a_1 & & \Delta^2 a_0 & \\
 & \Delta a_1 & & \dots \\
 a_2 & & \Delta^2 a_1 & \\
 & \Delta a_2 & & \\
 a_3 & & \dots & \\
 \dots & & &
 \end{array} \right.$$

где положено $f(\alpha_v) = a_v$; Δa_v означает $a_{v+1} - a_v$; $\Delta^2 a_v$ означает $\Delta \Delta a_v = \Delta a_{v+1} - \Delta a_v = a_{v+2} - 2a_{v+1} + a_v$, и т. д. Если $a_0, a_1, \dots$ — значения полинома n -й степени, то, по предыдущему, n -е разности постоянны, а $(n+1)$ -е разности равны нулю. Сам же полином даётся формулой (2) с

$$(9) \quad \lambda_k = \frac{\Delta^k a_0}{k!}.$$

Оказывается, что верно также обратное утверждение.

Если $(n+1)$ -е разности последовательности $a_0, a_1, a_2, \dots$ равны нулю, то $a_0, a_1, \dots$ суть значения полинома n -й степени $f(x)$, определяемого формулами (2) и (9).

Действительно, образуем для указанного полинома $f(x)$ схему разностей и сравним её со схемой (8). Начальные элементы $a_0, \Delta a_0, \Delta^2 a_0, \dots, \Delta^n a_0$ всех столбцов будут во всяком случае совпадать, $(n+1)$ -й же столбец в обоих случаях будет состоять из одних нулей. Но отсюда будет последовательно вытекать совпадение элементов n -х столбцов, $(n-1)$ -х столбцов, $\dots$, наконец, первых столбцов обеих схем.

Проведённое сейчас рассуждение показывает одновременно, каким образом можно, отправляясь от последнего столбца, вычислить все элементы схемы (8), если заданы начальные элементы столбцов $\Delta^k a_0 = k! \lambda_k$ ($k = 0, 1, \dots, n$). Это вычисление можно проиллюстрировать следующим примером ($n=3$, $a_0=0$, $\Delta a_0=1$, $\Delta^2 a_0=6$, $\Delta^3 a_0=6$):

$$\begin{array}{ccccccc}
 f & & & & & & \\
 0 & 1 & 6 & 6 & 0 & \lambda_0 = 0 \\
 1 & & 7 & 6 & & \lambda_1 = 1 \\
 8 & 12 & & & & \\
 27 & 19 & 6 & 0 & \lambda_2 = \frac{6}{2} = 3 \\
 64 & 37 & 6 & & \lambda_3 = \frac{6}{6} = 1 \\
 & 61 & & & \\
 & 125 & & &
 \end{array}$$

$$\begin{aligned}
 f(x) &= \lambda_0 + \lambda_1 x + \lambda_2 x(x-1) + \lambda_3 x(x-1)(x-2) = \\
 &= x + 3x(x-1) + x(x-1)(x-2) = x^3.
 \end{aligned}$$

Арифметической прогрессией нулевого порядка называют последовательность одинаковых чисел $s, s, s, \dots$, а арифметической прогрессией n -го порядка — последовательность, разности членов которой образуют арифметическую прогрессию $(n-1)$ -го порядка. Очевидно, первый столбец схемы (8) представляет собой арифметическую прогрессию n -го порядка, если $(n+2)$ -й столбец состоит из одних нулей. Мы можем поэтому сформулировать полученные результаты следующим образом:

Значения каждого полинома n -й степени $f(x)$ при $x=0, 1, 2, 3, \dots$ образуют арифметическую прогрессию n -го порядка, и, наоборот, каждая арифметическая прогрессия n -го порядка состоит из значений полинома степени $\leq n$ при указанных значениях аргумента, а именно, полинома, определяемого формулами (2) и (9). Тем самым общий член a_x арифметической прогрессии

n -го порядка задаётся формулой

$$a_x = f(x) = a_0 + (\Delta a_0)x + \frac{\Delta^2 a_0}{2}x(x-1) + \dots + \frac{\Delta^n a_0}{n!}x(x-1)\dots(x-n+1).$$

Разностная схема (8) находит практическое применение при интерполировании и интегрировании таблично заданных (например, эмпирических) функций. Если $a_0, a_1, a_2, \dots$ — значения функции $\varphi(x)$ для равноотстоящих значений аргумента $\alpha_0, \alpha_0 + h, \alpha_0 + 2h, \dots$, то, как показывает практика, при достаточно закономерном течении функции и не слишком большой длине интервала h вторые, третьи, четвёртые или, в крайнем случае, пятые разности значений a_k практически равны нулю и, таким образом, функция ведёт себя на протяжении нескольких последовательных интервалов почти точно как полином не выше четвёртой степени. Поэтому для целей численного интерполирования или интегрирования можно заменить функцию полиномом, принимающим для нескольких (от двух до пяти) последовательных значений аргумента значения из заданной таблицы. Интерполяция производится по формуле (2); при этом почти всегда ограничиваются первыми и вторыми разностями, т. е. обходятся линейными или квадратными полиномами. При переходе от разностей $\Delta^k a$, к разностным отношениям, в знаменателях наряду с факториалами $k!$ появляются ещё степени длины интервала h , так что место формулы (9) занимает формула

$$\lambda_k = \frac{\Delta^k a_0}{k! h^k}.$$

Если же значения аргумента $\alpha_0, \alpha_1, \dots$ не являются равноотстоящими, то вместо разностей $\Delta^k a$, с самого начала образуются разностные отношения (7). По поводу дальнейших подробностей вычислительного характера, а также оценки погрешности интерполяции и т. п. отсылаем читателя к специальной учебной литературе¹⁾.

Задача 1. Частные суммы $s_m = \sum_{v=0}^{m-1} a_v$, арифметической прогрессии n -го порядка (при дополнительном условии $s_0 = 0$) образуют арифметическую прогрессию $(n+1)$ -го порядка. Вывести отсюда формулу

$$s_m = m a_0 + \binom{m}{2} \Delta a_0 + \dots + \binom{m}{n+1} \Delta^n a_0.$$

Задача 2. Вывести формулы для сумм $\sum_{v=0}^{m-1} v$, $\sum_{v=0}^{m-1} v^2$, $\sum_{v=0}^{m-1} v^3$.

¹⁾ См., напр., В. Л. Гончаров, Теория интерполирования и приближения функций, ГИИТ, 1934 г.; менее подробное изложение в книге: Р. Куррант, Курс дифференциального и интегрального исчисления, часть I, Дополнения к шестой главе.

§ 23. Разложение на множители.

Мы уже видели в § 19, что в области полиномов $K[x]$, где K — поле, справедлива теорема об однозначном разложении на простые множители. Мы докажем теперь следующую, более общую, основную теорему:

Если $\mathfrak{S}$ — область целостности с единицей и если в $\mathfrak{S}$ имеет место теорема об однозначном разложении на простые множители, то эта теорема справедлива и в области полиномов $\mathfrak{S}[x]$.

Излагаемое ниже доказательство восходит к Гауссу.

Пусть $f(x) = \sum_{i=0}^n a_i x^i$ — полином из $\mathfrak{S}[x]$, отличный от нуля.

Наибольший общий делитель d коэффициентов $a_0, \dots, a_n$ в $\mathfrak{S}$ (см. § 19, задача 7) мы будем называть содержанием полинома $f(x)$. Вынеся d за скобки, получим:

$$f(x) = d \cdot g(x),$$

где $g(x)$ имеет содержание 1. $g(x)$ и d определены однозначно с точностью до делителей единицы. Полиномы с содержанием 1 называются примитивными полиномами (относительно $\mathfrak{S}$).

Лемма 1. *Произведение двух примитивных полиномов есть снова примитивный полином.*

Доказательство. Пусть

$$f(x) = a_0 + a_1 x + \dots$$

и

$$g(x) = b_0 + b_1 x + \dots$$

— примитивные полиномы, и предположим, что, в противоречие с утверждением леммы, коэффициенты их произведения $f(x) \cdot g(x)$ имеют общий делитель d , не являющийся делителем единицы. Пусть p — простой множитель элемента d ; p должен тогда входить множителем во все коэффициенты произведения $f(x)g(x)$. Пусть a_r — первый не делящийся на p коэффициент полинома $f(x)$ (такой коэффициент обязательно существует, ибо иначе $f(x)$ не был бы примитивным полиномом), и, соответственно, b_s — первый не делящийся на p коэффициент полинома $g(x)$.

Коэффициент при x^{r+s} в произведении $f(x)g(x)$ равен сумме

$$a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \dots + a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \dots$$

Эта сумма должна делиться на p . Но все её члены, кроме первого, делятся на p . Следовательно, и $a_r b_s$ делится на p , откуда либо a_r , либо b_s должно делиться на p , что, однако, противоречит предположению. Тем самым лемма доказана.

Пусть теперь Σ — поле отношений области целостности $\mathfrak{S}$ (§ 13). Каждый полином в $\Sigma[x]$ однозначно разложим (§ 19). Для перехода от разложения в $\Sigma[x]$ к разложению в $\mathfrak{S}[x]$ мы воспользуемся теперь тем обстоятельством, что каждый полином $\varphi(x)$ из $\Sigma[x]$ можно записать в виде $\frac{F(x)}{b}$, где $F(x)$ — полином из $\mathfrak{S}[x]$, b — элемент из $\mathfrak{S}$, беря в качестве b , например, произведение знаменателей всех коэффициентов полинома $\varphi(x)$; в свою очередь, числитель $F(x)$ можно записать в виде произведения его содержания на примитивный полином:

$$F(x) = a \cdot f(x);$$

таким образом,

$$(1) \quad \varphi(x) = \frac{a}{b} \cdot f(x).$$

Мы утверждаем теперь:

Лемма 2. *1) Примитивный полином $f(x)$, входящий в формулу (1), определяется полиномом $\varphi(x)$ однозначно с точностью до делителей единицы из $\mathfrak{S}$. И обратно, $\varphi(x)$ определяется по формуле (1) примитивным полиномом $f(x)$ однозначно с точностью до делителей единицы из $\Sigma[x]$. 2) При этом произведению двух полиномов $\varphi(x), \psi(x)$ из $\Sigma[x]$ отвечает с точностью до делителей единицы произведение соответствующих примитивных полиномов (и обратно). 3) Если $\varphi(x)$ неразложим в $\Sigma[x]$, то $f(x)$ неразложим в $\mathfrak{S}[x]$ (и обратно).*

Доказательство. Пусть даны два различных представления одного и того же полинома $\varphi(x)$ из $\Sigma[x]$:

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x).$$

Тогда

$$(2) \quad adf(x) = cbg(x).$$

Содержанием левой части служит ad , содержанием правой части — cb ; поэтому должно иметь место равенство

$$ad = \varepsilon cb,$$

где ε — делитель единицы из $\mathfrak{S}$. Подставляя это в (2) и сокращая на $c\hat{b}$, получаем:

$$\varepsilon f(x) = g(x).$$

Таким образом, $f(x)$ и $g(x)$ отличаются друг от друга лишь делителем единицы из $\mathfrak{S}$.

Составляя произведение двух полиномов

$$\varphi(x) = \frac{a}{b} f(x), \quad \psi(x) = \frac{c}{d} g(x),$$

получаем:

$$\varphi(x)\psi(x) = \frac{ac}{bd}f(x)g(x),$$

и в силу леммы 1, $f(x)g(x)$ есть снова примитивный полином. Таким образом, произведению $\varphi(x)\psi(x)$ соответствует произведение $f(x)g(x)$.

Наконец, если $\varphi(x)$ неразложим, то неразложим также соответствующий ему примитивный полином $f(x)$; ибо из разложения $f(x) = g(x)h(x)$ тотчас же вытекало бы разложение

$$\varphi(x) = \frac{a}{b}f(x) = \frac{a}{b}g(x) \cdot h(x).$$

Так же доказывается и обратное утверждение.

Тем самым лемма 2 доказана.

В силу этой леммы однозначная разложимость полиномов $\varphi(x)$ на простые множители непосредственно переносится на соответствующие примитивные полиномы. Таким образом, примитивные полиномы разлагаются на простые множители, также являющиеся примитивными полиномами, однозначно, с точностью до делителей единицы.

Обратимся теперь к разложению произвольных полиномов в $\mathbb{S}[x]$. Неразложимые полиномы необходимо должны быть либо неразложимыми константами, либо неразложимыми примитивными полиномами.

Таким образом, для разложения какого-либо полинома $f(x)$ нужно сперва расщепить его на содержание и примитивный полином и затем разлагать на простые множители каждую из этих составных частей отдельно. Разложение первой из них возможно с точностью до делителей единицы однозначным образом согласно предположению основной теоремы, а разложение второй — по доказанному. Тем самым основная теорема доказана.

Попутно мы получили следующий важный результат:

Если полином $F(x)$ из $\mathbb{S}[x]$ разложим в $\Sigma[x]$, то он разложим уже в $\mathbb{S}[x]$.

Действительно, $F(x) = df(x)$, где $f(x)$ — примитивный полином, и в силу леммы 2 разложимость $F(x)$ в $\Sigma[x]$ влечёт за собой разложимость $f(x)$ в $\mathbb{S}[x]$; но вместе с $f(x)$ разложим также $F(x)$. 663

Так, например, каждый полином с целыми рациональными коэффициентами, разложимый на множители с рациональными коэффициентами, разложим уже на множители с целыми коэффициентами.

Следовательно, если целочисленный полином неразложим в области полиномов с целыми коэффициентами, то он неразложим и в области полиномов с рациональными коэффициентами.

Из основной теоремы методом полной индукции получается дальнейший результат:

Если $\mathbb{S}$ — область целостности с единицей и в $\mathbb{S}$ имеет место теорема об однозначном разложении на простые множители, то эта теорема справедлива также в области $\mathbb{S}[x_1, \dots, x_n]$.

Отсюда следует, в частности, однозначная разложимость целочисленных полиномов (от любого числа переменных), полиномов с коэффициентами из поля и т. д.

Понятие «примитивного полинома», введенное выше в леммах Гаусса, имеет особенно важное применение в областях полиномов от нескольких переменных. Пусть K — поле. Полином f из $K[x_1, \dots, x_n]$ называется *примитивным относительно $x_1, \dots, x_{n-1}$* , если он не имеет делителей, не являющихся константами и зависящих только от $x_1, \dots, x_{n-1}$. Так, например, полином, «регулярный относительно x_n », т. е. у которого коэффициент при старшей степени x_n является константой (не зависит от $x_1, \dots, x_{n-1}$), примитивен относительно $x_1, \dots, x_{n-1}$.

Задача 1. Делителями единицы в $\mathbb{S}[x]$ являются лишь делители единицы $\mathbb{S}$.

Задача 2. Доказать, что в разложение однородного полинома могут входить лишь однородные множители.

Задача 3. Доказать, что определитель

$$\Delta = \begin{vmatrix} x_{11} \dots x_{1n} \\ \dots \dots \dots \\ x_{n1} \dots x_{nn} \end{vmatrix}$$

неразложим в области полиномов $\mathbb{S}[x_{11}, \dots, x_{nn}]$. (Выделить одно неизвестное, скажем x_{11} , и показать, что Δ примитивен относительно остальных неизвестных.)

Задача 4. Указать способ, который позволял бы для каждого целочисленного полинома решать, имеет ли он множитель первой степени или нет.

Задача 5. Доказать неразложимость полинома

$$x^4 - x^2 + 1 \quad Z = \frac{\pm \sqrt{1-4}}{2} \text{ Кошани}$$

в области целочисленных полиномов от неизвестного x . Разложим ли этот полином, если областью коэффициентов служит поле рациональных чисел? кольцо гауссовских чисел?

В рач. поле не раз
а в кольце гаусс. раз

§ 24. Признаки неприводимости.

Пусть $\mathbb{S}$ — область целостности с единицей и пусть в $\mathbb{S}$ имеет место однозначная разложимость на простые множители. Следующая теорема позволяет во многих случаях установить неприводимость полинома

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

из $\mathbb{S}[x]$.

Теорема Эйзенштейна. Если в $\mathfrak{O}$ существует такой простой элемент p , что

$$a_n \not\equiv 0 \pmod{p},$$

$$a_i \equiv 0 \pmod{p} \text{ для всех } i < n,$$

$$a_0 \not\equiv 0 \pmod{p^2},$$

то $f(x)$, с точностью до постоянного множителя, неприводим в $\mathfrak{O}[x]$; иными словами, $f(x)$ неприводим в $\Sigma[x]$, где Σ означает поле отношений области $\mathfrak{O}$.

Доказательство. Пусть, в противоречие с утверждением теоремы, полином $f(x)$ разложим:

$$f(x) = g(x) \cdot h(x),$$

$$g(x) = \sum_{v=0}^r b_v x^v,$$

$$h(x) = \sum_{v=0}^s c_v x^v,$$

$$r > 0, s > 0, r + s = n.$$

$$a_0 = b_0 c_0.$$

Но $a_0 \equiv 0 \pmod{p}$. Следовательно, либо $b_0 \equiv 0 \pmod{p}$, либо $c_0 \equiv 0 \pmod{p}$. Пусть, скажем, $b_0 \equiv 0 \pmod{p}$. Тогда $c_0 \not\equiv 0 \pmod{p}$, ибо иначе мы имели бы $a_0 = b_0 c_0 \equiv 0 \pmod{p^2}$.

На p не могут делиться все коэффициенты полинома $g(x)$. Действительно, в противном случае на p делились бы все коэффициенты и произведения $f(x) = g(x) \cdot h(x)$, в частности, должен был бы делиться на p и коэффициент a_n , что, однако, противоречит предположению. Пусть b_i — первый коэффициент полинома $g(x)$, не делящийся на p ($0 < i \leq r < n$). Имеем

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i,$$

$$a_i \equiv 0 \pmod{p},$$

$$b_{i-1} \equiv 0 \pmod{p},$$

$$\dots \dots \dots$$

$$b_0 \equiv 0 \pmod{p},$$

$$b_i c_0 \equiv 0 \pmod{p},$$

$$c_0 \not\equiv 0 \pmod{p},$$

$$b_i \equiv 0 \pmod{p},$$

следовательно,

и так как

то, значит,

что, однако, противоречит предположению.

Полученное противоречие показывает, что $f(x)$, с точностью до постоянных множителей, неприводим.

Признак Эйзенштейна отнюдь не всегда решает вопрос о неприводимости полинома: существует много полиномов, как, например, полином $x^2 + 1$ над кольцом целых чисел, не подходящих под этот признак, но, тем не менее, неприводимых. Однако, в благоприятных случаях из него получаются весьма общие результаты.

Пример 1. Полином $x^m - p$ (p — простое) неприводим в области полиномов с целыми (а значит, и вообще с рациональными) коэффициентами.

Следовательно, корень $\sqrt[m]{p}$ ($m > 1$, p — простое) всегда иррационален.

Здесь
мы
используем
предположение
теоремы

Пример 2. Полином $f(x) = x^{p-1} + x^{p-2} + \dots + 1$ при p — простом представляет собой левую часть «уравнения деления круга». Докажем, что он также неприводим в области полиномов с целыми (а значит, и вообще с рациональными) коэффициентами. Признак Эйзенштейна здесь непосредственно неприменим. Но вопрос можно свести к нему следующим образом. Если бы $f(x)$ был приводим, то и $f(x+1)$ был бы приводим. Но

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x}{x} = \\ = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}.$$

Здесь все коэффициенты, кроме коэффициента при x^{p-1} , делятся на p , ибо в формуле

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!},$$

где $i < p$, числитель делится на p , а знаменатель не делится. Кроме того, постоянный член $\binom{p}{p-1} = p$ не делится на p^2 . Таким образом, согласно признаку Эйзенштейна, $f(x+1)$ неприводим, а следовательно, неприводим и $f(x)$.

Пример 3. То же преобразование решает вопрос и для $f(x) = x^2 + 1$, так как

$$f(x+1) = x^2 + 2x + 2.$$

Задача 1. Доказать иррациональность корня $\sqrt[m]{p_1 p_2 \dots p_r}$, где $p_1, p_2, \dots, p_r$ — различные простые числа и $m > 1$.

Задача 2. Доказать неприводимость полинома

$$x^2 + y^2 - 1$$

в области $P[x, y]$, где P — любое поле, в котором $-1 \neq -1$.

Задача 3. Доказать неприводимость полиномов

$$x^4 + 1, \quad x^6 + x^3 + 1$$

в области целочисленных полиномов.

Теорема Эйзенштейна основывается, в сущности, на переходе от равенства

$$f(x) = g(x) \cdot h(x)$$

к сравнению

$$f(x) \equiv g(x) \cdot h(x)$$

по модулю p^2 и приведении этого последнего сравнения к абсурду. Оказывается, что и в очень многих других случаях возможно получить доказательство неприводимости путём перехода от равенств к сравнениям по какому-нибудь модулю q из области $\mathfrak{S}$ и исследования разложимости рассматриваемого полинома $f(x)$ по этому модулю. Если, в частности, $\mathfrak{S}$ — кольцо целых чисел S , то над областью классов вычетов по q имеется лишь конечное число полиномов заданной степени, и потому всегда подлжит исследованию лишь конечное число возможностей распада полинома $f(x)$ по модулю q . Если при этом окажется, что $f(x)$ неприводим по модулю q , то это будет означать, что $f(x)$ неприводим и в $S[x]$; но даже и в противном случае можно при некоторых обстоятельствах основать доказательство неприводимости на свойствах найденного разложения по модулю q , причём в случае, когда q — простое число, можно опираться

на теорему об однозначной разложимости полиномов на простые множители по модулю q (§ 19, задача 3).

Пример 1. $\mathfrak{S} = \mathbb{C}$; $f(x) = x^5 - x^2 + 1$. Если $f(x)$ разложим, то один из множителей должен быть линейным или квадратным. Но существует лишь два линейных полинома по модулю 2, а именно

$$x \text{ и } x+1,$$

и лишь один неприводимый квадратный полином по модулю 2, а именно

$$x^2 + x + 1.$$

Выполняя деление, убеждаемся, что $x^5 - x^2 + 1$ ни на один из этих полиномов не делится по модулю 2. Это же видно и непосредственно из сравнения

$$x^5 - x^2 + 1 = x^3(x^2 - 1) + 1 \equiv x^2(x+1)(x^2+x+1) + 1.$$

Следовательно, $f(x)$ неприводим.

Пример 2. $\mathfrak{S} = \mathbb{C}$; $f(x) = x^4 + 3x^3 + 3x^2 - 5$. По модулю 2 полином $f(x)$ разложим:

$$f(x) \equiv (x+1)(x^3+x+1);$$

при этом второй множитель неприводим по модулю 2. Если поэтому $f(x)$ вообще разложим, то он должен распадаться на линейный и кубический множители. Но легко непосредственно показать, что $f(x)$ не может содержать линейного множителя: проще всего — проверив, что единственно возможные по модулю 3 линейные множители x , $x+1$, $x-1$ не входят в $f(x)$.

Существенное обобщение эйзенштейновского признака неприводимости предложил Дюма (G. Dumas). Пусть снова p — простой элемент из $\mathfrak{S}$. Каждому отличному от нуля члену $ax^\lambda = cpr^\mu x^\lambda$, $(c, p) = 1$, полинома $f(x)$ соответствует пара показателей (λ, μ) , и мы можем рассматривать эти пары чисел как координаты целых точек плоскости λ, μ ; этих точек будет столько, сколько членов содержится в полиноме $f(x)$.

Будем теперь приписывать каждому члену $cpr^\mu x^\lambda$ вес $\alpha\lambda + \beta\mu$, где α и β — взаимно простые числа, причём $\beta > 0$. Иными словами, присвоим множителям x вес α , множителям p — положительный вес β , взаимно простым с p множителям c — вес 0, и положим вес произведения равным сумме весов сомножителей.

Какие бы мы ни взяли числа α и β , среди членов полинома $f(x)$ всегда будут существовать некоторые, имеющие наименьший (при данных α и β) вес γ . Выберем теперь α и β так, чтобы наименьшим весом обладали по меньшей мере два члена полинома $f(x)$. Для этого нужно выбрать такую прямую $\alpha\lambda + \beta\mu = \gamma$, чтобы из рассматриваемых целых точек по меньшей мере две лежали на ней и ни одной — под ней; числа α и β и определяются тогда из представления углового коэффициента этой прямой в виде несократимой дроби $\frac{\alpha}{\beta}$.

Пусть, скажем, (λ_1, μ_1) и (λ_2, μ_2) — те две из пар (λ, μ) , для которых $\alpha\lambda + \beta\mu$ принимает наименьшее возможное значение γ , причём λ_1 — наименьшее, а λ_2 — наибольшее из чисел, удовлетворяющих этому условию. Из равенств

$$\alpha\lambda_1 + \beta\mu_1 = \alpha\lambda_2 + \beta\mu_2 = \gamma$$

имеем тогда

$$(1) \quad \alpha(\lambda_2 - \lambda_1) + \beta(\mu_2 - \mu_1) = 0$$

и, следовательно, $\alpha(\lambda_2 - \lambda_1)$, а потому также $\lambda_2 - \lambda_1$ делится на β :

$$\lambda_2 - \lambda_1 = m\beta, \quad \mu_2 - \mu_1 = -m\alpha, \quad m = (\lambda_2 - \lambda_1, \mu_2 - \mu_1).$$

Мы утверждаем теперь: Если полином $f(x)$ степени n разложим в произведение двух полиномов, то степени их необходимо имеют вид

$$(2) \quad m_1\beta + r_1 \text{ и } m_2\beta + r_2,$$

где

$$m_1, m_2, r_1, r_2 \text{ все } \geq 0, \quad m_1 + m_2 = m, \quad r_1 + r_2 = n - m\beta.$$

Доказательство. Пусть $f(x) = g_1(x) \cdot g_2(x)$ и γ_1 — наименьший из весов членов полинома $g_1(x)$, а γ_2 — наименьший из весов членов полинома $g_2(x)$ (при ранее выбранных нами α и β). Среди членов полинома $g_1(x)$, имеющих вес γ_1 , пусть dx^{δ} — имеющий наименьший показатель δ и ex^{ϵ} — имеющий наибольший показатель ϵ , и пусть rx^{ρ} и sx^{σ} — аналогично определённые члены полинома $g_2(x)$. Составляя теперь произведение $g_1(x)g_2(x)$, мы получим некоторое число членов веса $\gamma_1 + \gamma_2$, и среди них член $drx^{\delta+\rho}$ с наименьшим и член $esx^{\epsilon+\sigma}$ с наибольшим показателем; остальные члены будут обладать большими весами. Но объединение какого-нибудь члена с весом $\gamma_1 + \gamma_2$, как, например, члена $drx^{\delta+\rho}$ или $esx^{\epsilon+\sigma}$, с членами, имеющими большие веса, не изменит его веса. Если теперь произведение g_1g_2 совпадает с $f(x)$, то, очевидно, должны выполняться равенства

$$\gamma_1 + \gamma_2 = \gamma, \quad \delta + \rho = \lambda_1, \quad \epsilon + \sigma = \lambda_2,$$

откуда

$$(\epsilon - \delta) + (\sigma - \rho) = \lambda_2 - \lambda_1 = m\beta.$$

Далее, на таком же основании, как ранее $\lambda_2 - \lambda_1$, также $\epsilon - \delta$ и $\sigma - \rho$ должны делиться на β , ибо, например, δ и ϵ играют для $g_1(x)$ ту же роль, что λ_1 и λ_2 для $f(x)$. Следовательно,

$$\epsilon - \delta = m_1\beta, \quad \sigma - \rho = m_2\beta, \quad m_1 + m_2 = m.$$

Наконец, степень полинома $g_1(x)$ не меньше чем ϵ и, значит, $\geq m_1\beta$; точно так же степень полинома $g_2(x)$ не меньше чем $m_2\beta$. Отсюда непосредственно и вытекают утверждаемые выражения для степеней полиномов $g_1(x)$ и $g_2(x)$.

Следствие 1. По крайней мере одна из степеней (2) будет $\geq \beta$.

Следствие 2. Если первый и последний члены полинома $f(x)$ обладают наименьшим весом γ , то степени полиномов g_1 и g_2 делятся на β . Действительно, в этом случае

$$m\beta = \lambda_2 - \lambda_1 = n - 0 = n, \quad r_1 + r_2 = n - m\beta = 0, \quad r_1 = r_2 = 0.$$

Следствие 3. Если $\beta = n$, то полином $f(x)$ неприводим (вытекает из следствия 1).

Беря, в частности, $\alpha = 1$, $\beta = \gamma = n$, получим признак Эйзенштейна.

Пример 1. Пусть $f(x) = x^n + cx^p$, ($c, p = 1$, ($m, n = 1$). Линейная форма $m\lambda + n\mu$ принимает для обоих членов полинома $f(x)$ значение nm . Таким образом, следует положить $\alpha = m$, $\beta = n$. Согласно следствию 3, $f(x)$ неразложим.

Пример 2. Пусть $n \geq 2$ и $f(x) = x^n + px + bp^2$. Линейная форма $\lambda + (n-1)\mu$ принимает для первых двух членов значение n , а для последнего — значение $2n-2 \geq n$. Мы можем поэтому положить $\alpha = 1$, $\beta = n-1$. Если полином $f(x)$ разложим, то, согласно следствию 1, один из его множителей должен быть $(n-1)$ -й степени, и потому другой — линейным.

Из многочисленных работ, посвящённых дальнейшим обобщениям критериев неприводимости, отметим работы О. Ore, *Math. Zeitschr.*, 18 (1923), 278—288, I. Schur, *Sitzungsber. Preuss. Akad., Berlin* (1929), 125—136 и 370—391, H. L. Dörwart and O. Ore, *Ann. of Math.*, 34 (1933), 81—94.

§ 25. Разложение на множители конечным числом проб.

Хотя мы и убедились в теоретической возможности разложения на простые множители каждого полинома из $\Sigma[x_1, \dots, x_n]$ при заданном поле Σ , а в некоторых случаях указали также средства для действительного выполнения этого разложения или же, наоборот, обнаружения его невозможности, — тем не менее мы ещё не обладаем общим методом, который позволял бы в каждом случае выполнить разложение конечным числом проб. В настоящем параграфе мы изложим подобный метод, годный, по крайней мере, для случая, когда Σ есть поле рациональных чисел.

Согласно § 23, мы можем ограничиться рассмотрением полиномов с целыми коэффициентами и разлагать их на такие же полиномы. Очевидно, в самом кольце C целых чисел разложение на простые множители можно выполнить конечным числом проб; кроме того, в этом кольце имеется лишь конечное число делителей единицы (а именно, $+1$ и -1) и, значит, возможно лишь конечное число разложений. В области полиномов $C[x_1, \dots, x_n]$ делителями единицы служат также лишь $+1$ и -1 . Таким образом, полной индукцией по числу переменных n всё сводится к следующей проблеме:

Пусть в $\mathfrak{S}$ каждый элемент может быть разложен на простые множители конечным числом проб; пусть, кроме того, в $\mathfrak{S}$ существует лишь конечное число делителей единицы. Найти метод разложения каждого полинома из $\mathfrak{S}[x]$ на простые множители конечным числом проб.

Излагаемое ниже решение этой проблемы принадлежит Кронекеру.

Пусть $f(x)$ — полином n -й степени из $\mathfrak{S}[x]$. Если $f(x)$ разложим, то один из множителей будет степени $\leq \frac{n}{2}$; таким образом, надо исследовать, может ли $f(x)$ иметь делитель $g(x)$ степени $\leq s$, где s — наибольшее целое число, не превосходящее $\frac{n}{2}$.

Найдём значения $f(a_0), f(a_1), \dots, f(a_s)$ полинома $f(x)$ для $s+1$ произвольно выбранных целочисленных значений аргумента $a_0, a_1, \dots, a_s$. Если теперь $f(x)$ делится на $g(x)$, то $f(a_0)$ должно делиться на $g(a_0)$, $f(a_1)$ — на $g(a_1)$ и т. д. Но так как каждое $f(a_i)$ обладает в $\mathfrak{S}$ лишь конечным числом делителей, то для каждого $g(a_i)$ имеется лишь конечное число возможных значений, причём, по предположению, все они могут быть найдены. Для каждой возможной комбинации значений $g(a_0), g(a_1), \dots, g(a_s)$ существует, согласно теореме § 22, единственный полином $g(x)$, причём этот полином всегда может быть задан в явном виде (например, с помощью интерполяционной формулы Лагранжа или — что удобнее — Ньютона). Тем самым будет найдено конечное число полиномов $g(x)$, среди которых только и могут содержаться делители полинома $f(x)$. Для каждого из этих полиномов $g(x)$ можно с помощью алгоритма деления установить, действительно ли он является делителем полинома $f(x)$. Если ни один из этих полиномов, за исключением делителей единицы, не является делителем полинома $f(x)$, то $f(x)$ неразложим; в противном случае будет найдено разложение $f(x)$ на два множителя и каждый из них, в свою очередь, может быть подвергнут такому же исследованию, и т. д. В конце концов мы придём таким способом к неразложимым далее множителям.

В случае $\mathfrak{S} = C$ описанный процесс часто можно весьма значительно сократить. Прежде всего, разлагая заданный полином по модулю 2 и, возможно, ещё по модулю 3, можно определить, каковы должны быть степени предполагаемых полиномиальных делителей $g(x)$ и к каким классам вычетов по модулю 2 или 3 должны принадлежать коэффициенты этих полиномов. Это уже существенно ограничивает число возможных делителей $g(x)$.

под весом полинома $\varphi(\sigma_1, \dots, \sigma_n)$ наивысший из весов входящих в него членов. Таким образом полиномы $\varphi_1(\sigma_1, \dots, \sigma_n)$ веса k будут давать симметрические полиномы от x_i степени $\leq k$.

Так называемая основная теорема о симметрических функциях утверждает теперь, что эта связь действительна и в обратную сторону:

Каждая целая рациональная симметрическая функция степени k из $\sigma[x_1, \dots, x_n]$ может быть записана в виде полинома $\varphi(\sigma_1, \dots, \sigma_n)$ веса k .

Разумеется, наиболее существенным в этой теореме является то, что каждая симметрическая функция может быть выражена через элементарные симметрические функции $\sigma_1, \dots, \sigma_n$; прибавление о степени и весе служит главным образом для облегчения доказательства методом полной индукции.

Предпошлём доказательству следующее замечание: если два полинома из $\sigma[x_1, \dots, x_n]$ равны и делятся на x_1 , то равенство полиномов сохранится и после сокращения всех членов на x_1 ; это справедливо независимо от того, обладает ли σ делителями нуля или нет, просто потому, что равенство двух полиномов означает полное совпадение их соответственных коэффициентов.

Полагая теперь в обеих частях тождества (1) $x_n = 0$, а прочие x_i оставляя неизвестными, мы получим:

$$(z - x_1) \dots (z - x_{n-1}) z = z^n - (\sigma_1)_0 z^{n-1} + \dots + (-1)^{n-1} (\sigma_{n-1})_0 z,$$

где $(\sigma_i)_0$ означает выражение, получающееся из σ_i при $x_n = 0$. Сокращая, на основании сделанного только что замечания, обе части на z , получим:

$$(z - x_1) \dots (z - x_{n-1}) = z^{n-1} - (\sigma_1)_0 z^{n-2} + \dots + (-1)^{n-1} (\sigma_{n-1})_0.$$

Это равенство показывает, что выражения $(\sigma_1)_0, \dots, (\sigma_{n-1})_0$ являются элементарными симметрическими функциями первых $n-1$ неизвестных.

Доказательство основной теоремы мы проведём путём индукции по n . Для $n=1$ теорема верна, поскольку относительно одной лишь переменной x_1 каждый полином $f(x_1)$ симметричен и $\sigma_1 = x_1$, так что $f(x_1) = f(\sigma_1)$. Пусть, таким образом, теорема уже доказана для полиномов от $n-1$ переменных ($n > 1$); покажем, что она верна тогда и для n переменных.

Для полиномов нулевой степени от n переменных теорема тривиальна. Мы можем поэтому принять ещё, что она доказана уже для всех полиномов степеней $< k$ от n переменных, и доказывать её лишь для полиномов k -й степени от n переменных.

Пусть теперь $f(x_1, \dots, x_n)$ — заданный симметрический полином k -й степени. Положив $x_n = 0$, будем иметь по предположениям индукции

$$f(x_1, \dots, x_{n-1}, 0) = \varphi((\sigma_1)_0, \dots, (\sigma_{n-1})_0),$$

где φ , как функция от элементарных симметрических функций от $x_1, \dots, x_{n-1}$, имеет вес $\leq k$. Поэтому функция $\varphi(\sigma_1, \dots, \sigma_{n-1})$ также имеет вес $\leq k$. Образует теперь разность

$$f_1 = f(x_1, \dots, x_{n-1}, x_n) - \varphi(\sigma_1, \dots, \sigma_{n-1}).$$

Полином $f_1(x_1, \dots, x_n)$, очевидно, является симметрическим. Первый член правой части имеет степень k , а второй — вес $\leq k$ и, значит, как полином от $x_1, \dots, x_n$, — степень $\leq k$; следовательно, f_1 имеет степень $\leq k$. Кроме того, f_1 при $x_n = 0$ обращается в нуль, откуда следует, что все члены этого полинома содержат множителем x_n . Но так как f_1 — симметрическая функция, то все члены содержат множителями также $x_1, x_2, \dots, x_{n-1}$. Вынося из всех членов произведение $x_1 x_2 \dots x_n = \sigma_n$, мы получим:

$$f_1 = \sigma_n g(x_1, \dots, x_n),$$

где g есть снова симметрический полином, причём степень его $\leq k - n < k$. Согласно предположению, g может быть выражен через $\sigma_1, \dots, \sigma_n$:

$$g = \psi(\sigma_1, \dots, \sigma_n),$$

где ψ — полином веса $\leq k - n$. Отсюда для f получается представление

$$f = f_1 + \varphi(\sigma_1, \dots, \sigma_{n-1}) = \sigma_n \psi(\sigma_1, \dots, \sigma_n) + \varphi(\sigma_1, \dots, \sigma_{n-1}).$$

Правая часть есть целая рациональная функция от $\sigma_1, \dots, \sigma_n$ и имеет вес, не превосходящий k . Он не может быть и меньше k , так как иначе полином f имел бы степень $< k$. Таким образом, вес правой части равен точно k , и теорема полностью доказана.

Изложенное доказательство доставляет одновременно способ действительного нахождения выражения любой заданной симметрической функции через элементарные симметрические функции σ_i . Но этот метод несколько громоздок; ниже мы укажем метод, быстрее приводящий к цели.

Из доказательства видно ещё, что однородные симметрические функции могут быть представлены в виде «изобарных» выражений от σ_i , т. е. выражений, все члены которых имеют один и тот же вес.

Покажем теперь, что симметрическая функция может быть выражена в виде целой рациональной функции от $\sigma_1, \dots, \sigma_n$ лишь единственным образом; точнее:

Если $\varphi_1(y_1, \dots, y_n)$ и $\varphi_2(y_1, \dots, y_n)$ — два полинома от неизвестных $y_1, \dots, y_n$, и

$$\varphi_1(y_1, \dots, y_n) \neq \varphi_2(y_1, \dots, y_n),$$

то также

$$\varphi_1(\sigma_1, \dots, \sigma_n) \neq \varphi_2(\sigma_1, \dots, \sigma_n).$$

т. е. если $\varphi_1(y_1, \dots, y_n) \neq \varphi_2(y_1, \dots, y_n)$, то полиномы φ_1 и φ_2 таковы, что $\varphi_1(\sigma_1, \dots, \sigma_n) \neq \varphi_2(\sigma_1, \dots, \sigma_n)$ т. е. φ -символ

Рассмотрение разности $\varphi_1 - \varphi_2 = \varphi$ показывает, что достаточно доказать следующее предложение:

Из $\varphi(y_1, \dots, y_n) \neq 0$ следует $\varphi(\sigma_1, \dots, \sigma_n) \neq 0$.

Теорема верна для $n=1$, так как тогда σ_1 есть само неизвестное x_1 и тем самым из $\varphi(y_1) \neq 0$ всегда следует $\varphi(\sigma_1) \neq 0$.

Таким образом, достаточно доказать теорему для произвольного $n > 1$ в предположении, что она уже справедлива для любого меньшего числа неизвестных. Но предположим, что для n теорема уже не верна. Тогда существует полином $\varphi(y_1, \dots, y_n) \neq 0$ такой, что $\varphi(\sigma_1, \dots, \sigma_n) = 0$, причём мы можем считать степень его m относительно y_n наименьшей возможной. Развёртывая $\varphi(y_1, \dots, y_n)$ по степеням y_n , получаем пару соотношений вида

$$\varphi_m y_n^m + \varphi_{m-1} y_n^{m-1} + \dots + \varphi_0 \neq 0,$$

$$(2) \quad \varphi_m(\sigma_1, \dots, \sigma_{n-1}) \sigma_n^m + \dots + \varphi_0(\sigma_1, \dots, \sigma_{n-1}) = 0.$$

Здесь $\varphi_0(y_1, \dots, y_{n-1}) \neq 0$, так как в противном случае мы могли бы все члены первого соотношения сократить на y_n и точно так же все члены второго — на σ_n , и получили бы:

$$\bar{\varphi}(y_1, \dots, y_n) = \varphi_m y_n^{m-1} + \dots + \varphi_1 \neq 0,$$

$$\bar{\varphi}(\sigma_1, \dots, \sigma_n) = \varphi_m(\sigma_1, \dots, \sigma_{n-1}) \sigma_n^{m-1} + \dots + \varphi_1(\sigma_1, \dots, \sigma_{n-1}) = 0,$$

где $\bar{\varphi}$ — полином степени $< m$, что, однако, противоречит предположению. Положив теперь в (2) $x_n = 0$, мы получим:

$$\varphi_0((\sigma_1)_0, \dots, (\sigma_{n-1})_0) = 0,$$

хотя, как только что было замечено, $\varphi_0(y_1, \dots, y_{n-1})$ должно быть $\neq 0$. Но это противоречит предположению индукции.

Итак, мы доказали следующее предложение:

Каждый симметрический полином из $\sigma[x_1, \dots, x_n]$ может быть записан в виде полинома от $\sigma_1, \dots, \sigma_n$ одним и только одним способом; вес этого полинома от $\sigma_1, \dots, \sigma_n$ равен степени заданного симметрического полинома от $x_1, \dots, x_n$.

Все целые рациональные соотношения между симметрическими функциями остаются в силе и в том случае, когда x_i суть не неизвестные, а величины из σ , например, корни полинома $f(z)$, распадающегося в $\sigma[z]$ на линейные множители. Таким образом, из доказанного следует, в частности, что каждая симметрическая функция от корней полинома $f(z)$ может быть выражена через его коэффициенты.

Существуют различные практические методы выражения заданной симметрической функции через элементарные симметрические функции $\sigma_1, \dots, \sigma_n$. Мы приведём здесь лишь ещё один из них. Расположим заданный симметрический полином «лексикографически»

(как в словаре), т. е. так, чтобы член $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ предшествовал члену $x_1^{\beta_1} \dots x_n^{\beta_n}$ в том случае, когда первая отличная от нуля разность $\alpha_i - \beta_i$ положительна. В симметрическом полиноме вместе с членом $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ содержатся также члены, получающиеся путём всевозможных перестановок показателей α_i ; мы не будем их отдельно выписывать, обозначая сразу всю совокупность этих получающихся друг из друга членов символом $\sum x_1^{\alpha_1} \dots x_n^{\alpha_n}$, где всегда будем принимать $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$. Найдём теперь для начального члена $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$ заданного и лексикографически расположенного полинома произведение элементарных симметрических функций, имеющее (после перемножения и лексикографического расположения) тот же начальный член $ax_1^{\alpha_1} \dots x_n^{\alpha_n}$; таким произведением будет, очевидно, служить

$$a\sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \dots \sigma_n^{\alpha_n}.$$

Вычтем затем это произведение из заданного полинома, расположим разность снова в лексикографическом порядке, поступим с её начальным членом таким же образом, и т. д.

Задача 1. Показать, что описанный процесс всегда приводит к цели, и извлечь отсюда второе доказательство основной теоремы, а также теоремы единственности.

Задача 2. Выразить при любом n «степенные суммы» $\sum x_i$, $\sum x_i^2$, $\sum x_i^3$ через элементарные симметрические функции.

Задача 3. Пусть $\sum x_i^p = s_p$. Доказать формулы:

$$s_p - s_{p-1}\sigma_1 + s_{p-2}\sigma_2 - \dots + (-1)^{p-1}s_1\sigma_{p-1} + (-1)^p\sigma_p = 0 \text{ при } p \leq n,$$

$$s_p - s_{p-1}\sigma_1 + \dots + (-1)^n s_{p-n}\sigma_n = 0 \text{ при } p > n$$

и выразить с их помощью степенные суммы s_1, s_2, s_3, s_4, s_5 через элементарные симметрические функции.

Задача 4. Если положить, в соответствии с основной теоремой,

$$s_p = \sum a_{\lambda_1, \dots, \lambda_n} \sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \dots \sigma_n^{\lambda_n}$$

(где суммирование производится по всем λ_i , удовлетворяющим условию $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \dots = p$), то получим из формул задачи 3 следующие рекуррентные формулы для $a_{\lambda_1, \dots, \lambda_n}$:

$$a_{\lambda_1, \dots, \lambda_n} = a_{\lambda_1-1, \dots, \lambda_n} - a_{\lambda_1, \lambda_2-1, \dots, \lambda_n} + \dots [+ (-1)^{p-1} \rho],$$

где член в прямых скобках встречается (и притом в качестве единственного) лишь тогда, когда $\lambda_p = 1$, а все остальные $\lambda_i = 0$, и где все a , содержащие отрицательный индекс, принимаются равными

нулю. Показать, что решением этого рекуррентного соотношения служит

$$a_{\lambda_1, \dots, \lambda_n} = (-1)^{\lambda_1 + \lambda_2 + \dots + \lambda_n} \frac{\rho \cdot (\lambda_1 + \lambda_2 + \dots + \lambda_n - 1)!}{\lambda_1! \lambda_2! \dots \lambda_n!}.$$

Задача 5. Пусть

$$(k_1, \dots, k_h) = \sum x_1^{k_1} x_2^{k_2} \dots x_h^{k_h},$$

где суммируются все различные члены, получающиеся, если, оставляя все показатели на месте, переставлять индексы 1, 2, ..., h неизвестных x. Доказать, что

$$\begin{aligned} (k_1, \dots, k_h) \cdot (m) &= \\ &= c_1(k_1 + m, k_2, \dots, k_h) + c_2(k_1, k_2 + m, \dots, k_h) + \dots \\ &\quad \dots + c_h(k_1, k_2, \dots, k_h + m) + c_0(k_1, \dots, k_h, m), \end{aligned}$$

где коэффициенты c_i ($i = 1, \dots, h$), соответственно c_0 , означают число тех содержащихся в стоящем рядом символе чисел, которые равны $k_i + m$, соответственно m .

Задача 6. Разрешить формулу предыдущей задачи относительно $(k_1, \dots, k_h, m)$ и извлечь отсюда способ представления любой симметрической функции через степенные суммы (m) (в предположении, что в основном кольце возможно деление на любое отличное от нуля целое число).

Важной симметрической функцией является произведение квадратов разностей:

$$D = \prod_{i < k} (x_i - x_k)^2.$$

Выражение этой функции D в виде полинома от $a_1 = -\sigma_1$, $a_2 = \sigma_2, \dots, a_n = (-1)^n \sigma_n$ называется дискриминантом полинома $f(z) = z^n + a_1 z^{n-1} + \dots + a_n$; обращение дискриминанта для частной системы значений $a_1, \dots, a_n$ в нуль указывает, что соответствующий полином $f(z)$ имеет кратный линейный множитель.

Если, более обще, $f(z)$ — полином с произвольным старшим коэффициентом a_0 :

$$f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n,$$

то

$$\sigma_1 = -\frac{a_1}{a_0}, \quad \sigma_2 = \frac{a_2}{a_0}, \quad \dots, \quad \sigma_n = (-1)^n \frac{a_n}{a_0}.$$

В этом случае дискриминантом называют произведение квадратов разностей, умноженное на a_0^{2n-2} :

$$D = a_0^{2n-2} \prod_{i < k} (x_i - x_k)^2.$$

Как мы увидим в § 28, D есть полином от $a_0, a_1, \dots, a_n$.

ограничить
дискриминант
D=0
если
k_i = x_i

Применяя изложенный выше общий метод, получаем следующие выражения дискриминантов:

для $a_0x^2 + a_1x + a_2$:

$$D = a_1^2 - 4a_0a_2,$$

для $a_0x^3 + a_1x^2 + a_2x + a_3$:

$$D = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3.$$

Задача 7. Дискриминант не изменяется при замене всех x_i на $x_i + h$. Вывести отсюда дифференциальное соотношение

$$\Omega D = n \frac{\partial D}{\partial a_1} + (n-1) a_1 \frac{\partial D}{\partial a_2} + \dots + a_{n-1} \frac{\partial D}{\partial a_n} = 0.$$

§ 27. Результат двух полиномов.

Пусть K — произвольное поле и

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n,$$

$$g(x) = b_0x^m + b_1x^{m-1} + \dots + b_m$$

— два полинома из $K[x]$. Найдём необходимое и достаточное условие для того, чтобы эти полиномы обладали общим делителем $\varphi(x)$, не являющимся константой.

При этом мы не будем считать исключённым, что $a_0 = 0$ или $b_0 = 0$, т. е. что степень $f(x)$ на самом деле меньше чем n или степень $g(x)$ — меньше чем m . Если полином $f(x)$ записан в указанном виде, начинаясь (возможно равным нулю) членом a_0x^n , то мы будем называть n *формальной степенью* этого полинома, а a_0 — *формальным старшим коэффициентом*. Мы примем пока, что по крайней мере один из старших коэффициентов a_0, b_0 отличен от нуля.

При этом предположении мы покажем прежде всего, что $f(x)$ и $g(x)$ тогда и только тогда обладают общим делителем $\varphi(x)$, не являющимся константой, если имеет место равенство вида

$$(1) \quad h(x)f(x) = k(x)g(x),$$

где степень полинома $h(x)$ не превышает $m-1$, степень полинома $k(x)$ не превышает $n-1$, и один, по крайней мере, из этих полиномов не равен тождественно нулю.

Действительно, если равенство (1) выполнено, то, разлагая обе его части на простые множители, мы должны и слева и справа получить одно и то же разложение. Пусть, скажем, $f(x)$ действительно имеет степень n , т. е. $a_0 \neq 0$ (в противном случае мы поменяли бы ролями $f(x)$ и $g(x)$). Все простые множители полинома $f(x)$ должны содержаться также в правой части равенства (1) и притом столько же раз, сколько они содержатся в $f(x)$. Но в одном

относительно элементов a_i и однородный полином степени n относительно элементов b_j ; далее, что он содержит «главный член» $a_0^m b_m^n$ (произведение элементов главной диагонали), и наконец, что он обращается в нуль не только тогда, когда полиномы f , g имеют общий делитель, но также и в том случае, когда (против сделанного вначале предположения) $a_0 = b_0 = 0$.

Итак:

Результант двух полиномов $f(x)$, $g(x)$ есть целая рациональная форма вида (3) от их коэффициентов. Если результат равен нулю, то либо полиномы f , g имеют общий делитель, не являющийся константой, либо в обоих полиномах старшие коэффициенты равны нулю, и обратно.

Метод исключения, которому мы следовали, принадлежит Эйлеру; выражение (3) наиболее известно под наименованием результата в форме Сильвестра.

В формулировке теоремы можно избежать исключительного случая $a_0 = b_0 = 0$, если вместо полиномов от одного переменного ввести однородные формы от двух переменных:

$$\begin{aligned} F(x) &= a_0 x_1^n + a_1 x_1^{n-1} x_2 + \dots + a_n x_2^n, \\ G(x) &= b_0 x_1^m + b_1 x_1^{m-1} x_2 + \dots + b_m x_2^m. \end{aligned}$$

Первоначальные полиномы f , g и числа m , n однозначно определяют формы F , G , и обратно. Каждому разложению на множители полинома f :

$$\begin{aligned} f(x) &= a_0 x^n + a_1 x^{n-1} + \dots + a_n = \\ &= (p_0 x^r + \dots + p_r)(q_0 x^s + \dots + q_s) \end{aligned}$$

соответствует разложение на множители формы F :

$$\begin{aligned} F(x) &= a_0 x_1^n + \dots + a_n x_2^n = \\ &= (p_0 x_1^r + \dots + p_r x_2^r)(q_0 x_1^s + \dots + q_s x_2^s), \end{aligned}$$

и то же верно для g и G . Поэтому каждому общему делителю полиномов f и g соответствует общий делитель форм F и G . И обратно, каждое разложение формы F или G , если положить в нём $x_1 = x$, $x_2 = 1$, тотчас же даёт разложение полинома f , соответственно, g , и каждый общий делитель форм F и G даёт общий делитель полиномов f и g ; однако, при этом может случиться, что этим общим делителем форм F и G служит степень переменного x_2 , и потому соответствующим общим делителем полиномов f и g является константа. Но этот случай, когда формы F и G обе делятся на x_2 , и есть как раз случай $a_0 = b_0 = 0$. Тем самым оба отмеченных в сформулированной выше теореме случая, при которых результат обращается в нуль, охватываются одним предложением: F и G обладают однородным общим делителем, не являющимся константой.

$a_0^m b_0^n$ на некоторую функцию, симметрическую как относительно корней x_i , так и относительно корней y_k . *и. е. R симметрич. ф-я*

Примем теперь сперва корни x_i и y_k за неизвестные. Полином R обращается в нуль при $x_i = y_k$, так как в этом случае полиномы $f(x)$ и $g(x)$ имеют общий линейный множитель. Поэтому R делится на $x_i - y_k$ (§ 21). Так как линейные формы $x_i - y_k$ взаимно просты, то R должен делиться на произведение

$$(1) \quad S = a_0^m b_0^n \prod_i \prod_k (x_i - y_k).$$

Это произведение можно преобразовать двояким образом. С одной стороны, подставляя $x = x_i$ ($i = 1, \dots, n$) в формулу

$$g(x) = b_0 \prod_k (x - y_k)$$

и перемножая результаты, получаем:

$$\prod_i g(x_i) = b_0^n \prod_i \prod_k (x_i - y_k), \dots$$

и, значит,

$$(2) \quad S = a_0^m \prod_i g(x_i).$$

С другой стороны, из равенства

$$f(x) = a_0 \prod_i (x - x_i) = (-1)^n a_0 \prod_i (x_i - x)$$

аналогичным образом получаем, что

$$(3) \quad S = (-1)^{mn} b_0^n \prod_k f(y_k).$$

Формула (2) показывает, что S есть целая однородная функция степени n относительно коэффициентов b , а формула (3), — что S есть целая однородная функция степени m относительно коэффициентов a . Но R имеет те же степени относительно коэффициентов a и b и делится на S ; следовательно, R должен с точностью до целочисленного множителя совпадать с S . Но так как членом, содержащим высшую степень коэффициента b_m , и в R и в S служит $+a_0^m b_m^n$, то этот числовой множитель равен единице, т. е.

$$R = S.$$

Тем самым мы нашли для R три представления (1), (2), (3). Согласно теореме единственности из § 26, равенство (2) имеет место тождественно относительно коэффициентов b , и (3) — тождественно относительно коэффициентов a ; таким образом, (2) выполняется и в том случае, когда $g(x)$ не разлагается на линейные множители.

Отсюда легко следует также неразложимость результата, как полинома относительно неизвестных $a_0, \dots, b_m$, и притом нераз-

ложимость не только в области целочисленных полиномов, но и абсолютная неприводимость, т. е. неразложимость в области полиномов от тех же неизвестных с коэффициентами из произвольного поля. Действительно, если бы R разлагался на два множителя A, B , то мы снова могли бы записать A и B в виде симметрических функций от корней¹⁾. Так как R делится на $x_1 - y_1$, то на $x_1 - y_1$ должен делиться один из сомножителей A, B — пусть это будет, скажем, A . Но тогда, будучи симметрической функцией, A должно делиться и на все другие $x_i - y_k$, а значит, и на произведение

$$\prod_i \prod_k (x_i - y_k).$$

Но так как

$$R = a_0^m b_0^n \prod_i \prod_k (x_i - y_k),$$

то для второго множителя B остаётся лишь возможность $B = a_0^p b_0^q$.

Однако, R , как полином относительно коэффициентов a и b , не делится ни на a_0 , ни на b_0 . Следовательно, необходимо $B = 1$. Тем самым и доказана неприводимость результата R .

Другое доказательство см. в книге F. S. Macauley. The algebraic Theory of Modular Systems, § 3. Cambridge, 1916.

Имеется интересная связь между результатом двух полиномов и дискриминантом одного полинома. А именно, образуем результат $R(f, f')$ полинома

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n = a_0 (x - x_1)(x - x_2) \dots (x - x_n)$$

и его производной $f'(x)$. Тогда, согласно формуле (2),

$$(4) \quad R(f, f') = a_0^{n-1} \prod_i f'(x_i).$$

Но в силу правила дифференцирования произведения,

$$f'(x) = \sum_i a_0 (x - x_1) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_n),$$

и

$$f'(x_i) = a_0 (x_i - x_1) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_n).$$

Подставив это в (4), получим:

$$R(f, f') = a_0^{2n-1} \prod_{i \neq k} (x_i - x_k) = a_0^{2n-1} \prod_{i < k} (x_i - x_k)^2$$

или, обозначая дискриминант полинома f через D ,

$$(5) \quad R(f, f') = a_0 D.$$

¹⁾ Здесь автор существенно опирается на теорему о существовании корня всякого алгебраического уравнения в надлежащем расширении поля коэффициентов, которая будет доказана лишь в § 32 (см. также § 35, где вводится понятие поля разложения). *Перев.*

Если записать $R(f, f')$, по § 27, в виде определителя, то из первого столбца можно будет вынести множителем a_0 . Таким образом, D есть полином от $a_0, \dots, a_n$. Разумеется, формула (5) выполняется снова тождественно относительно $a_0, \dots, a_n$, независимо от того, разлагается ли в действительности $f(x)$ на линейные множители.

Задача 1. Результат полиномов f и g изобарен с весом mn по совокупности коэффициентов a и b (см. § 26).

Задача 2. Если $y_1, \dots, y_{n-1}$ — корни производной $f'(x)$, то

$$D = n^n a_0^{n-1} \prod_k f(y_k).$$

Задача 3. Дискриминант D полинома $f(x)$ обращается в нуль тогда и только тогда, когда $f(x)$ и $f'(x)$ имеют общий делитель. Если D равен нулю, то в разложении полинома $f(x)$ на простые множители содержится либо кратный множитель, либо множитель, производная которого тождественно равна нулю.

§ 29. Разложение рациональных функций на простейшие дроби.

Разложение рациональных функций на простейшие дроби основывается на следующей теореме о целых рациональных функциях.

Пусть $g(x)$ и $h(x)$ — два взаимно простых полинома над некоторым полем K , $g(x)$ — степени a , $h(x)$ — степени b , и пусть $f(x)$ — произвольный полином, степень которого меньше чем $a + b$. Тогда имеет место тождество

$$(1) \quad f(x) = r(x) g(x) + s(x) h(x),$$

где $r(x)$ — некоторый полином, степень которого меньше чем b , и $s(x)$ — полином, степень которого меньше чем a .

Доказательство. По предположению, наибольший общий делитель полиномов $g(x)$ и $h(x)$ равен единице. Поэтому имеет место тождество

$$1 = c(x) g(x) + d(x) h(x).$$

Умножив обе части на $f(x)$, получим:

$$(2) \quad f(x) = \underline{f(x) c(x)} g(x) + f(x) d(x) h(x).$$

Для приведения степени полинома, стоящего множителем при $g(x)$, к значению, меньшему чем b , разделим полином $f(x) c(x)$ на $h(x)$; получим:

$$(3) \quad f(x) c(x) = q(x) h(x) + r(x),$$

где степень остатка $r(x)$ меньше степени делителя $h(x)$, т. е. меньше чем b . Подставляя (3) в (2), получаем:

$$\begin{aligned} f(x) &= r(x) g(x) + [f(x) d(x) + q(x) g(x)] h(x) = \\ &= r(x) g(x) + s(x) h(x). \end{aligned}$$

При этом левая часть и первый член правой части имеют степень, меньшую чем $a + b$, а потому и степень последнего члена правой части меньше чем $a + b$, откуда следует, что степень полинома $s(x)$ меньше чем a . Тем самым утверждение теоремы доказано.

Деля обе части тождества (1) на $g(x)h(x)$, мы получим разложение дроби $\frac{f(x)}{g(x)h(x)}$ на сумму двух дробей

$$\frac{f(x)}{g(x)h(x)} = \frac{r(x)}{h(x)} + \frac{s(x)}{g(x)}.$$

В левой части степень числителя по предположению меньше степени знаменателя. То же имеет место и для обеих дробей в правой части. Если в какой-нибудь из этих дробей знаменатель может быть дальше разложен на два взаимно простых множителя, то эту дробь можно, в свою очередь, разложить указанным образом на сумму двух дробей. Так можно продолжать до тех пор, пока в знаменателях не останутся степени простых полиномов. Это даёт следующую теорему:

Каждая дробь $\frac{f(x)}{k(x)}$ со степенью числителя, меньшей степени знаменателя, представима в виде суммы дробей, знаменателями которых служат те степени простых полиномов, на которые разлагается знаменатель $k(x)$.

Полученные таким способом дроби $\frac{r(x)}{q(x)}$ с знаменателями $q(x) = p(x)^t$ можно подвергнуть дальнейшему расщеплению. А именно, если степень простого полинома $p(x)$ равна l , и, значит, степень $q(x)$ равна lt , то можно числитель $r(x)$, степень которого меньше чем lt , разделить сначала на $p(x)^{t-1}$ с остатком, степень которого будет меньше чем $l(t-1)$, затем этот остаток разделить на $p(x)^{t-2}$ с остатком, степень которого будет меньше чем $l(t-2)$, и т. д.:

$$r(x) = s_1(x)p(x)^{t-1} + r_1(x),$$

$$r_1(x) = s_2(x)p(x)^{t-2} + r_2(x),$$

$$\dots \dots \dots$$

$$r_{t-2}(x) = s_{t-1}(x)p(x) + r_{t-1}(x),$$

$$r_{t-1}(x) = s_t(x).$$

При этом все частные $s_1, \dots, s_t$ будут иметь степени, меньшие чем l . Из совокупности всех этих равенств следует, что

$$r(x) = s_1(x)p(x)^{t-1} + s_2(x)p(x)^{t-2} + \dots + s_{t-1}(x)p(x) + s_t(x),$$

$$(4) \quad \frac{r(x)}{p(x)^t} = \frac{s_1(x)}{p(x)} + \frac{s_2(x)}{p(x)^2} + \dots + \frac{s_{t-1}(x)}{p(x)^{t-1}} + \frac{s_t(x)}{p(x)^t}.$$

Таким образом мы получаем в итоге теорему о разложении на простейшие дроби:

Каждая дробь $\frac{f(x)}{k(x)}$ со степенью числителя, меньшей степени знаменателя, и со знаменателем, обладающим разложением на простые множители

$$k(x) = p_1(x)^{t_1} p_2(x)^{t_2} \dots p_h(x)^{t_h},$$

может быть представлена в виде суммы простейших дробей, знаменателями которых служат степени $p_\nu(x)^{\mu_\nu}$ ($\mu_\nu = 1, 2, \dots, t_\nu$; $\nu = 1, 2, \dots, h$), а числители либо равны нулю, либо имеют, каждой, степень, меньшую чем простой полином $p_\nu(x)$, входящий в знаменатель.

Если, в частности, все простые множители $p_\nu(x)$ линейны, то числители простейших дробей являются константами. В этом важном частном случае можно производить разложение на простейшие дроби с помощью очень простого приёма, отделяя каждый раз простейшую дробь с наибольшей возможной степенью знаменателя и тем самым постоянно понижая степень знаменателя. А именно, записывая знаменатель в виде $k(x) = (x-a)^t g(x)$, где $g(x)$ уже не содержит множителя $x-a$, имеем: -

$$(5) \quad \frac{f(x)}{k(x)} = \frac{f(x)}{(x-a)^t g(x)} = \frac{b}{(x-a)^t} + \frac{f(x) - bg(x)}{(x-a)^t g(x)},$$

где константу b можно всегда определить так, чтобы числитель второй дроби в правой части обращался в нуль при $x=a$ и потому делился на $x-a$:

$$\begin{aligned} f(a) - bg(a) &= 0, \\ f(x) - bg(x) &= (x-a) f_1(x). \end{aligned}$$

После этого мы сможем сократить эту вторую дробь на множитель $x-a$ и затем применять к результату тот же приём, и так до тех пор, пока не придём к полному разложению на простейшие дроби.

ГЛАВА ПЯТАЯ. ТЕОРИЯ ПОЛЕЙ.

Целью этой главы является изложение первоначальных сведений о строении полей, о их простейших подполях и расширениях. Часть излагаемых фактов (§§ 30, 31, 33, 34) относится, впрочем, к произвольным телам.

§ 30. Подполе. Простое поле.

Пусть Σ — тело.

Если некоторое множество Δ элементов тела Σ само есть тело, то оно называется *подтелом* тела Σ . Для этого необходимо и достаточно, во-первых, чтобы Δ было подкольцом (т. е. вместе с a и b содержало также $a - b$ и $a \cdot b$), и, во-вторых, чтобы Δ содержало единицу и вместе с каждым $a \neq 0$ также обратный элемент a^{-1} . Вместо этого можно также потребовать, чтобы Δ содержало хотя бы один элемент, отличный от нуля, и вместе с a и b содержало также $a - b$ и ab^{-1} .

Очевидно, *пересечение произвольного множества подтел тела Σ снова есть подтело этого тела.*

Простым телом называется тело, не обладающее никаким собственным подтелом. Как мы увидим, все простые тела коммутативны.

В каждом теле Σ содержится одно и только одно простое тело.

Доказательство. Пересечение всех подтел тела Σ есть тело, очевидно, уже не обладающее никаким собственным подтелом. Если бы в Σ содержалось два различных простых тела, то их пересечение, будучи подтелом каждого из них, совпадало бы с ними обоими, и, значит, эти тела на самом деле не были бы различны.

Типы простых тел. Пусть Π — простое тело, содержащееся в Σ . Оно содержит нуль и единицу e , а потому также все целые кратные $n \cdot e = \pm \sum e$.

Сложение и умножение этих элементов *не* производится по правилам

$$ne + me = (n + m)e,$$

$$ne \cdot me = nm \cdot e^2 = nm \cdot e.$$

$$1.15.$$

$$(e + \dots + e)(e + \dots + e) = ee + ee + \dots = nme^2$$

Таким образом, *целые кратные не образуют коммутативное кольцо* $\mathfrak{P}$. Далее, соответствие $n \rightarrow ne$ порождает гомоморфное отображение кольца C целых чисел на кольцо $\mathfrak{P}$. Поэтому, в силу теоремы о гомоморфизмах (§ 16), $\mathfrak{P}$ изоморфно некоторому факторкольцу $C/\mathfrak{p}$, где $\mathfrak{p}$ — идеал, образованный теми целыми числами n , которым соответствует нуль, т. е. для которых $ne = 0$. (Во многих известных телах равенство $ne = 0$ возможно лишь при $n = 0$, так что $\mathfrak{p}$ есть нулевой идеал. С другой стороны, например, в поле $C/(p)$ классов вычетов по простому числу p имеет место равенство $pe = 0$.)

Так как $\mathfrak{P}$ не содержит делителей нуля, то и $C/\mathfrak{p}$ не может их содержать; следовательно, $\mathfrak{p}$ должен быть простым идеалом. Далее, $\mathfrak{p}$ не может быть единичным идеалом, ибо в противном случае мы имели бы уже $1 \cdot e = 0$. Таким образом, имеются две возможности:

1. $\mathfrak{p} = (p)$, где p — простое число. p есть тогда наименьшее положительное число, обладающее свойством $pe = 0$. Имеем:

$$\mathfrak{P} \cong C/(p).$$

Но $C/(p)$ есть поле. Следовательно, также кольцо $\mathfrak{P}$ есть поле, представляя собою тем самым искомое простое тело. Таким образом, *в этом случае простое тело Π изоморфно факторкольцу по некоторому простому числу в кольце целых чисел: с элементами $n \cdot e$ можно оперировать как с классами вычетов чисел n по модулю p .*

2. $\mathfrak{p} = 0$. Гомоморфизм $C \rightarrow \mathfrak{P}$ есть изоморфизм. В этом случае кратные ne все различны: из $ne = 0$ следует $n = 0$. Теперь кольцо $\mathfrak{P}$ не является ещё телом, поскольку телом не является кольцо целых чисел. Простое тело Π должно содержать не только элементы кольца $\mathfrak{P}$, но и их отношения. Но мы знаем из § 13, что изоморфные области целостности $\mathfrak{P}$, C должны обладать также изоморфными полями отношений. Тем самым в этом случае *простое тело Π изоморфно полю Γ рациональных чисел.*

Мы видим, таким образом, что все простые тела коммутативны; поэтому мы будем называть их в дальнейшем *простыми полями*.

Строение простого поля, содержащегося в Σ , вполне определяется заданием числа p или 0, порождающего идеал $\mathfrak{p}$ (где, как указано, $\mathfrak{p}$ состоит из тех целых чисел n , для которых $ne = 0$). Число p , соответственно 0, называется *характеристикой* тела Σ или простого поля Π .

Все обычные числовые и функциональные поля, содержащие поле рациональных чисел, имеют характеристику 0.

Из определения характеристики непосредственно вытекает следующая теорема:

Пусть $a \neq 0$ — элемент тела Σ и k — характеристика этого тела. Тогда из $na = ta$ всегда следует $n \equiv t (k)$, и обратно.

В н
Тела
Рис.
Тела
их
иде

Доказательство. Умножая равенство $na = ma$ на a^{-1} , получаем $ne = me$, откуда по определению характеристики $n \equiv m (k)$; то же рассуждение можно провести и в обратном порядке.

Аналогично доказывается, что из $na = nb$ и $n \not\equiv 0 (k)$ следует $a = b$.

Выведем ещё две важные формулы:

В полях характеристики p

$$(a + b)^p = a^p + b^p,$$

$$(a - b)^p = a^p - b^p.$$

Доказательство. По биномиальной теореме (§ 11, задача 5)

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \dots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Но при $0 < i < p$ имеем:

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1 \cdot 2 \dots i} \equiv 0 (p),$$

так как множитель p , содержащийся в числителе, не может сократиться. Следовательно, остаются лишь крайние члены a^p и b^p :

$$(a + b)^p = a^p + b^p.$$

Положив здесь $a + b = a'$, получим:

$$a'^p = (a' - b)^p + b^p,$$

$$(a' - b)^p = a'^p - b^p,$$

чем доказано и второе утверждение.

Задача 1. Доказать индукцией по f , что в случае поля характеристики p

$$(a + b)^{p^f} = a^{p^f} + b^{p^f},$$

$$(a - b)^{p^f} = a^{p^f} - b^{p^f}.$$

Задача 2. Аналогичным образом

$$(a_1 + a_2 + \dots + a_n)^p = a_1^p + a_2^p + \dots + a_n^p.$$

Задача 3. Применить формулу задачи 2 к сумме $1 + 1 + \dots + 1$ по модулю p .

Задача 4. Доказать, что для поля характеристики p

$$(a - b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}.$$

Задача 5. Какие характеристики имеют факторкольца по простым идеалам $(1 + i)$, (3) , $(2 + i)$ в кольце целых гауссовских чисел? (§ 17, задача 3.)

§ 31. Присоединение.

Если Δ — подтело тела Ω , то Ω называется *расширением* или *надтелом* тела Δ .

Целью теории тел является описание всех возможных расширений заданного тела Δ . Тем самым было бы получено одновременно и описание всех вообще возможных тел, поскольку каждое тело можно рассматривать как расширение содержащегося в нём простого поля. Однако, эту цель можно считать достигнутой в наиболее существенных чертах лишь в коммутативном случае.

Пусть Ω — заданное расширение тела Δ , и $\mathcal{S}$ — произвольное множество элементов из Ω . Существуют подтела тела Ω , содержащие Δ и $\mathcal{S}$: таким подтелом является, например, само Ω . Пересечение всех подтел, содержащих Δ и $\mathcal{S}$, само является подтелом, содержащим Δ и $\mathcal{S}$; мы будем обозначать его символом $\Delta(\mathcal{S})$. Это — наименьшее тело, содержащее Δ и $\mathcal{S}$. Мы будем говорить, что $\Delta(\mathcal{S})$ получается из Δ путём *присоединения* множества $\mathcal{S}$. Имеем:

$$\Delta \subseteq \Delta(\mathcal{S}) \subseteq \Omega;$$

оба крайних случая суть: $\Delta(\mathcal{S}) = \Delta$, $\Delta(\mathcal{S}) = \Omega$.

В $\Delta(\mathcal{S})$ содержатся все элементы из Δ и из $\mathcal{S}$, а значит, также все элементы, получающиеся путём сложения, вычитания, умножения и деления из элементов тела Δ и множества $\mathcal{S}$. Но уже сами эти элементы в своей совокупности образуют тело; оно должно, следовательно, совпадать с $\Delta(\mathcal{S})$. Тем самым, $\Delta(\mathcal{S})$ состоит из всех рациональных комбинаций элементов множества $\mathcal{S}$ и тела Δ . В коммутативном случае эти комбинации можно записывать просто в виде отношений целых рациональных функций от элементов множества $\mathcal{S}$ с коэффициентами из поля Δ .

Если $\mathcal{S}$ — конечное множество: $\mathcal{S} = \{u_1, \dots, u_n\}$, то вместо $\Delta(\mathcal{S})$ пишут также $\Delta(u_1, \dots, u_n)$ и говорят, что к Δ присоединены элементы $u_1, \dots, u_n$. Таким образом, круглые скобки обозначают всегда расширение до тела (образование всех вообще рациональных комбинаций), тогда как прямые скобки, например, в $\Delta[x]$, обозначают расширение до кольца (образование всех целых рациональных комбинаций).

В рациональном выражении элемента из $\Delta(\mathcal{S})$ через элементы из Δ и $\mathcal{S}$ содержится в каждом случае лишь конечное число элементов из $\mathcal{S}$. Таким образом, каждый элемент тела $\Delta(\mathcal{S})$ содержится уже в некотором теле $\Delta(\mathcal{I})$, где $\mathcal{I}$ — конечное подмножество множества $\mathcal{S}$. Поэтому $\Delta(\mathcal{S})$ *есть объединение всех тел $\Delta(\mathcal{I})$, где $\mathcal{I}$ может быть произвольным конечным подмножеством множества $\mathcal{S}$.* Тем самым присоединение произвольного множества сводится к присоединению конечных множеств и объединению полученных тел.

Если $\mathfrak{S}$ — объединение множеств $\mathfrak{S}_1$ и $\mathfrak{S}_2$, то, очевидно,

$$\Delta(\mathfrak{S}) = \Delta(\mathfrak{S}_1)(\mathfrak{S}_2).$$

Действительно, $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$ содержит $\Delta(\mathfrak{S}_1)$ и $\mathfrak{S}_2$, следовательно, содержит Δ , $\mathfrak{S}_1$ и $\mathfrak{S}_2$, следовательно, содержит Δ и $\mathfrak{S}$, а потому содержит и $\Delta(\mathfrak{S})$; и обратно, $\Delta(\mathfrak{S})$ во всяком случае содержит Δ , $\mathfrak{S}_1$ и $\mathfrak{S}_2$, следовательно, содержит $\Delta(\mathfrak{S}_1)$ и $\mathfrak{S}_2$, а потому содержит и $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$.

Вследствие этого присоединение конечного множества может быть сведено к конечному числу последовательных присоединений по одному элементу. Расширение тела путём присоединения одного единственного элемента называют простым расширением. Эти расширения для коммутативного случая мы изучим в следующем параграфе.

§ 32. Простые расширения поля.

В этом параграфе мы будем рассматривать только коммутативный случай.

Пусть снова $\Delta \subseteq \Omega$ и ϑ — произвольный элемент из Ω ; исследуем простое расширение $\Delta(\vartheta)$ поля Δ .

Это поле $\Delta(\vartheta)$ содержит, прежде всего, кольцо $\mathfrak{S}$ всех полиномов $\sum a_k \vartheta^k$ ($a_k \in \Delta$). Сравним $\mathfrak{S}$ с областью $\Delta[x]$ полиномов от одного неизвестного x .

Соответствие $f(x) \rightarrow f(\vartheta)$, точнее:

$$\sum a_k x^k \rightarrow \sum a_k \vartheta^k$$

гомоморфно отображает ^{Кольцо} кольцо $\Delta[x]$ на $\mathfrak{S}^1$). Следовательно, согласно теореме о гомоморфизмах,

$$\mathfrak{S} \cong \Delta[x]/\mathfrak{p},$$

где $\mathfrak{p}$ — идеал, образованный теми полиномами $f(x)$, которые имеют ϑ своим корнем, т. е. для которых $f(\vartheta) = 0$.

Так как $\mathfrak{S}$ не содержит делителей нуля, то также факторкольцо $\Delta[x]/\mathfrak{p}$ должно быть свободно от делителей нуля, т. е. идеал $\mathfrak{p}$ должен быть простым. Далее, $\mathfrak{p}$ не может быть единичным идеалом, так как единице отвечает при указанном гомоморфизме не нуль, а снова единица. Так как в $\Delta[x]$ каждый идеал является главным, то остаются лишь две возможности:

1) В некоммутативном случае это уже неверно, ибо переменное x всегда предполагается перестановочным с коэффициентами a_k , тогда как величина ϑ может и не обладать этим свойством. Все рассмотрения настоящего параграфа сохраняют силу лишь в том специальном случае, когда ϑ перестановочно со всеми элементами из Δ .

1. $p = (\varphi(x))$, где $\varphi(x)$ — некоторый полином, неразложимый в $\Delta[x]$ ¹⁾. $\varphi(x)$ есть полином наименьшей степени, обладающий свойством $\varphi(\vartheta) = 0$. Итак, в этом случае

$$\mathfrak{S} \cong \Delta[x]/(\varphi(x)).$$

Но факторкольцо, стоящее в правой части, есть поле (§ 19); в таком случае и кольцо $\mathfrak{S}$ является полем. Следовательно, $\mathfrak{S}$ и есть искомое простое расширение $\Delta(\vartheta)$.

2. $p = (0)$. Гомоморфизм $\Delta[x] \sim \mathfrak{S}$ является на самом деле изоморфизмом. Кроме нуля не существует никакого полинома $f(x)$, который удовлетворял бы условию $f(\vartheta) = 0$, и с выражениями $f(\vartheta)$ можно оперировать так, как если бы ϑ было неизвестным x . В этом случае кольцо $\mathfrak{S} \cong \Delta[x]$ не является ещё полем. Но из изоморфизма этих колец следует изоморфизм их полей отношений: *поле $\Delta(\vartheta)$ — поле отношений кольца $\mathfrak{S}$ — изоморфно полю рациональных функций от одного неизвестного x .*

В первом случае, когда ϑ удовлетворяет алгебраическому уравнению $\varphi(\vartheta) = 0$ с коэффициентами из Δ , ϑ называется *алгебраическим относительно Δ* , а поле $\Delta(\vartheta)$ — *простым алгебраическим расширением* поля Δ ; во втором случае, когда из $f(\vartheta) = 0$ следует $f(x) = 0$, ϑ называется *трансцендентным относительно Δ* , а поле $\Delta(\vartheta)$ — *простым трансцендентным расширением* поля Δ . Согласно сказанному выше, с трансцендентной величиной можно оперировать как с неизвестной: $\Delta(\vartheta) \cong \Delta(x)$. Напротив, в случае алгебраической величины

$$\Delta(\vartheta) = \mathfrak{S} \cong \Delta[x]/(\varphi(x)),$$

где $\varphi(x)$ есть (неразложимый) полином наименьшей степени, имеющий корень ϑ .

Этим, в алгебраическом случае, обуславливаются следующие факты:

а) Каждая рациональная функция от ϑ может быть также записана в виде полинома $\sum a_k \vartheta^k$. (Действительно, $\mathfrak{S}$ было определено как совокупность таких полиномов.)

б) С этими полиномами можно оперировать как с классами вычетов по модулю $\varphi(x)$ в области полиномов $\Delta[x]$.

с) Равенство

$$f(\vartheta) = 0$$

может быть обращено в сравнение

$$f(x) \equiv 0 \pmod{\varphi(x)},$$

и обратно.

¹⁾ Вместо «неразложимый в $\Delta[x]$ » мы будем говорить также «неразложимый над полем Δ ».

Каждые два простых трансцендентных расширения поля Δ эквивалентны.

Действительно, соответствие $\frac{f(x)}{g(x)} \rightarrow \frac{f(\vartheta)}{g(\vartheta)}$ устанавливает эквивалентность каждого простого трансцендентного расширения $\Delta(\vartheta)$ с полем рациональных функций от неизвестного x .

Каждые два простых алгебраических расширения $\Delta(\alpha)$, $\Delta(\beta)$, где α и β — корни одного и того же неприводимого в $\Delta[x]$ полинома $\varphi[x]$, эквивалентны, причём существует изоморфизм, оставляющий все элементы поля Δ на месте и переводящий α в β .

Доказательство. Элементы поля $\Delta(\alpha)$ имеют вид $\sum_{k=0}^{n-1} a_k \alpha^k$, элементы поля $\Delta(\beta)$ — вид $\sum_{k=0}^{n-1} a_k \beta^k$. Операции и с теми, и с другими элементами производятся как с полиномами по модулю $\varphi(x)$. Следовательно, соответствие

$$\sum a_k \alpha^k \rightarrow \sum a_k \beta^k$$

и является изоморфизмом требуемого рода.

Полином $\varphi(x)$, неприводимый в поле Δ , может уже не быть неприводимым в расширении Ω этого поля. Если он имеет в Ω корень ϑ , то от него отщепляется по меньшей мере один линейный множитель $x - \vartheta$. Может случиться, что $\varphi(x)$ имеет над Ω ещё и другие линейные и нелинейные множители:

$$\varphi(x) = (x - \vartheta)(x - \vartheta_2) \dots (x - \vartheta_j) \varphi_1(x) \dots \varphi_k(x).$$

В этом случае, по доказанному, поля $\Delta(\vartheta)$, $\Delta(\vartheta_2), \dots, \Delta(\vartheta_j)$ все эквивалентны, и при изоморфизмах

$$\Delta(\vartheta) \cong \Delta(\vartheta_2) \cong \dots \cong \Delta(\vartheta_j)$$

ϑ переходит в $\vartheta_2, \dots, \vartheta_j$.

Эквивалентные расширения [такие, как $\Delta(\vartheta)$, $\Delta(\vartheta_2), \dots, \Delta(\vartheta_j)$], содержащиеся в одном общем надполе Ω , называют взаимно сопряжёнными (относительно поля Δ), а величины $\vartheta, \vartheta_2, \dots$, переходящие при соответственных изоморфизмах друг в друга, называют сопряжёнными величинами¹⁾. Из доказанного следует: все лежащие в Ω корни неприводимого в $\Delta[x]$ полинома $\varphi(x)$ являются взаимно сопряжёнными относительно поля Δ . И обратно, сопряжённые величины, в случае их алгебраичности, всегда являются корнями одного и того же неприводимого полинома $\varphi(x)$; действительно, если существует изоморфизм, оставляющий все элементы поля Δ на месте и переводящий ϑ_1 в ϑ_2 , то из $\varphi(\vartheta_1) = 0$ просто в силу этого изоморфизма следует, что и $\varphi(\vartheta_2) = 0$.

¹⁾ Эта терминология применяется главным образом к алгебраическим величинам ϑ . Величины трансцендентные (по отношению к одному и тому же полю) всегда являются взаимно сопряжёнными (см. выше).

Существование простых расширений. До сих пор Ω всюду предполагалось заданным надполем и исследовалось строение простых расширений $\Delta(\vartheta)$ внутри Ω . Теперь же мы поставим проблему иначе: задано поле Δ и разыскивается его расширение $\Delta(\vartheta)$, причём требуется, либо чтобы ϑ было трансцендентным, либо чтобы ϑ было корнем заданного полинома, неприводимого в $\Delta[x]$.

В случае трансцендентного ϑ проблема решается просто: в качестве ϑ берём неизвестное:

$$\vartheta = x,$$

образуем область полиномов $\Delta[x]$ и её поле отношений $\Delta(x)$, т. е. поле рациональных функций от неизвестного x . Как мы видели, $\Delta(x)$ есть, с точностью до эквивалентности, единственное простое трансцендентное расширение поля Δ .

Итак:

Существует, и притом с точностью до эквивалентных расширений, только одно, простое трансцендентное расширение $\Delta(\vartheta)$ заданного поля Δ .

Если же ϑ должно быть алгебраическим, а именно — корнем неприводимого в $\Delta[x]$ полинома $\varphi(x)$, то мы можем, прежде всего, принять, что φ не есть полином первой степени, так как иначе мы имели бы $\Delta(\vartheta) = \Delta$.

Искомое поле $\Delta(\vartheta)$ должно быть по предыдущему изоморфно полю классов вычетов

$$\Sigma' = \Delta[x]/(\varphi(x)).$$

Но, теперь, каждому полиному f из $\Delta[x]$ соответствует некоторый класс вычетов $\bar{f}$ в Σ' , и это отображение гомоморфно. В частности, каждой константе a из Δ соответствует некоторый класс вычетов $\bar{a}$, и это отображение поля Δ не только гомоморфно, но даже изоморфно, так как нуль является единственной константой, которая $\equiv 0 \pmod{\varphi(x)}$. Поэтому, в соответствии со сказанным в конце § 12, мы можем в поле Σ' заменить классы вычетов $\bar{a}$ соответствующими им элементами a из Δ . Тем самым Σ' перейдёт в поле Σ , содержащее Δ и изоморфное полю Σ' .

Класс вычетов, соответствующий полиному x , мы обозначим через ϑ , и построим в Σ поле $\Delta(\vartheta)$. (Впрочем, как легко видеть, $\Delta(\vartheta) = \Delta(\vartheta)$.) Из

$$\varphi(x) = \sum_0^n a_k x^k \equiv 0 \pmod{\varphi(x)}$$

следует в силу изоморфизма, что

$$\sum_0^n \bar{a}_k \vartheta^k = 0 \quad (\text{в } \Sigma'),$$

Важно
Замечание
то, что
 $\varphi(x)$ не
является
в $\Delta[x]$
а то,
то
 $\varphi(\vartheta) = 0$
не дано
до этого
доказано
и сейчас
видим
то, что
указано

откуда, заменяя $\bar{a}_k$ на a_k , получаем:

$$\varphi(\vartheta) = \sum_0^n a_k \vartheta^k = 0.$$

Таким образом, ϑ есть корень полинома $\varphi(x)$.

Тем самым доказано следующее предложение:

Для заданного поля Δ существует (и притом с точностью до эквивалентных расширений, — единственное) простое алгебраическое расширение $\Delta(\vartheta)$, обладающее тем свойством, что ϑ удовлетворяет наперед заданному неприводимому в $\Delta[x]$ уравнению $\varphi(x) = 0$.

Использованное при доказательстве «символическое присоединение» с помощью факторкольца и символа ϑ в некотором смысле противоположно несимволическому присоединению, возможному, когда в нашем распоряжении заранее находится объемлющее поле Ω , содержащее уже величину ϑ , обладающую требуемыми свойствами (см. начало этого параграфа). Если, например, Δ — поле рациональных чисел, то возможности несимволического присоединения алгебраических чисел, т. е. корней алгебраических уравнений с рациональными коэффициентами, можно достичь, отправляясь от построенного трансцендентным путём поля Ω комплексных чисел: действительно, согласно «основной теореме алгебры», в этом поле каждое уравнение с рациональными числовыми коэффициентами разрешимо. Изложенное выше символическое присоединение позволяет избежать этого трансцендентного обходного пути, вводя алгебраическое число непосредственно как символ некоторого класса вычетов и прямо определяя правила оперирования с ним. При этом не вводится никаких отношений порядка ($>$, $<$), либо других специальных свойств вещественных чисел. И тем не менее, и при символическом, и при трансцендентном несимволическом способе получается всегда (с алгебраической точки зрения) одно и то же поле $\Delta(\vartheta)$, так как, согласно доказанному выше, все возможные расширения $\Delta(\vartheta)$, в которых ϑ удовлетворяет одному и тому же неприводимому уравнению, эквивалентны. Действительно, как символическое, так и несимволическое присоединение подходят под общее понятие присоединения, данное в § 31; единственное различие состоит в том, что объемлющее поле Ω или Σ , наличие которого необходимо для того, чтобы присоединение возможно было осуществить, в одном случае считается уже заранее известным, а в другом — лишь строится.

Вопрос о связи между отношениями порядка $>$, $<$ и алгебраическими отношениями будет рассмотрен в главах 9 и 10.

Задача 5. Полином $x^4 + 1$ неприводим в поле Γ рациональных чисел (§ 24, задача 3). Присоединить один его корень ϑ и разложить указанный полином на простые множители в расширенном поле $\Gamma(\vartheta)$.

теоремы, а значит, и те же следствия из них, что и для понятия линейной зависимости.

Основных теорем — три. Первая из них совершенно очевидна.
Основная теорема 1. Каждое u_i ($i=1, \dots, n$) линейно зависит от $u_1, \dots, u_n$.

Основная теорема 2. Если v линейно зависит от $u_1, \dots, u_n$, но не от $u_1, \dots, u_{n-1}$, то u_n линейно зависит от $u_1, \dots, u_{n-1}$, v .
 Доказательство. В равенстве

$$\beta_0 v + \beta_1 u_1 + \dots + \beta_n u_n = 0 \quad (\beta_0 \neq 0)$$

β_n должно быть отлично от нуля, ибо иначе v линейно зависело бы уже от $u_1, \dots, u_{n-1}$.

Основная теорема 3. Если w линейно зависит от $v_1, \dots, v_s$, а каждое v_j ($j=1, \dots, s$) линейно зависит от $u_1, \dots, u_n$, то w линейно зависит от $u_1, \dots, u_n$.

Доказательство. Из $w = \sum_i \alpha_i v_i$ и $v_i = \sum_k \beta_{ik} u_k$ следует:

$$w = \sum_i \alpha_i \left(\sum_k \beta_{ik} u_k \right) = \sum_{i,k} \alpha_i \beta_{ik} u_k = \sum_k \left(\sum_i \alpha_i \beta_{ik} \right) u_k.$$

Из основных теорем 1 и 3 вытекает

Следствие 1. Если w линейно зависит от $v_1, \dots, v_s$, то w линейно зависит также от каждой системы $\{u_1, \dots, u_n\}$, содержащей $\{v_1, \dots, v_s\}$.

В частности, под это подходит и тот случай, когда $v_1, \dots, v_s$ с точностью до порядка нумерации совпадают с $u_1, \dots, u_n$. Таким образом, понятие линейной зависимости не зависит от порядка нумерации элементов $u_1, \dots, u_n$.

Определение. Элементы $u_1, \dots, u_n$ называются линейно независимыми, если ни один из них не зависит линейно от остальных.

Это означает, таким образом, что в каждом соотношении

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0$$

необходимо $\alpha_1 = 0, \dots, \alpha_n = 0$ (однако при выводе следствий мы не будем делать никакого употребления из этого пояснения смысла понятия линейной независимости). Понятие линейной независимости не зависит от порядка нумерации элементов $u_1, \dots, u_n$. Пустое множество всегда будет причисляться к линейно независимым. Отдельный элемент u линейно независим, если он не зависит линейно от пустого множества, т. е. если $u \neq 0$.

Следствие 2. Если $u_1, \dots, u_{n-1}$ линейно независимы, но $u_1, \dots, u_{n-1}, u_n$ уже не являются линейно независимыми, то u_n линейно зависит от $u_1, \dots, u_{n-1}$.

Доказательство. Один из элементов $u_1, \dots, u_{n-1}, u_n$ должен линейно зависеть от остальных. Если это u_n , то нечего дока-

зывать. Если же это, скажем, u_{n-1} , то u_{n-1} линейно зависит от $u_1, \dots, u_{n-2}, u_n$, но не от $u_1, \dots, u_{n-2}$, а тогда (основная теорема 2) u_n линейно зависит от $u_1, \dots, u_{n-2}, u_{n-1}$.

Следствие 3. *Каждая конечная система элементов $u_1, \dots, u_n$ содержит (возможно — и пустую) линейно независимую подсистему, от которой линейно зависят все u_i ($i = 1, \dots, n$).*

Доказательство. Выберем из рассматриваемой системы подсистему из наибольшего возможного числа линейно независимых элементов. Каждый содержащийся в этой подсистеме элемент u_i зависит от неё в силу основной теоремы 1, а каждый не содержащийся в ней — в силу следствия 2.

Определение. *Две конечные системы $u_1, \dots, u_n$ и $v_1, \dots, v_s$ называются (линейно) эквивалентными, если каждое v_k линейно зависит от $u_1, \dots, u_n$, и каждое u_i линейно зависит от $v_1, \dots, v_s$.*

Отношение эквивалентности по определению симметрично, по основной теореме 1 рефлексивно и по основной теореме 3 транзитивно. Если элемент w линейно зависит от одной из двух эквивалентных систем, то в силу основной теоремы 3 он линейно зависит также от другой. Согласно следствию 3 каждая конечная система эквивалентна некоторой линейно независимой подсистеме.

Следствие 4 (теорема о замене). *Если $v_1, \dots, v_s$ линейно независимы и каждое v_j линейно зависит от $u_1, \dots, u_n$, то в системе $\{u_1, \dots, u_n\}$ существует подсистема $\{u_{i_1}, \dots, u_{i_s}\}$ из s элементов, которую можно заменить на $\{v_1, \dots, v_s\}$ так, что система, которая получится из $\{u_1, \dots, u_n\}$ после этой замены, будет эквивалентна первоначальной системе $\{u_1, \dots, u_n\}$. Таким образом, в частности, $s \leq n$.*

Доказательство. Для $s = 0$ утверждение тривиально: нет никаких v_j и ничто не заменяется. Пусть, таким образом, утверждение уже доказано для $\{v_1, \dots, v_{s-1}\}$ и пусть системой $\{v_1, \dots, v_{s-1}\}$ заменена система $\{u_{i_1}, \dots, u_{i_{s-1}}\}$. При этой замене $\{u_1, \dots, u_n\}$ переходит в эквивалентную систему $\{v_1, \dots, v_{s-1}, u_k, u_{i_s}, \dots\}$. Но v_s линейно зависит от $\{u_1, \dots, u_n\}$, а значит, также от эквивалентной ей системы $\{v_1, \dots, v_{s-1}, u_k, u_{i_s}, \dots\}$. Таким образом, существует и наименьшая подсистема системы $\{v_1, \dots, v_{s-1}, u_k, u_{i_s}, \dots\}$, от которой ещё линейно зависит v_s . Эта наименьшая подсистема не может состоять из одних лишь v_j , так как все v_j и v_s линейно независимы. Таким образом она содержит по крайней мере одно u_k ; пусть это будет $u_k = u_{i_s}$. По основной теореме 2 элемент $u_k = u_{i_s}$ линейно зависит от системы, получающейся из указанной наименьшей подсистемы $\{v_j, \dots, u_k\}$ путём замены u_k на v_s , а значит, и от обобщающей её системы $\{v_1, \dots, v_{s-1}, v_s, u_{i_s}, \dots\}$, получающейся из $\{v_1, \dots, v_{s-1}, u_k, u_{i_s}, \dots\}$ при подстановке $u_k \rightarrow v_s$. Эта система $\{v_1, \dots, v_{s-1}, v_s, u_{i_s}, \dots\}$ эквивалентна системе $\{v_1, \dots, v_{s-1}, u_k, u_{i_s}, \dots\}$, так как u_k линейно зависит от первой из этих систем, а v_s — от

второй. Тем самым мы продвинули замену ещё на один шаг. Новая система $\{v_1, \dots, v_{s-1}, v_s, u_1, \dots\}$, будучи эквивалентной системе $\{v_1, \dots, v_{s-1}, u_k, u_l, \dots\}$, эквивалентна также первоначальной системе $\{u_1, \dots, u_n\}$. *(в силу транзитивности)*

Следствие 5. Две эквивалентные линейно независимые системы $\{u_1, \dots, u_r\}$ и $\{v_1, \dots, v_s\}$ состоят из одинакового числа элементов.

Доказательство. Согласно следствию 4 имеем: $s \leq r$ и $r \leq s$.

Определение. Говорят, что множество $\mathcal{M}$ элементов из $\mathfrak{A}$ — конечного ранга над телом Δ или, короче, конечно над Δ , если все элементы этого множества линейно зависят от конечного числа из них.

Так, например, простое алгебраическое расширение $\Delta(\vartheta)$ конечно над Δ , ибо все элементы из $\Delta(\vartheta)$, согласно § 32, линейно выражаются через $1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}$. Разумеется, вообще каждая алгебра с конечным базисом над Δ имеет конечный ранг.

Согласно следствию 3, из конечного числа элементов, от которых линейно зависят все элементы множества $\mathcal{M}$, можно выбрать эквивалентную линейно независимую подсистему $\{u_1, \dots, u_r\}$. Такая линейно независимая подсистема, от которой линейно зависят все элементы множества $\mathcal{M}$, называется базисом, точнее, Δ -базисом¹⁾ (а также «минимальным базисом» или «линейно независимым базисом») множества $\mathcal{M}$.

В линейном выражении

$$(1) \quad u = \alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_r u_r$$

элемента множества $\mathcal{M}$ через элементы базиса коэффициенты $\alpha_1, \dots, \alpha_r$ однозначно определены. Действительно, из

$$\alpha_1 u_1 + \dots + \alpha_r u_r = \beta_1 u_1 + \dots + \beta_r u_r$$

следует

$$\sum_i (\alpha_i - \beta_i) u_i = 0$$

и, значит, в силу линейной независимости,

$$\alpha_i - \beta_i = 0.$$

Обратно, из однозначности представления (1) следует линейная независимость элементов базиса.

Согласно следствию 5, число элементов в каждом базисе множества $\mathcal{M}$ одно и то же. Это число называют линейным рангом множества $\mathcal{M}$ над телом Δ и обозначают символом $(\mathcal{M} : \Delta)$. В случае, когда $\mathcal{M}$ есть векторное пространство, линейный ранг $(\mathcal{M} : \Delta)$ называется также размерностью пространства $\mathcal{M}$.

¹⁾ Понятие Δ -базиса не следует смешивать с понятием базиса идеала (§ 16). Оба они представляют собой частные случаи более общего понятия базиса модуля (относительно некоторой системы операторов).

Если r — линейный ранг множества $\mathcal{M}$, то, согласно следствию 4, для каждой линейно независимой системы $v_1, \dots, v_s$ в $\mathcal{M}$ имеет место неравенство $s \leq r$. Таким образом, линейный ранг r можно охарактеризовать также как максимальное число линейно независимых элементов данного множества. Отсюда вытекает:

Следствие 6. Подмножество $\mathcal{N}$ множества $\mathcal{M}$, конечного над Δ , также конечно над Δ , причём линейный ранг подмножества $\mathcal{N}$ не превышает линейного ранга множества $\mathcal{M}$.

Задача 1. Если r — ранг множества $\mathcal{M}$, то каждые r линейно независимых элементов этого множества образуют его базис.

Задача 2. Если $\mathcal{M}$ имеет конечный ранг, то каждый базис подмножества $\mathcal{N}$ множества $\mathcal{M}$ может быть расширен до базиса всего множества $\mathcal{M}$.

Задача 3. Из $\mathcal{Q} \cong \Delta$ и $(\mathcal{Q} : \Delta) = 1$ следует $\mathcal{Q} = \Delta$.

Применим теперь понятие линейного ранга, в частности, к расширениям тела Δ , конечным над Δ , т. е., как будем говорить дальше, к конечным расширениям тела Δ . В коммутативном случае линейный ранг $(\Sigma : \Delta)$ будет большей частью называться степенью поля Σ над Δ . Если степень равна 2, 3, 4, то рассматриваемое расширение называют соответственно квадратичным, кубическим, би-квадратичным. Простое алгебраическое расширение $\Sigma = \Delta(\vartheta)$, порождённое алгебраическим элементом ϑ степени n , является конечным степени n , так как его базис образуют линейно независимые степени $1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}$.

Пусть Σ — тело, заключённое между Δ и $\mathcal{Q}$, т. е. $\Delta \subseteq \Sigma \subseteq \mathcal{Q}$. Тогда имеет место следующая

Теорема. Если $\mathcal{Q}$ конечно над Δ , то также Σ конечно над Δ и $\mathcal{Q}$ конечно над Σ . И обратно, если Σ конечно над Δ и $\mathcal{Q}$ конечно над Σ , то $\mathcal{Q}$ конечно над Δ . При этом имеет место соотношение

$$(2) \quad (\mathcal{Q} : \Delta) = (\mathcal{Q} : \Sigma)(\Sigma : \Delta).$$

Доказательство. Если $\mathcal{Q}$ конечно над Δ , то, в силу следствия 6, Σ также конечно над Δ . То, что $\mathcal{Q}$ конечно над Σ , — ясно, так как $\mathcal{Q}$ конечно даже над Δ . Пусть теперь, обратно, $(\Sigma : \Delta)$ и $(\mathcal{Q} : \Sigma)$ конечны и пусть $\{u_1, \dots, u_r\}$ есть базис Σ относительно Δ и точно так же $\{v_1, \dots, v_s\}$ — базис $\mathcal{Q}$ относительно Σ . Тогда каждый элемент w из $\mathcal{Q}$ может быть представлен в виде

$$\begin{aligned} w &= \sum_i \sigma_i v_i \quad (\sigma_i \in \Sigma) \\ &= \sum_i \left(\sum_k \delta_{ik} u_k \right) v_i \quad (\delta_{ik} \in \Delta) \\ &= \sum_i \sum_k \delta_{ik} (u_k v_i). \end{aligned}$$

Таким образом, каждый элемент из Ω линейно зависит от rs величин $u_k v_i$. Но эти величины линейно независимы относительно Δ . Действительно, из равенства

$$\sum_i \sum_k \delta_{ik} u_k v_i = 0 \quad (\delta_{ik} \in \Delta)$$

в силу линейной независимости величин v относительно Σ следует, что

$$\sum_k \delta_{ik} u_k = 0,$$

а тогда из линейной независимости величин u относительно Δ следует, что

$$\delta_{ik} = 0.$$

Таким образом, rs есть линейный ранг Ω над Δ , что и требовалось доказать.

Следствия из соотношения (2):

а) Если $\Delta \subseteq \Sigma \subseteq \Omega$ и $(\Omega: \Delta) = (\Sigma: \Delta)$, то $\Omega = \Sigma$. Действительно, в этом случае из (2) вытекает, что $(\Omega: \Sigma) = 1$. *и задача 3.*

Аналогичным образом:

б) Если $\Delta \subseteq \Sigma \subseteq \Omega$ и $(\Omega: \Sigma) = (\Omega: \Delta)$, то $\Sigma = \Delta$. *Также*

Далее:

с) Если $\Delta \subseteq \Sigma \subseteq \Omega$, то степень $(\Sigma: \Delta)$ является делителем степени $(\Omega: \Delta)$.

Задача 4. Какова степень поля $\Gamma(i, \sqrt{2})$ над полем Γ рациональных чисел?

Задача 5. Все элементы конечного коммутативного расширения Ω поля Δ алгебраичны относительно Δ , и их степени суть делители степени $(\Omega: \Delta)$ поля Ω над Δ . *аа*

Задача 6. Каково число элементов поля характеристики p , имеющего степень n над содержащимся в нём простым полем? *(pp)*

§. 34. Линейные уравнения над телом.

Важной областью применения теории линейной зависимости является теория решения систем линейных уравнений.

Пусть $l_1, \dots, l_m$ — линейные формы от неизвестных $x_1, \dots, x_n$ с коэффициентами из некоторого тела Δ :

$$(1) \quad l_i = \sum a_{ik} x_k.$$

Пусть, далее, $\beta_1, \dots, \beta_m$ — заданные элементы из Δ . Найдём (в Δ) все решения $(\zeta_1, \dots, \zeta_n)$ системы уравнений

$$(2) \quad l_i(\zeta) = \sum a_{ik} \zeta_k = \beta_i \quad (i = 1, 2, \dots, m).$$

Число r линейно-независимых среди форм $l_1, \dots, l_m$ называется рангом системы (2). Мы будем предполагать нумерацию линейных

либо любой ~~выбрав~~ $l_1, \dots, l_r$ $l_1, \dots, l_r = l_1, \dots, l_r$

*90/11
Этот
слог
ср-сав*

форм l_i выбранной так, что $l_1, \dots, l_r$ линейно независимы, а остальные l_i линейно зависят от них:

$$(3) \quad l_i = \sum_1^r e_{ik} l_k \quad (i = r+1, \dots, m).$$

Соотношения (3) остаются верными и после подстановки вместо входящих в формы l_i неизвестных x_j элементов ζ_j . Теперь, для того чтобы система уравнений (2) была разрешима, необходимо, чтобы полученные соотношения (3) оставались верными также после замены l_i на β_i :

$$(4) \quad \beta_i = \sum_1^r e_{ik} \beta_k \quad (i = r+1, \dots, m).$$

Если эти условия выполнены, то уравнения (2) являются все следствиями первых r из них. Таким образом, остаётся рассмотреть ещё лишь эти r независимых уравнений.

Линейные формы $l_1, \dots, l_r$ линейно зависят от неизвестных $x_1, \dots, x_n$. Следовательно, по теореме о замене (§ 33, следствие 4) можно r из этих неизвестных, скажем (при должной нумерации) $x_1, \dots, x_r$, заменить на $l_1, \dots, l_r$, так что новая система $\{l_1, \dots, l_r, x_{r+1}, \dots, x_n\}$ будет эквивалентна системе $\{x_1, \dots, x_n\}$. Это означает, что все неизвестные x линейно зависят от $l_1, \dots, l_r, x_{r+1}, \dots, x_n$:

$$(5) \quad x_i = \sum_1^r \gamma_{ij} l_j + \sum_{r+1}^n \delta_{ik} x_k \quad (i = 1, \dots, r).$$

И эти соотношения должны сохранять силу после подстановки ζ_i вместо x_i и β_j вместо l_j :

$$(6) \quad \zeta_i = \sum_1^r \gamma_{ij} \beta_j + \sum_{r+1}^n \delta_{ik} \zeta_k \quad (i = 1, \dots, r).$$

Таким образом, r неизвестных $\zeta_1, \dots, \zeta_r$ можно линейно выразить через остальные $\zeta_{r+1}, \dots, \zeta_n$.

Пока что мы установили лишь необходимые условия, которым должны удовлетворять все решения предложенной системы линейных уравнений. Мы утверждаем теперь, что эти необходимые условия также достаточны:

Если условия (4) выполнены, то система уравнений (2) разрешима, причём решения находятся по формуле (6), в которой элементы $\zeta_{r+1}, \dots, \zeta_n$ могут быть выбраны произвольно.

Доказательство. Так как система $\{l_1, \dots, l_r, x_{r+1}, \dots, x_n\}$ эквивалентна $\{x_1, \dots, x_n\}$, то она имеет ранг n , и так как она состоит точно из n элементов, то эти элементы линейно независимы. Таким образом, подставляя (3) и (5) в (1), мы получим тождество относительно $l_1, \dots, l_r, x_{r+1}, \dots, x_n$, которое остаётся в силе и

§ 35. Алгебраические расширения полей.

Расширение Σ поля Δ называется *алгебраическим над Δ* , если каждый элемент поля Σ алгебраичен над Δ .

Теорема. Каждое конечное расширение Σ поля Δ является алгебраическим над Δ и может быть получено путём присоединения к Δ конечного числа алгебраических элементов.

Доказательство. Пусть n — степень конечного расширения Σ и α — произвольный элемент из Σ . Тогда среди степеней $1, \alpha, \alpha^2, \dots, \alpha^n$ имеется не более n линейно независимых. Следовательно,

должно иметь место соотношение вида $\sum_{k=0}^n c_k \alpha^k = 0$ с коэффициентами c_k из Δ , которые не все равны нулю, т. е. α должно быть алгебраическим над Δ . Тем самым и поле Σ является алгебраическим над Δ . В качестве множества, присоединение которого порождает расширение Σ , можно выбрать базис поля Σ .

Основываясь на этой теореме, можно вместо «конечное расширение» говорить также «конечное алгебраическое расширение».

Обратная теорема. Каждое расширение поля Δ , получающееся путём присоединения к Δ конечного числа величин, алгебраических над Δ , является конечным (и, следовательно, алгебраическим).

Доказательство. Присоединение алгебраической величины θ степени n даёт конечное расширение с базисом $1, \theta, \dots, \theta^{n-1}$. Последовательное образование конечного числа конечных расширений, в силу последней теоремы § 33, даёт всегда снова конечное расширение.

Следствие. *Сумма, разность, произведение и частное алгебраических величин суть снова алгебраические величины.*

Теорема. *Если элемент α алгебраичен над Σ , а Σ алгебраично над Δ , то α алгебраичен над Δ .*

Доказательство. В алгебраическое уравнение для α с коэффициентами из Σ входит в качестве коэффициентов лишь конечное число элементов $\beta, \gamma, \dots$ из Σ . Поле $\Sigma' = \Delta(\beta, \gamma, \dots)$ конечно над Δ , а поле $\Sigma'(\alpha)$, в свою очередь, конечно над Σ' ; следовательно, $\Sigma'(\alpha)$ конечно также над Δ , и, значит, α алгебраичен над Δ .

Поля разложения. Среди конечных алгебраических расширений, особенно важны «поля разложения» полинома $f(x)$, получаемые путём «присоединения всех корней уравнения $f(x) = 0$ ». Под этим понимают такое поле $\Delta(\alpha_1, \dots, \alpha_n)$, в котором заданный полином $f(x)$ из $\Delta[x]$ полностью распадается на линейные множители ¹⁾:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n),$$

¹⁾ Здесь и в дальнейшем старший коэффициент полинома $f(x)$ будет приниматься равным 1, что, очевидно, не нарушает общности рассуждений.

причём оно получается путём присоединения к Δ корней α_i этих линейных множителей. Относительно этих полей имеют место следующие теоремы:

Для каждого полинома $f(x)$ из $\Delta[x]$ существует поле разложения.

Доказательство. Пусть

$$f(x) = \varphi_1(x) \varphi_2(x) \dots \varphi_r(x)$$

— разложение полинома $f(x)$ на множители, неразложимые далее в $\Delta[x]$. Присоединив сначала корень α_1 неприводимого полинома $\varphi_1(x)$, мы получим поле $\Delta(\alpha_1)$, над которым от $\varphi_1(x)$, а значит, и от $f(x)$ отделится линейный множитель $x - \alpha_1$. Пусть теперь уже построено поле $\Delta_k = \Delta(\alpha_1, \dots, \alpha_k)$ ($k < n$), над которым от полинома $f(x)$ отделяются (различные или одинаковые) линейные множители $x - \alpha_1, \dots, x - \alpha_k$, так что $f(x)$ обладает в поле Δ_k следующим разложением:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_k) \cdot \psi_{k+1}(x) \dots \psi_l(x).$$

Присоединим теперь к Δ_k корень α_{k+1} полинома $\psi_{k+1}(x)$. В расширенном таким образом поле $\Delta_k(\alpha_{k+1}) = \Delta(\alpha_1, \dots, \alpha_{k+1})$ от $f(x)$ отделятся линейные множители $x - \alpha_1, \dots, x - \alpha_{k+1}$ (а возможно, и другие).

Продолжая так шаг за шагом, мы придём, наконец, к искомому полю $\Delta_n = \Delta(\alpha_1, \dots, \alpha_n)$.

Покажем теперь, далее, что поле разложения заданного полинома $f(x)$, с точностью до эквивалентных расширений, определено однозначно. При этом нам понадобится понятие *продолжения изоморфизма*.

Пусть $\Delta \subseteq \Sigma$ и $\bar{\Delta} \subseteq \bar{\Sigma}$, и пусть задан изоморфизм $\Delta \cong \bar{\Delta}$. Изоморфизм $\Sigma \cong \bar{\Sigma}$ называется *продолжением* заданного изоморфизма $\Delta \cong \bar{\Delta}$, если каждый элемент a из Δ , имеющий при старом изоморфизме $\Delta \cong \bar{\Delta}$ образ $\bar{a}$, имеет и при новом изоморфизме $\Sigma \cong \bar{\Sigma}$ тот же самый образ $\bar{a}$ из $\bar{\Delta}$.

Все теоремы о продолжениях изоморфизмов при алгебраических расширениях основываются на следующем предложении:

Если при изоморфизме $\Delta \cong \bar{\Delta}$ неприводимый полином $\varphi(x)$ из $\Delta[x]$ переходит в полином $\bar{\varphi}(x)$ из $\bar{\Delta}[x]$ (разумеется, снова неприводимый), и если, далее, α есть корень полинома $\varphi(x)$ в некотором расширении поля Δ , $\bar{\alpha}$ — корень полинома $\bar{\varphi}(x)$ в некотором расширении поля $\bar{\Delta}$, то заданный изоморфизм $\Delta \cong \bar{\Delta}$ может быть продолжен до изоморфизма $\Delta(\alpha) \cong \bar{\Delta}(\bar{\alpha})$, переводящего α в $\bar{\alpha}$.

Доказательство. Элементы поля $\Delta(\alpha)$ имеют вид $\sum c_k \alpha^k$ ($c_k \in \Delta$) и подчиняются правилам действий с полиномами по модулю $\varphi(x)$. Аналогично, элементы поля $\bar{\Delta}(\bar{\alpha})$ имеют вид $\sum \bar{c}_k \bar{\alpha}^k$ ($\bar{c}_k \in \bar{\Delta}$) и подчиняются правилам действий с полиномами по модулю $\bar{\varphi}(x)$, т. е. тем же точно правилам. Следовательно, соответствие

$$\sum c_k \alpha^k \rightarrow \sum \bar{c}_k \bar{\alpha}^k$$

(где $\bar{c}_k$ — элементы, соответствующие элементам c_k при изоморфизме $\Delta \cong \bar{\Delta}$) есть изоморфизм, обладающий требуемыми свойствами.

Если, в частности, $\Delta = \bar{\Delta}$ и заданным изоморфизмом является отображение каждого элемента из Δ на себя, то мы вновь приходим к доказанной ранее теореме, по которой все расширения $\Delta(\alpha)$, $\Delta(\bar{\alpha})$, ..., получающиеся путём присоединения корня одного и того же неприводимого уравнения, эквивалентны, причём каждый корень может быть переведён путём соответствующего изоморфизма в любой другой.

Оказывается, что соответствующая теорема верна и в случае присоединения всех корней полинома вместо одного:

Если при изоморфизме $\Delta \cong \bar{\Delta}$ произвольный полином $f(x)$ из $\Delta[x]$ переходит в полином $\bar{f}(x)$ из $\bar{\Delta}[x]$, то этот изоморфизм может быть продолжён до изоморфизма произвольного поля разложения $\Delta(\alpha_1, \dots, \alpha_n)$ полинома $f(x)$ с произвольным полем разложения $\bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$ полинома $\bar{f}(x)$, переводящего $\alpha_1, \dots, \alpha_n$ в некотором порядке в $\bar{\alpha}_1, \dots, \bar{\alpha}_n$.

Доказательство. Пусть изоморфизм $\Delta \cong \bar{\Delta}$ уже продолжен (возможно, с изменением нумерации корней) до изоморфизма $\Delta(\alpha_1, \dots, \alpha_k) \cong \bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_k)$, причём каждое α_i переходит в $\bar{\alpha}_i$. (Для $k=0$ это действительно имеет место.) Пусть

$$f(x) = (x - \alpha_1) \dots (x - \alpha_k) \cdot \varphi_{k+1}(x) \dots \varphi_h(x)$$

— разложение $f(x)$ в $\Delta(\alpha_1, \dots, \alpha_k)$. Тогда, в силу изоморфизма, $\bar{f}(x)$ обладает в $\bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_k)$ соответствующим разложением

$$\bar{f}(x) = (x - \bar{\alpha}_1) \dots (x - \bar{\alpha}_k) \cdot \bar{\varphi}_{k+1}(x) \dots \bar{\varphi}_h(x).$$

В $\Delta(\alpha_1, \dots, \alpha_n)$ и $\bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$ множители φ_i и $\bar{\varphi}_i$ разлагаются далее в произведения $(x - \alpha_{k+1}) \dots (x - \alpha_n)$ и $(x - \bar{\alpha}_{k+1}) \dots (x - \bar{\alpha}_n)$. Элементы $\alpha_{k+1}, \dots, \alpha_n$ и $\bar{\alpha}_{k+1}, \dots, \bar{\alpha}_n$ можно считать занумерованными так, что α_{k+1} есть корень полинома $\varphi_{k+1}(x)$ и $\bar{\alpha}_{k+1}$ — корень полинома $\bar{\varphi}_{k+1}(x)$. Тогда, по предыдущей теореме, изоморфизм

$$\Delta(\alpha_1, \dots, \alpha_k) \cong \bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_k)$$

может быть продолжен до изоморфизма

$$\Delta(\alpha_1, \dots, \alpha_{k+1}) \cong \bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_{k+1}),$$

переводящего α_{k+1} в $\bar{\alpha}_{k+1}$.

Продвигаясь так шаг за шагом, начиная от $k=0$, мы придём, наконец, к искомому изоморфизму

$$\Delta(\alpha_1, \dots, \alpha_n) \cong \bar{\Delta}(\bar{\alpha}_1, \dots, \bar{\alpha}_n),$$

причём по построению каждое α_i переходит в $\bar{\alpha}_i$.

Если, в частности, $\Delta = \bar{\Delta}$ и заданный изоморфизм $\Delta \cong \Delta$ оставляет каждый элемент из Δ на месте, то $\bar{f} = f$ и продолженный изоморфизм

$$\Delta(\alpha_1, \dots, \alpha_n) \cong \Delta(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$$

также оставляет все элементы из Δ на месте, т. е. оба поля разложения полинома $f(x)$ эквивалентны. Тем самым поле разложения полинома $f(x)$, с точностью до эквивалентных расширений, однозначно определено.

Отсюда следует, что алгебраические свойства корней не зависят от способа построения поля разложения. Например, будем ли мы разлагать полином в поле комплексных чисел или же путём символического присоединения, мы всегда придём по существу, т. е. с точностью до эквивалентности, к одному и тому же результату.

В частности, каждый корень полинома $f(x)$ имеет определённую кратность, с которой он входит в разложение

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n).$$

Кратные корни полином $f(x)$ имеет тогда и только тогда, если $f(x)$ и $f'(x)$ обладают над полем разложения общим делителем, не являющимся константой (§ 21). На наибольший общий делитель полиномов $f(x)$ и $f'(x)$ над произвольным расширением поля Δ — тот же, что и наибольший общий делитель в $\Delta[x]$ (§ 18, задача 1). Поэтому уже нахождение наибольшего общего делителя полинома $f(x)$ и его производной $f'(x)$ в $\Delta[x]$ позволяет узнать, обладает ли $f(x)$ в своём поле разложения кратными корнями.

Два поля разложения одного и того же полинома, содержащиеся в общем объемлющем поле Ω , не только эквивалентны, но даже просто совпадают. Действительно, если в Ω имеют место два разложения:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n),$$

$$f(x) = (x - \bar{\alpha}_1) \dots (x - \bar{\alpha}_n),$$

то по теореме об однозначной разложимости в $\Omega[x]$ множители этих разложений будут с точностью до нумерации одни и те же.

Нормальные расширения. Расширение Σ поля Δ называется нормальным расширением или расширением Галуа над Δ , если, во-первых, оно является алгебраическим над Δ и, во-вторых, каждый неприводимый в $\Delta[x]$ полином $g(x)$, имеющий в Σ один корень α , полностью распадается в $\Sigma[x]$ на линейные множители¹⁾.

Построенные нами выше поля разложения нормальны, как показывает следующая теорема:

Поле, получающееся путём присоединения к Δ всех корней одного, или нескольких, или даже бесконечного множества полиномов из $\Delta[x]$, нормально.

Прежде всего, случай бесконечного множества полиномов можно свести к случаю конечного множества. Действительно, каждый отдельный элемент α этого поля зависит всё же лишь от корней конечного числа рассматриваемых полиномов, и мы можем при разложении неприводимого полинома, имеющего α своим корнем, вполне ограничиться полем, порождённым этим конечным множеством корней.

Затем случай конечного числа полиномов можно свести к случаю одного единственного полинома, перемножив все эти полиномы и присоединив корни полученного произведения, ибо это всё равно, что присоединить корни всех сомножителей.

Пусть, таким образом, $\Sigma = \Delta(\alpha_1, \dots, \alpha_n)$, где α_i — корни некоторого полинома $f(x)$, и пусть неприводимый полином $g(x)$ из $\Delta[x]$ имеет корень β в Σ . Если $g(x)$ не распадается полностью в Σ , то мы можем расширить Σ до поля $\Sigma(\beta')$, где β' — не содержащийся в Σ корень полинома $g(x)$. Тогда, так как β и β' сопряжены, имеем:

$$\Delta(\beta) \cong \Delta(\beta'),$$

причём величины из Δ , и в частности коэффициенты полинома $f(x)$, переходят в себя. Присоединяя теперь слева и справа все корни полинома $f(x)$, мы можем этот изоморфизм продолжить:

$$\Delta(\beta, \alpha_1, \dots, \alpha_n) \cong \Delta(\beta', \alpha_1, \dots, \alpha_n).$$

¹⁾ Это определение можно высказать также в следующей форме: алгебраическое расширение Σ нормально, если Σ вместе с величиной α содержит также все сопряжённые с α величины (из любого объемлющего поля). Действительно, сопряжённые с α величины произвольного объемлющего поля являются не чем иным, как корнями того же неприводимого полинома $g(x)$, корнем которого служит α , а объемлющее поле можно всегда выбрать так, чтобы в нём $g(x)$ полностью разлагался на линейные множители. Однако мы предпочли обойтись без этого определения, так как оно опирается на понятие совокупности всех объемлющих полей, что (отвлекаясь от рискованности этого понятия с теоретико-множественной точки зрения, что можно было бы устранить) представляется излишне сложным, поскольку в действительности речь идёт о некотором свойстве одних лишь полей Σ и Δ .

причём α_i будут переходить снова в α_j , но, быть может, в другом порядке. Но β есть рациональная функция от $\alpha_1, \dots, \alpha_n$ с коэффициентами из Δ :

$$\beta = r(\alpha_1, \dots, \alpha_n),$$

и это рациональное соотношение сохраняется при любом изоморфизме. Тем самым и β' есть рациональная функция от $\alpha_1, \dots, \alpha_n$, а значит, точно так же принадлежит полю Σ , в противоречие с нашим предположением.

Обратная теорема. Всякое нормальное расширение Σ поля Δ может быть получено путём присоединения к Δ всех корней некоторого множества полиномов, а если Σ конечно над Δ , — то даже путём присоединения всех корней одного полинома.

Доказательство. Пусть поле Σ получено путём присоединения к Δ некоторого множества $\mathcal{M}$ алгебраических величин. (В общем случае можно, например, принять $\mathcal{M} = \Sigma$; если Σ конечно, то и $\mathcal{M}$ можно взять конечным.) Каждый элемент из $\mathcal{M}$ удовлетворяет некоторому алгебраическому уравнению $f(x) = 0$ с коэффициентами из Δ , полностью распадающемуся в Σ . Присоединение всех корней всех этих полиномов $f(x)$ (а если этих полиномов — лишь конечное число, то всех корней их произведения) даёт не меньше, а в силу нормальности поля Σ — и не больше, чем присоединение одного множества $\mathcal{M}$, т. е. всё поле Σ , что и требовалось доказать.

Неприводимое уравнение $f(x) = 0$ называется *нормальным* (или *уравнением Галуа*), если присоединение уже одного его корня даёт нормальное поле, иными словами, если $f(x)$ полностью распадается в этом поле.

Резольвентой Галуа уравнения $f(x) = 0$ называется неприводимое уравнение $g(x) = 0$, обладающее тем свойством, что присоединение одного корня этого уравнения даёт уже полное поле разложения полинома $f(x)$. Существование таких резольвент будет доказано позже (§ 40).

Задача 1. Если $\Delta \subseteq \Sigma \subseteq \Omega$ и Ω есть поле Галуа над Δ , то Σ есть поле Галуа и над Δ .

Задача 2. Построить поле разложения полинома $x^3 - 2$, принимая поле Γ рациональных чисел за основное. Показать, что если α — корень этого полинома, то $\Gamma(\alpha)$ не является нормальным полем.

Задача 3. Если $f(x)$ неприводим в поле K , то в любом нормальном расширении поля K $f(x)$ разлагается на множители одинаковой степени, сопряжённые относительно K .

Задача 4. Каждое поле, квадратичное над Δ , является нормальным над Δ .

§ 36. Корни из единицы.

В предыдущих параграфах были изложены общие основы теории полей. Прежде чем перейти к дальнейшему развёртыванию общей теории, мы применим полученные теоремы к некоторым совсем специальным уравнениям и полям.

Пусть Π — простое поле и h — натуральное число, не делящееся на характеристику поля Π . (Таким образом, если характеристика равна нулю, то h может быть любым натуральным числом.) Под корнем h -той степени из единицы понимают корень полинома

$$f(x) = x^h - 1$$

в некотором коммутативном расширении поля Π .

Корни h -той степени из единицы образуют по умножению абелеву группу.

Действительно, если $\alpha^h = 1$ и $\beta^h = 1$, то также и $\left(\frac{\alpha}{\beta}\right)^h = 1$, откуда и следует групповое свойство. Коммутативность группы очевидна.

Порядок произвольного элемента α этой группы является делителем числа h , ибо должно выполняться равенство $\alpha^h = 1$.

Поле разложения Σ полинома $f(x) = x^h - 1$ называется полем корней h -той степени из единицы над простым полем Π . Линейные множители, на которые распадается полином $f(x)$, все различны; действительно, так как h не делится на характеристику, то производная

$$f'(x) = hx^{h-1}$$

обращается в нуль лишь при $x = 0$ и, значит, не имеет с $f(x)$ ни одного общего корня. Таким образом, в Σ существует точно h корней h -той степени из единицы.

Разложим теперь h на простые множители:

$$h = \prod_{i=1}^m q_i^{v_i}.$$

В группе корней h -той степени из единицы имеется не более $\frac{h}{q_i}$ элементов a , для которых $a^{\frac{h}{q_i}} = 1$, поскольку полином $x^{\frac{h}{q_i}} - 1$ имеет не более $\frac{h}{q_i}$ корней. Таким образом, в указанной группе существует элемент a_i такой, что

$$a_i^{\frac{h}{q_i}} \neq 1.$$

Элемент

$$b_i = a_i^{\frac{h}{q_i^{v_i}}}$$

имеет тогда порядок $q_i^{v_i}$. Действительно, возведение его в степень $q_i^{v_i}$ даёт 1, и потому порядок его является делителем числа $q_i^{v_i}$, но результат возведения его в степень $q_i^{v_i-1}$ отличен от 1, и, значит, его порядок не может быть собственным делителем числа $q_i^{v_i}$. Произведение

$$\zeta = \prod_1^m b_i$$

имеет теперь, как произведение элементов с взаимно простыми порядками $q_1^{v_1}, \dots, q_m^{v_m}$, в точности порядок

$$\prod_1^m q_i^{v_i} = h$$

(§ 7, задача 1). Такой корень h -той степени из единицы, порядок которого равен в точности h , называют *первообразным корнем h -той степени из единицы*.

Степени 1, ζ , $\zeta^2, \dots, \zeta^{h-1}$ первообразного корня h -той степени из единицы все различны; а так как вся группа этих корней содержит лишь h элементов, то все её элементы суть степени первообразного корня ζ . Тем самым мы получили следующий результат:

Группа корней h -той степени из единицы циклична и порождается любым первообразным корнем h -той степени из единицы ζ .

Число первообразных корней h -той степени из единицы, которое мы обозначим через $\varphi(h)$, легко определить. $\varphi(h)$ есть число элементов порядка h в циклической группе порядка h^1). Пусть сначала h есть степень простого числа, $h = q^v$; тогда из q^v степеней первообразного корня ζ все, за вычетом q^{v-1} степеней элемента ζ^q , имеют порядок h ; тем самым

$$(1) \quad \varphi(q^v) = q^v - q^{v-1} = q^{v-1}(q - 1) = q^{v-1}\left(1 - \frac{1}{q}\right).$$

Пусть теперь h разложимо на два взаимно простых множителя: $h = rs$. Тогда каждый элемент h -того порядка однозначно представим в виде произведения элемента r -того порядка и элемента s -того порядка (§ 18, задача 3), и обратно, каждое такое произведение есть элемент h -того порядка. Но элементы r -того порядка принад-

1) Согласно задаче 4 § 18, $\varphi(h)$ есть вместе с тем число натуральных чисел, взаимно простых с h и не превосходящих h . $\varphi(h)$ называют *эulerовой функцией*.

лежат к циклической группе r -того порядка, порождённой степенью ζ^s ; их число равно поэтому $\varphi(r)$. Точно так же, число элементов s -того порядка равно $\varphi(s)$. Следовательно, для числа указанных произведений получаем равенство

$$\varphi(h) = \varphi(r) \varphi(s).$$

Повторное применение этой формулы к разложению

$$h = \prod_1^m q_i^{v_i}$$

числа h на степени простых чисел даёт:

$$\varphi(h) = \varphi(q_1^{v_1} q_2^{v_2} \dots q_m^{v_m}) = \varphi(q_1^{v_1}) \varphi(q_2^{v_2}) \dots \varphi(q_m^{v_m}),$$

откуда, в силу равенства (1),

$$\begin{aligned} \varphi(h) &= q_1^{v_1-1} (q_1 - 1) q_2^{v_2-1} (q_2 - 1) \dots q_m^{v_m-1} (q_m - 1) = \\ &= h \left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) \dots \left(1 - \frac{1}{q_m}\right). \end{aligned}$$

Итак, мы получили, что число первообразных корней h -той степени из единицы равно

$$\varphi(h) = h \prod_1^m \left(1 - \frac{1}{q_i}\right).$$

Положим $\varphi(h) = n$. Пусть первообразные корни h -той степени из единицы будут $\zeta_1, \dots, \zeta_n$. Они служат корнями полинома

$$(x - \zeta_1)(x - \zeta_2) \dots (x - \zeta_n) = \Phi_h(x).$$

Имеет место равенство

$$(2) \quad x^h - 1 = \prod_{d|h} \Phi_d(x),$$

где d пробегает все положительные делители числа h ¹⁾. Действительно, каждый корень h -той степени из единицы является первообразным корнем d -той степени из единицы для одного и только одного положительного делителя d числа h , и потому каждый линейный множитель полинома $x^h - 1$ входит в один и только один полином $\Phi_d(x)$.

$\Phi_h(x)$ однозначно определяется формулой (2). Действительно, из неё прежде всего следует

$$\Phi_1(x) = x - 1,$$

а если Φ_d уже известны для всех положительных $d < h$, то Φ_h находится делением из (2).

¹⁾ $a|b$ означает (и читается): a делит b .

Так как эти деления, согласно алгоритму, можно производить, не выходя из области целочисленных полиномов, то получаем следующий результат:

Каждое $\Phi_h(x)$ является целочисленным полиномом и не зависит от характеристики поля Π (в предположении, что h не делится на эту характеристику).

Полиномы $\Phi_h(x)$ называют, по причинам, которые выяснятся позже, *полиномами деления круга*. Можно указать для них явные рациональные выражения, содержащие «мёбиусовскую функцию» $\mu(n)$, определяемую следующим образом:

$$\mu(n) = \begin{cases} 0, & \text{если } p_i^2 | n \text{ для какого-либо } p_i, \\ (-1)^\lambda, & \text{если } n = p_1 p_2 \dots p_\lambda \text{ (т. е. } n \text{ «свободно от квадратов»)}, \\ 1, & \text{если } n = 1 \end{cases}$$

($p_1, \dots, p_\lambda$ означают здесь различные простые множители числа n). Мёбиусовская функция обладает следующим важным свойством:

$$\sum_{d|h} \mu(d) = \begin{cases} 1 & \text{при } h = 1, \\ 0 & \text{при } h > 1. \end{cases}$$

Для его доказательства можно поступить следующим образом.

Если $h = q_1^{a_1} \dots q_m^{a_m}$, то развернём произведение $\prod_{i=1}^m (1 - z_i)$ и затем положим в нём все z_i равными 1. Члены

$$(-1)^\lambda z_{i_1} z_{i_2} \dots z_{i_\lambda}$$

этого произведения будут соответствовать как раз свободным от квадратов делителям $d = q_{i_1} q_{i_2} \dots q_{i_\lambda}$ числа h , причём

$$(-1)^\lambda = \mu(d).$$

Таким образом, положив все $z_i = 1$, мы получим при $m > 0$ (т. е. $h > 1$):

$$0 = \prod_{i=1}^m (1 - 1) = \sum_{d|h} \mu(d),$$

тогда как при $h = 1$, очевидно, $\sum_{d|h} \mu(d) = 1$.

Мы утверждаем теперь:

Полиномы деления круга могут быть заданы формулой

$$(3) \quad \Phi_h(x) = \prod_{d|h} (x^d - 1)^{\mu\left(\frac{h}{d}\right)}.$$

Для доказательства достаточно показать, что выражение, стоящее в правой части, удовлетворяет уравнению (2), т. е. что

$$x^h - 1 = \prod_{d|h} \prod_{d'|d} (x^{d'} - 1)^{\mu\left(\frac{d}{d'}\right)}.$$

Но каждое фиксированное $x^{d'} - 1$ входит в это произведение с показателями $\mu\left(\frac{d}{d'}\right)$, где d пробегает все делители числа h , являющиеся одновременно кратными числа d' , т. е. с показателями $\mu(\lambda)$, где λ пробегает все делители числа $\frac{h}{d'}$. Сумма этих показателей, по ранее доказанному, вообще равна нулю, за исключением случая $\frac{h}{d'} = 1$, когда эта сумма сводится к одному слагаемому, равному единице. Таким образом, из всего двойного произведения, стоящего в правой части, остаётся лишь один множитель $x^h - 1$, имеющий притом показателем 1. Тем самым уравнение (2) действительно удовлетворяется функциями (3).

Примеры:

$$\begin{aligned}\Phi_{12}(x) &= (x^{12} - 1)^{+1} (x^6 - 1)^{-1} (x^4 - 1)^{-1} (x^2 - 1)^{+1} = \\ &= (x^6 + 1)^{+1} (x^2 + 1)^{-1} = x^4 - x^2 + 1;\end{aligned}$$

$$\begin{aligned}\Phi_{q^v}(x) &= (x^{q^v} - 1)^{+1} (x^{q^{v-1}} - 1)^{-1} = \\ &= 1 + x^{q^{v-1}} + x^{2q^{v-1}} + \dots + x^{(q-1)q^{v-1}}\end{aligned}$$

для каждого простого q .

Полином $\Phi_h(x)$, вообще говоря, может быть приводимым; так, например, для поля характеристики 11

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 - 5x + 1)(x^2 + 5x + 1).$$

Но позже (в § 53) мы увидим, что в простом поле характеристики нуль полиномы $\Phi_h(x)$ неприводимы, и тем самым все первообразные корни h -той степени из единицы сопряжены. В § 24 справедливость этого была обнаружена с помощью теоремы Эйзенштейна для всех простых чисел h ; для $\Phi_8 = x^4 + 1$ и $\Phi_{12} = x^4 - x^2 + 1$ тот же результат составлял содержание задачи 3 § 24 и задачи 5 § 23.

Часто оказывается полезной следующая теорема:

Если ζ — корень h -той степени из единицы, то

$$1 + \zeta + \zeta^2 + \dots + \zeta^{h-1} = \begin{cases} h & (\zeta = 1), \\ 0 & (\zeta \neq 1). \end{cases}$$

Доказательство получается непосредственно из формулы для суммы геометрической прогрессии: при $\zeta \neq 1$ имеем

$$\frac{1 - \zeta^h}{1 - \zeta} = 0.$$

Задача 1. Поле корней h -той степени из единицы при нечётном h является одновременно полем корней $2h$ -той степени из единицы.

Задача 2. Поля корней третьей и четвёртой степеней из единицы над полем рациональных чисел квадратичны. Выразить эти корни из единицы с помощью квадратных корней.

Задача 3. Поле корней восьмой степени из единицы квадратично относительно поля гауссовских чисел $\Gamma(i)$. Выразить первообразный корень восьмой степени из единицы с помощью квадратного корня из элемента поля $\Gamma(i)$.

Задача 4. В случае поля характеристики p корни степени p^h из единицы являются одновременно корнями степени h из единицы. (Этим оправдывается сделанное с самого начала ограничение $h \neq 0(p)$.)

Задача 5. «Уравнение деления круга» $\Phi_h(x) = 0$ всегда нормально.

§ 37. Поля Галуа (конечные поля).

Мы уже встречались на примере простых полей характеристик p с полями, состоящими из конечного числа элементов. Конечные поля в честь открывшего их Галуа называются *полями Галуа*. Исследуем сначала их общие свойства.

Пусть Δ — поле Галуа и q — число его элементов.

Характеристика поля Δ не может быть равна нулю, так как в противном случае уже простое поле Π , лежащее в Δ , содержало бы бесконечное множество элементов. Пусть характеристикой будет p . Простое поле Π изоморфно тогда факторкольцу кольца целых чисел по модулю p и содержит, таким образом, p элементов.

Так как в Δ всего имеется лишь конечное число элементов, то в Δ существует также максимальная система линейно независимых относительно Π элементов $\alpha_1, \dots, \alpha_n$. n есть степень $(\Delta : \Pi)$ поля Δ относительно Π , и каждый элемент из Δ имеет вид

$$(1) \quad c_1 \alpha_1 + \dots + c_n \alpha_n$$

с однозначно определёнными коэффициентами c_i из Π .

Каждый из коэффициентов c_i может принимать p значений; таким образом, существует всего ровно p^n выражений вида (1). Так как ими исчерпывается вся совокупность элементов поля, то заключаем, что

$$q = p^n.$$

Тем самым доказано, что число элементов поля Галуа Δ является степенью характеристики p ; показатель этой степени равен степени $(\Delta : \Pi)$ поля Δ над содержащимся в нём простым полем Π .

Совокупность всех элементов любого тела, отличных от нуля, образует мультипликативную группу. В случае поля Галуа с q элементами это — абелева группа порядка $q - 1$. Порядок любого её элемента α должен быть делителем числа $q - 1$, откуда

$$\alpha^{q-1} = 1 \text{ для каждого } \alpha \neq 0.$$

Вытекающее отсюда равенство

$$\alpha^q - \alpha = 0$$

выполняется также для $\alpha = 0$. Таким образом, все элементы поля являются корнями полинома $x^q - x$. Если $\alpha_1, \dots, \alpha_q$ — все элементы поля, то $x^q - x$ должно делиться на

$$\prod_{i=1}^q (x - \alpha_i),$$

откуда, вследствие равенства степеней и старших коэффициентов,

$$x^q - x = \prod_{i=1}^q (x - \alpha_i).$$

Тем самым Δ получается путём присоединения к Π всех корней одного единственного полинома $x^q - x$. Но этим поле Δ , с точностью до изоморфизма, однозначно определено (§ 35). Таким образом:

При заданных p и n все поля, имеющие p^n элементов, изоморфны.

Мы покажем теперь, что для каждого $n > 0$ и каждого простого p действительно существует поле, имеющее $q = p^n$ элементов.

Для этого, положив в основу простое поле Π характеристики p , построим над ним поле, в котором $x^q - x$ полностью распадается на линейные множители. Рассмотрим в этом поле множество всех корней полинома $x^q - x$. Это множество является полем. Действительно, из $x^{p^n} = x$ и $y^{p^n} = y$ следует, согласно задаче 1 § 30, что

$$(x - y)^{p^n} = x^{p^n} - y^{p^n} = x - y$$

и в случае $y \neq 0$ также

$$\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}} = \frac{x}{y};$$

тем самым разность и отношение двух корней полинома $x^q - x$ снова суть корни этого полинома.

Полином $x^q - x$ не имеет кратных корней, так как его производная $qx^{q-1} - 1$, в силу соотношения $q \equiv 0 (p)$, равна -1 и, значит, никогда не обращается в нуль. Таким образом, множество корней полинома $x^q - x$ есть поле из q элементов.

Тем самым доказано следующее предложение:

Для каждой степени простого числа $q = p^n$ ($n > 0$) существует, и притом с точностью до изоморфизма только одно, поле Галуа, состоящее из q элементов. Элементами этого поля служат корни полинома $x^q - x$.

Поле Галуа, состоящее из p^n элементов, будет в дальнейшем обозначаться символом $GF(p^n)$.

*Этот шаг
нужен для
ссылки на
предложение 1.*

$a^{p^k} = a$ посыл 5.1
 для всех $a \in A$ тогда
 в случае $k=1$ [гл. V]

степени этого автоморфизма переводят a в $a^p, a^{p^2}, \dots, a^{p^m} = a$.
 Тем самым мы уже нашли m автоморфизмов.

В § 38 мы увидим, что больше чем m автоморфизмов существовать не может. Таким образом, найденные только что m автоморфизмов $a \rightarrow a^{p^i}$ являются единственными.

Теоремы, доказанные для полей $GF(p^n)$, дают в применении к случаю $n=1$ и факторкольцу $C/(p)$ известные теоремы элементарной теории чисел, а именно:

1. Число корней сравнения по простому модулю p не превышает степени сравнения. $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$ т.к. $C/(p)$ поле, $a_i \in C/(p)$ и $a_i \not\equiv 0 \pmod{p}$ (иначе f делится на x).
2. Теорема Ферма: $a^{p-1} \equiv 1 \pmod{p}$ при $a \not\equiv 0 \pmod{p}$.

представляет собой частный случай теоремы

$$a^{p^n-1} \equiv 1 \pmod{p} \text{ при } a \not\equiv 0 \pmod{p}.$$

имеющей место для $GF(p^n)$.

3. Существует «первообразный корень по модулю p », т. е. число ζ такое, что каждое b , взаимно простое с p , сравнимо с некоторой степенью ζ по модулю p . (Иными словами: группа классов вычетов по модулю p , отличных от нулевого класса, циклическа.)

4. Произведение всех элементов $a_1, a_2, \dots, a_h$ поля $GF(p^n)$, отличных от нуля, равно -1 , как это следует из равенства

$$x^h - 1 = \prod_{i=1}^h (x - a_i).$$

При $n=1$ это даёт «теорему Вильсона»:

$$(p-1)! \equiv -1 \pmod{p}.$$

Задача 1. Если элемент a поля $GF(p^n)$ является корнем неприводимого в $\Pi[x]$ полинома $f(x)$ степени m , то

$$a^p, a^{p^2}, \dots, a^{p^m} = a$$

представляет собой совокупность всех корней этого полинома (т. е. всех сопряжённых с a величин).

Задача 2. Если r взаимно просто с $p^n - 1$, то каждый элемент из $GF(p^n)$ является r -той степенью. Если r — делитель числа $p^n - 1$, то r -тыми степенями являются те и только те из элементов a поля $GF(p^n)$, которые удовлетворяют уравнению

$$\frac{a^{p^n-1}-1}{a^r-1} = 1.$$

Указать теоретико-числовую специализацию (« r -тые степенные вычеты»).

Задача 3. Если простой идеал $\mathfrak{p}$ коммутативного кольца $\mathfrak{o}$ обладает лишь конечным числом классов вычетов, то $\mathfrak{o}/\mathfrak{p}$ есть поле Галуа.

Задача 4. Исследовать, в частности, факторкольца по простым идеалам $(1+i)$, (3) , $(2+i)$, (7) в кольце целых гауссовских чисел.

Задача 5. Указать неприводимое в $GF(3)$ уравнение для первообразного корня восьмой степени из единицы из $GF(9)$ и, аналогично, неприводимое в $GF(2)$ уравнение для первообразного корня седьмой степени из $GF(8)$.

Задача 6. Для каждой пары значений p и m существуют целочисленные полиномы $f(x)$ степени m , неприводимые по модулю p . Все они являются по модулю p делителями полинома $x^{p^m} - x$.

Интересное свойство полей Галуа доказал С. Chevalley: *Abh. math. Sem. Hamburg*, 11 (1936), 73—75.

§ 38. Сепарабельные и несепарабельные расширения.

Пусть Δ — некоторое поле.

Поставим вопрос: может ли полином, неприводимый в $\Delta[x]$, иметь кратные корни в некотором расширении поля Δ ?

Для того чтобы полином $f(x)$ имел кратные корни, $f(x)$ и $f'(x)$ должны обладать общим множителем, не являющимся константой, причём этот множитель можно тогда, согласно § 18, вычислить, не выходя за пределы кольца $\Delta[x]$. Но если $f(x)$ неприводим, то ни с одним полиномом нижней степени он не может иметь общего множителя, не являющегося константой. Таким образом для неприводимого полинома $f(x)$, имеющего кратные корни, должно выполняться условие $f'(x) = 0$.

Пусть

$$f(x) = \sum_0^n a_v x^v$$

и, значит,

$$f'(x) = \sum_1^n v a_v x^{v-1}.$$

Для того чтобы было $f'(x) = 0$, каждый коэффициент полинома $f'(x)$ должен быть равен нулю:

$$v a_v = 0 \quad (v = 1, 2, \dots).$$

В случае, когда характеристика поля Δ равна нулю, отсюда следует, что $a_v = 0$ для всех $v \neq 0$. Таким образом, в этом случае никакой полином, не являющийся константой, не может иметь кратных корней. Но в случае поля характеристики p равенство $v a_v = 0$ возможно и при $a_v \neq 0$; однако тогда должно быть

$$v \equiv 0 \pmod{p}.$$

Таким образом, для того чтобы полином $f(x)$ имел кратные корни все его члены, за исключением членов $a_v x^v$ с $v \equiv 0 \pmod{p}$, должны обращаться в нуль, т. е. этот полином должен иметь вид

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$$

И обратно, если $f(x)$ имеет указанный вид, то $f'(x) = 0$. В этом случае можно записать $f(x)$ в форме

$$f(x) = \varphi(x^p).$$

Итак, мы доказали следующее предложение:

Для поля Δ характеристики нуль неприводимый в $\Delta[x]$ полином $f(x)$ имеет лишь простые корни; для поля характеристики p неприводимый полином $f(x)$ (не являющийся константой) имеет кратные корни тогда и только тогда, когда он может быть записан в виде функции от x^p .

В последнем случае $\varphi(x)$, в свою очередь, может оказаться функцией от x^p . Тогда $f(x)$ есть функция от x^{p^2} . Пусть, вообще, $f(x)$ есть функция от x^{p^e} :

$$f(x) = \psi(x^{p^e}),$$

но уже не является функцией от $x^{p^{e+1}}$. Разумеется, полином $\psi(y)$ тогда неприводим. Далее, $\psi'(y) \neq 0$, так как иначе мы имели бы $\psi(y) = \chi(y^p)$ и, значит, $f(x) = \chi(x^{p^{e+1}})$, в противоречие с предположением. Таким образом, $\psi(y)$ имеет уже только простые корни.

Разложим $\psi(y)$ в некотором расширении поля Δ на линейные множители ¹⁾:

$$\psi(y) = \prod_{i=1}^{n_0} (y - \beta_i).$$

Тогда

$$f(x) = \prod_{i=1}^{n_0} (x^{p^e} - \beta_i).$$

Пусть α_i — какой-нибудь корень множителя $x^{p^e} - \beta_i$. Тогда

$$\alpha_i^{p^e} = \beta_i,$$

$$x^{p^e} - \beta_i = x^{p^e} - \alpha_i^{p^e} = (x - \alpha_i)^{p^e}.$$

Тем самым α_i является корнем множителя $x^{p^e} - \beta_i$, имеющим кратность p^e , и

$$f(x) = \prod_{i=1}^{n_0} (x - \alpha_i)^{p^e}.$$

¹⁾ Старший коэффициент в $\psi(y)$ можно без ограничения общности положить равным 1; n_0 есть степень полинома $\psi(y)$.

Таким образом, все корни полинома $f(x)$ имеют одну и ту же кратность p^e .

Степень n_0 полинома φ называется *приведённой степенью* полинома $f(x)$ (как и его корней α_i); e называется *показателем* полинома $f(x)$ (как и корней α_i) относительно поля Δ . Степень, приведённая степень и показатель связаны соотношением

$$n = n_0 p^e.$$

n_0 есть, вместе с тем, число различных корней полинома $f(x)$.

Элемент ϑ , являющийся корнем неприводимого в $\Delta[x]$ полинома, имеющего лишь различные (простые) корни, называется *сепарабельным* или элементом *первого рода*¹⁾ относительно Δ . Сепарабельным называется и сам неприводимый полином $f(x)$, все корни которого сепарабельны. В противоположном случае алгебраический элемент ϑ и неприводимый полином $f(x)$ называются *несепарабельными* или элементом, соответственно полиномом, *второго рода*. Наконец, алгебраическое надполе Σ , все элементы которого сепарабельны относительно Δ , называется *сепарабельным* относительно Δ , а каждое алгебраическое надполе, не обладающее этим свойством, — *несепарабельным*.

В случае поля характеристики нуль каждый неприводимый полином (а тем самым и, каждое алгебраическое расширение) является, по предыдущему, сепарабельным; в случае же поля характеристики p сепарабельными являются лишь полиномы с показателем $e = 0$ (т. е. с приведённой степенью $n_0 = n$). В случае поля характеристики p неприводимый полином $\varphi(x)$, не являющийся константой, несепарабелен тогда и только тогда, если он может быть записан в виде полинома от x^p .

Ниже мы увидим, что наиболее важные и интересные расширения полей в большинстве своём сепарабельны и что существует обширный класс полей, не допускающих вообще никаких несепарабельных расширений (так называемые «совершенные поля»). Поэтому в дальнейшем всё связанное специально с несепарабельными расширениями мы будем помещать мелким шрифтом.

Рассмотрим теперь алгебраическое поле $\Sigma = \Delta(\vartheta)$. Мы видели, что степень n определяющего уравнения $f(x) = 0$ даёт одновременно степень поля $(\Sigma : \Delta)$. Оказывается, что приведённая степень n_0 даёт одновременно *число изоморфизмов* поля Σ , в следующем точном смысле: рассматриваются лишь такие изоморфизмы $\Sigma \cong \Sigma'$, которые оставляют на месте все элементы подполя Δ , переводя тем самым Σ в эквивалентные поля Σ' («относительные изоморфизмы Σ над Δ »), и притом лишь такие из них, при которых образ Σ' содержится

¹⁾ Термин «первого рода» принадлежит Штейнцу. Я предпочитаю слово «сепарабельный», как подчёркивающее то обстоятельство, что среди корней полинома $f(x)$ нет совпавших.

вместе с Σ в подходяще выбранном надполе Ω . А именно, имеет место следующая теорема:

При надлежащем выборе надполя Ω поле $\Sigma = \Delta(\vartheta)$ допускает ровно n_0 относительных изоморфизмов, и ни при каком выборе надполя Ω — более чем n_0 таких изоморфизмов.

Доказательство. Каждый относительный изоморфизм должен переводить ϑ в сопряжённую величину ϑ' из Ω [в корень того же неприводимого уравнения $f(x) = 0$]. Если теперь мы выберем Ω так, чтобы $f(x)$ целиком распадался в Ω на линейные множители, то ϑ действительно будет иметь n_0 сопряжённых $\vartheta, \vartheta', \dots$ и поля $\Delta(\vartheta), \Delta(\vartheta'), \dots$ действительно будут сопряжены или эквивалентны. При этом, как бы мы ни выбирали Ω , ϑ не сможет иметь больше чем n_0 сопряжённых элементов. Остается заметить, что относительный изоморфизм $\Delta(\vartheta) \cong \Delta(\vartheta')$ вполне определяется заданием соответствия $\vartheta \rightarrow \vartheta'$. Действительно, если ϑ переходит в ϑ' , а все величины из Δ остаются на месте, то каждый полином

$$\sum a_k \vartheta^k \quad (a_k \in \Delta)$$

переходит в

$$\sum a_k \vartheta'^k,$$

а это и определяет изоморфизм.

Если, в частности, ϑ сепарабельно, то $n_0 = n$, и тем самым число относительных изоморфизмов равно степени поля.

В дальнейшем, говоря об (относительных) изоморфизмах поля $\Sigma = \Delta(\vartheta)$, об элементах, сопряжённых с ϑ , или о полях, сопряжённых с Σ (относительно Δ), мы будем всегда иметь в виду изоморфизмы, соответственно сопряжённость, в некотором надлежаще выбранном надполе Ω , в качестве которого всегда можно, как выше, взять поле разложения полинома $f(x)$, т. е. наименьшее нормальное над Δ поле, содержащее поле Σ .

Если в нашем распоряжении имеется некоторое определённое надполе Ω , в котором каждый полином $f(x)$ полностью распадается на линейные множители (как это имеет, например, место в поле комплексных чисел), то в качестве Ω можно раз навсегда выбрать это определённое надполе Ω и соответственно этому во всех высказываниях относительно изоморфизмов опускать добавление «в Ω ». Так всегда поступают, например, в теории числовых полей. В § 62 будет показано, что и для абстрактных полей всегда можно разыскать такое поле Ω .

Задача 1. Если Π — поле характеристики p и x — неизвестное, то уравнение $z^p - x = 0$ неприводимо в $\Pi(x)[z]$, и определяемое этим уравнением поле $\Pi(x^{\frac{1}{p}})$ несепарабельно относительно $\Pi(x)$.

Задача 2. Принимая поле Γ рациональных чисел за основное, построить относительные изоморфизмы для:

а) поля корней пятой степени из единицы,

б) поля $\Gamma(\sqrt[3]{2})$.

Задача 3. Если $\vartheta^{p^e} = \gamma$ лежит в Δ , тогда как $\vartheta^{p^{e-1}}$ ещё не лежит в Δ , то полином $x^{p^e} - \gamma$ неприводим в $\Delta[x]$.

Установленная выше теорема допускает следующее обобщение:

Если надполе Σ получено из Δ путём последовательного присоединения m алгебраических величин $\alpha_1, \dots, \alpha_m$ и если каждое α_i является корнем неприводимого в $\Delta(\alpha_1, \dots, \alpha_{i-1})$ уравнения приведённой степени n_i' , то

Σ имеет в некотором надлежаще выбранном надполе Ω точно $\prod_1^m n_i'$ относительноных изоморфизмов над Δ , и ни в каком надполе не обладает больше чем $\prod_1^m n_i'$ такими изоморфизмами.

Доказательство. Для случая $m=1$ эта теорема была доказана выше. Предположим, таким образом, что её справедливость уже установлена для $\Sigma_1 = \Delta(\alpha_1, \dots, \alpha_{m-1})$, т. е. что в некотором Ω_1 существует точно

$\prod_1^{m-1} n_i'$ относительноных изоморфизмов поля Σ_1 , а большего их числа ни в каком надполе не существует. Пусть $\Sigma_1 \rightarrow \bar{\Sigma}_1$ — один из этих $\prod_1^{m-1} n_i'$ изо-

морфизмов. Мы утверждаем теперь, что этот изоморфизм может быть продолжен в некотором Ω до относительноных изоморфизмов $\Sigma = \Sigma_1(\alpha_m) \cong \bar{\Sigma} = \bar{\Sigma}_1(\bar{\alpha}_m)$ ровно n_m' способами, и ни в каком Ω нельзя этого сделать большим числом способов.

Элемент α_m удовлетворяет в Σ_1 уравнению $f_1(x) = 0$, имеющему в точности n_m' различных корней. Пусть при изоморфизме $\Sigma_1 \rightarrow \bar{\Sigma}_1$ $f_1(x)$ переходит в $\bar{f}_1(x)$. Тогда $\bar{f}_1(x)$ имеет в некотором надлежаще выбранном расширении поля $\bar{\Sigma}_1$ снова n_m' различных корней и ни в каком расширении не имеет большего числа различных корней. Выбрав один из этих корней $\bar{\alpha}_m$, мы можем продолжить изоморфизм $\Sigma_1 \cong \bar{\Sigma}_1$ до изоморфизма $\Sigma_1(\alpha_m) \cong \bar{\Sigma}_1(\bar{\alpha}_m)$, переводящего α_m в $\bar{\alpha}_m$ одним и только одним способом, а именно, по формуле

$$\sum c_k \alpha_m^k \rightarrow \sum \bar{c}_k \bar{\alpha}_m^k.$$

Так как выбор корня $\bar{\alpha}_m$ можно произвести n_m' способами, то для каждого выбранного изоморфизма $\Sigma_1 \rightarrow \bar{\Sigma}_1$ существует n_m' таких продолжений.

А так как изоморфизм $\Sigma_1 \rightarrow \bar{\Sigma}_1$, в свою очередь, может быть выбран $\prod_1^{m-1} n_i'$ способами, то всего существует (в таком надполе Ω , в котором целиком распадаются все рассматриваемые уравнения)

$$\prod_1^{m-1} n_i' \cdot n_m' = \prod_1^m n_i'$$

относительных изоморфизмов для Σ , и ни в каком надполе — не больше, что и требовалось доказать.

Если n_i — полная (не приведённая) степень элемента α_i относительно поля $\Delta(\alpha_1, \dots, \alpha_{i-1})$, то n_i есть одновременно степень поля $\Delta(\alpha_1, \dots, \alpha_i)$ от-

носителем $\Delta(\alpha_1, \dots, \alpha_{i-1})$; тем самым степень $(\Sigma: \Delta)$ поля Σ над Δ равна

$\prod_{i=1}^m n_i$. Сравнивая это число с числом изоморфизмов $\prod_{i=1}^m n_i'$, заключаем:

Число относительных изоморфизмов конечного расширения $\Sigma = \Delta(\alpha_1, \dots, \alpha_m)$ над Δ (в надлежаще выбранном расширении Ω) тогда и только тогда равно степени поля $(\Sigma: \Delta)$, когда каждое α_i сепарабельно относительно соответствующего $\Delta(\alpha_1, \dots, \alpha_{i-1})$. Если же хотя бы одно α_i не сепарабельно, то число изоморфизмов меньше степени поля.

Из этой теоремы тотчас же вытекает ряд важных следствий. Прежде всего, ею устанавливается, что сепарабельность каждого α_i относительно предыдущего поля выражает свойство поля Σ , независимое от выбора образующих α_i . Так как любой элемент β из поля может быть взят в качестве первой образующей, то заключаем, что каждый элемент β из поля Σ сепарабелен, раз только сепарабелы в указанном смысле все α_i . Итак:

Если последовательно присоединять к Δ элементы $\alpha_1, \dots, \alpha_m$ каждый из которых сепарабелен относительно поля, полученного путём присоединения предыдущих элементов, то получающаяся в итоге поле

$$\Sigma = \Delta(\alpha_1, \dots, \alpha_m)$$

сепарабельно относительно Δ .

В частности: сумма, разность, произведение и частное сепарабельных элементов сепарабельны.

Далее: если β сепарабельно относительно Σ и Σ сепарабельно относительно Δ , то β сепарабельно относительно Δ . Действительно, β удовлетворяет некоторому уравнению с конечным числом коэффициентов $\alpha_1, \dots, \alpha_m$ из Σ и, таким образом, сепарабельно относительно $\Delta(\alpha_1, \dots, \alpha_m)$. Потому и

$$\Delta(\alpha_1, \dots, \alpha_m, \beta)$$

сепарабельно.

Наконец, получаем, что число относительных изоморфизмов сепарабельного конечного расширения Σ поля Δ равно степени поля $(\Sigma: \Delta)$.

Так как, по предыдущему, все рациональные операции, будучи применены к сепарабельным элементам, дают снова сепарабельные элементы, то в любом надполе Ω поля Δ сепарабельные величины уже сами образуют некоторое поле Ω_0 . Это поле Ω_0 можно также охарактеризовать, как наибольшее сепарабельное расширение поля Δ , лежащее в Ω .

Если Ω алгебраично над Δ (но не обязательно сепарабельно), то результат возведения каждого элемента α из Ω в степень p^e , где e — показатель этого элемента, лежит в Ω_0 . Действительно, из изложенного в начале этого параграфа непосредственно следует, что α^{p^e} удовлетворяет уравнению, все корни которого различны. Таким образом:

Ω получается из Ω_0 уже путём извлечения одних лишь корней степеней p^e .

Если, в частности, Ω конечно над Δ , то показатели e , очевидно, ограничены. Наибольший из них — мы будем обозначать его снова через e — называется показателем поля Ω . Степень поля Ω_0 называется приведённой степенью поля Ω .

Разумеется, извлечение корней степени p^e может быть достигнуто также путём последовательного извлечения корней степени p . При извлечении корня p -той степени, не содержащегося до тех пор в поле (т. е. при присоединении корня неприводимого уравнения $x^p - \beta = 0$), степень поля умножается на p . Таким образом, если переход от Ω_0 к Ω производится путём f -кратного извлечения корня p -той степени, получаем:

$$(\Omega: \Delta) = (\Omega_0: \Delta) \cdot p^f,$$

или

степень = приведённой степени $\cdot p^f$,

как при простых несепарабельных расширениях.

Особенно просто оперирование с корнями степени p^e . Если α — корень степени p^e из β , то, как мы уже видели,

$$x^{p^e} - \beta = x^{p^e} - \alpha^{p^e} = (x - \alpha)^{p^e};$$

следовательно корень p^e -той степени из β в каждом поле, где он вообще существует, однозначно определён. Далее,

$$\sqrt[p^e]{\alpha + \beta} = \sqrt[p^e]{\alpha} + \sqrt[p^e]{\beta},$$

$$\sqrt[p^e]{\alpha\beta} = \sqrt[p^e]{\alpha}\sqrt[p^e]{\beta},$$

в чём можно убедиться возвышением в степень p^e .

Задача 4. Числа e и f , определённые для конечного несепарабельного расширения указанным выше образом, связаны неравенством $e \leq f$. При простом расширении $e = f$. Указать пример, когда $e < f$. [Присоединение корней p -той степени из двух или большего числа неизвестных.]

• § 39. Совершенные и несовершенные поля. Корневое поле.

Поле Δ называется совершенным, если каждый неприводимый в $\Delta[x]$ полином является сепарабельным. Поля, не обладающие этим свойством, называются несовершенными.

Следующие две теоремы устанавливают, когда поле является совершенным.

I. Поле характеристики нуль — всегда совершенное.

Доказательство. См. § 38. *стр 159*

II. Поле характеристики p является совершенным тогда и только тогда, когда в этом поле вместе с каждым элементом существует его корень p -той степени.

Доказательство. Если в поле для каждого элемента существует корень p -той степени, то каждый полином $f(x)$, содержащий лишь степени от x^p , является p -той степенью, так как

$$f(x) = \sum_k a_k (x^p)^k = \left\{ \sum_k \sqrt[p]{a_k} x^k \right\}^p = Y^p(x)$$

Таким образом, каждый неприводимый полином в этом случае сепарабелен, т. е. поле — совершенное.

С другой стороны, если в поле существует элемент α , не являющийся p -той степенью, то рассмотрим полином

$$f(x) = x^p - \alpha.$$

Пусть $\varphi(x)$ — неразложимый множитель этого полинома. После присоединения корня $\sqrt[p]{\alpha} = \beta$, $f(x)$ распадается на равные линейные множители $x - \beta$, следовательно, $\varphi(x)$, как делитель полинома $f(x)$,

тоже является степенью разности $x - \beta$. Если бы $\varphi(x)$ был линейным, т. е. $\varphi(x) = x - \beta$, то β принадлежало бы к полю Δ , что, однако, противоречит предположению. Тем самым $\varphi(x) = (x - \beta)^k$, где $k > 1$, т. е. $\varphi(x)$ есть несепарабельный неприводимый полином над Δ и, следовательно, Δ — несовершенное поле. Впрочем, степень полинома $\varphi(x)$, согласно § 38, должна делиться на p , значит, в данном случае равна p , т. е. $\varphi(x) = f(x)$.

Из II и одной теоремы, доказанной в § 37, непосредственно следует, что все поля Галуа — совершенные.

В алгебраически замкнутом поле (определение см. в § 62) каждый неприводимый полином является линейным. Тем самым все алгебраически замкнутые поля — совершенные.

Из определения совершенных полей непосредственно вытекают следующие две теоремы:

Каждое алгебраическое расширение совершенного поля сепарабельно относительно этого поля.

Каждое несовершенное поле допускает несепарабельные расширения.

А именно, эти несепарабельные расширения получаются путём присоединения произвольного корня несепарабельного неприводимого полинома.

Сделанное при доказательстве теоремы II замечание, что в совершенном поле характеристики p каждый полином $f(x)$, зависящий лишь от x^p , является p -той степенью, сохраняет силу, как видно из его доказательства, также для тех полиномов от нескольких неизвестных $f(x, y, z, \dots)$, которые являются одновременно полиномами от $x^p, y^p, z^p, \dots$. Это свойство совершенных полей характеристики p также часто применяется.

Корневое поле. Пусть Δ — какое-нибудь поле характеристики p . Ставя в соответствие каждому элементу x из Δ его p -тую степень x^p , мы получим отображение поля Δ в некоторое его подмножество; будем обозначать это подмножество через Δ^p . В случае совершенного Δ , как мы видели, $\Delta^p = \Delta$. Но и в любом случае установленное соответствие взаимно однозначно; действительно, так как

$$a^p - b^p = (a - b)^p,$$

то $a^p = b^p$ необходимо влечёт за собой $a = b$. Далее, это соответствие является изоморфизмом, так как

$$a^p + b^p = (a + b)^p,$$

$$a^p \cdot b^p = (a \cdot b)^p.$$

Таким образом, Δ^p есть поле, изоморфное полю Δ .

Таким же точно способом можно теперь, наоборот, исходя из поля Δ , построить изоморфное ему расширение $\Delta^{\frac{1}{p}}$, p -той степенью которого будет Δ . Для этого нужно лишь присоединить к полю Δ все ещё не содержа-

щиеся в нём корни p -той степени $a^{\frac{1}{p}}$ из его элементов и подчинить действия над ними правилам:

$$a^{\frac{1}{p}} + b^{\frac{1}{p}} = (a + b)^{\frac{1}{p}},$$

$$a^{\frac{1}{p}} \cdot b^{\frac{1}{p}} = (a \cdot b)^{\frac{1}{p}}.$$

То, что $\Delta^{\frac{1}{p}}$ действительно обладает свойствами поля, читатель докажет без труда, пользуясь изоморфным соответствием $a \rightarrow a^{\frac{1}{p}}$. Надполем $\Delta^{\frac{1}{p}}$, с точностью до эквивалентных расширений, однозначно определяется полем Δ .

Если Δ — совершенное поле, то, очевидно, $\Delta^{\frac{1}{p}} = \Delta$, и обратно.

$\Delta^{\frac{1}{p}}$ называют *корневым полем* поля Δ . Строя для $\Delta^{\frac{1}{p}}$, в свою очередь, корневое поле и т. д., мы получим последовательность полей

$$\Delta, \Delta^{\frac{1}{p}}, \Delta^{\frac{1}{p^2}}, \dots,$$

объединение которых есть, очевидно, совершенное поле, и притом наименьшее совершенное поле, содержащее Δ .

Задача 1. Провести доказательства.

Задача 2. Каждое алгебраическое расширение совершенного поля есть совершенное поле.

Задача 3. Каждое конечное алгебраическое расширение несовершенного поля есть несовершенное поле.

Задача 4. Построить корневое поле для $\Pi(x)$, где Π — совершенное поле характеристики p и x — неизвестное; построить также наименьшее совершенное поле, содержащее $\Pi(x)$.

§ 40. Простота алгебраических расширений.

Теорема о примитивном элементе.

Исследуем, в каких случаях коммутативное конечное расширение Σ поля Δ является простым, т. е. может быть получено путём присоединения одного единственного образующего или «примитивного» элемента. На этот вопрос для широкого класса случаев даёт ответ следующая

Теорема о примитивном элементе. Пусть $\Delta(\alpha_1, \dots, \alpha_n)$ — конечное алгебраическое расширение поля Δ и $\alpha_2, \dots, \alpha_n$ — сепарабельные элементы ¹⁾. Тогда $\Delta(\alpha_1, \dots, \alpha_n)$ является простым расширением.

$$\Delta(\alpha_1, \dots, \alpha_n) = \Delta(\theta).$$

Доказательство. Докажем эту теорему сначала для двух элементов α, β , из которых, по крайней мере, β — сепарабельный. Пусть

¹⁾ Сепарабельно ли α_1 и тем самым всё поле, или нет, — безразлично.

$f(x) = 0$ — неприводимое уравнение для α , и $g(x) = 0$ — неприводимое уравнение для β . Перейдём к полю, в котором $f(x)$ и $g(x)$ полностью распадаются. Пусть $\alpha_1, \dots, \alpha_r$ — различные корни полинома $f(x)$, $\beta_1, \dots, \beta_s$ — различные корни полинома $g(x)$, и, скажем, $\alpha_1 = \alpha$ и $\beta_1 = \beta$.

Мы можем предположить, что Δ содержит бесконечное множество элементов. Действительно, в противном случае также в $\Delta(\alpha, \beta)$ будет иметься лишь конечное число элементов, а для конечных полей существование примитивного элемента (и даже первообразного корня из единицы, степенями которого являются все элементы поля, отличные от нуля) было уже доказано в § 37.

При $k \neq 1$ имеем $\beta_k \neq \beta_1$; следовательно, уравнение

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

для каждого i и каждого $k \neq 1$ обладает в Δ не более чем одним корнем x . Если мы теперь возьмём c , отличное от корней всех этих линейных уравнений, то для каждого i и каждого $k \neq 1$ будем иметь:

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1.$$

Положим

$$\vartheta = \alpha_1 + c\beta_1 = \alpha + c\beta.$$

ϑ есть элемент поля $\Delta(\alpha, \beta)$. Я утверждаю, что ϑ уже обладает свойством искомого примитивного элемента: $\Delta(\alpha, \beta) = \Delta(\vartheta)$.

Элемент β удовлетворяет уравнениям

$$\begin{aligned} g(\beta) &= 0, \\ f(\vartheta - c\beta) &= f(\alpha) = 0, \end{aligned}$$

коэффициенты которых лежат в $\Delta(\vartheta)$. Полиномы $g(x)$, $f(\vartheta - cx)$ имеют общим лишь один корень β , так как для остальных корней β_k ($k \neq 1$) первого уравнения имеем

$$\vartheta - c\beta_k \neq \alpha_i \quad (i = 1, \dots, r),$$

и, следовательно,

$$f(\vartheta - c\beta_k) \neq 0.$$

β — простой корень полинома $g(x)$. Поэтому $g(x)$ и $f(\vartheta - cx)$ имеют общим делителем только линейный множитель $x - \beta$. Но коэффициенты этого наибольшего общего делителя должны лежать уже в $\Delta(\vartheta)$; таким образом, β лежит в $\Delta(\vartheta)$. Так как $\alpha = \vartheta - c\beta$, то это же верно и для α , и, значит, действительно $\Delta(\alpha, \beta) = \Delta(\vartheta)$.

Тем самым наша теорема доказана для $h = 2$. Но если она уже доказана для $h - 1$ (≥ 2), то имеем:

$$\Delta(\alpha_1, \dots, \alpha_{h-1}) = \Delta(\eta),$$

и следовательно, по доказанному,

$$\Delta(\alpha_1, \dots, \alpha_{h-1}, \alpha_h) = \Delta(\eta, \alpha_h) = \Delta(\vartheta),$$

т. е. теорема справедлива и для h .

Следствие. Каждое сепарабельное конечное расширение является простым.

Эта теорема часто весьма упрощает исследование конечных сепарабельных расширений, так как наличие обозримого базисного представления

$$\sum_0^{n-1} a_k \theta^k$$

позволяет легко овладеть структурой и изоморфизмами этого расширения. Например, мы получаем теперь новое доказательство для того факта, установленного в § 38 (мелкий шрифт) путём последовательного продолжения изоморфизмов, что *число относительных изоморфизмов конечного сепарабельного расширения Σ поля Δ равно степени $(\Sigma : \Delta)$* . Действительно, для простых сепарабельных расширений это утверждение было ещё раньше доказано в § 38, а, как мы теперь знаем, каждое конечное сепарабельное расширение является простым ¹⁾.

В случае поля характеристики нуль каждое конечное расширение является сепарабельным и, значит, простым. Но можно также в случае характеристики p точно указать, когда конечное расширение является простым:

Конечное расширение Σ поля Δ характеристики p является простым тогда и только тогда, когда

$$(1) \quad n = n_0 p^e,$$

где n — степень, n_0 — приведённая степень и e — показатель расширения Σ .

Доказательство. Начнём со следующего предварительного замечания: если $\Sigma = \Delta(\alpha_1, \dots, \alpha_r)$, то показатель расширения Σ равен максимуму e показателей элементов $\alpha_1, \dots, \alpha_r$. Действительно, прежде всего показатель расширения Σ во всяком случае $\geq e$. Но так как все элементы из Σ рационально выражаются через $\alpha_1, \dots, \alpha_r$ (с коэффициентами из Δ), то, в силу правила возвышения в степень, результаты возведения элементов поля Σ в степень p^e рационально выражаются через $\alpha_1^{p^e}, \dots, \alpha_r^{p^e}$. Тем самым эти степени являются сепарабельными элементами, и показатель поля Σ равен точно e . Согласно § 38, сепарабельные элементы поля Σ образуют в Σ расширение Σ_0 поля Δ , снова сепарабельное.

Пусть теперь Σ является простым расширением: $\Sigma = \Delta(\theta)$. Тогда $\theta^{p^e} \in \Sigma_0$. Таким образом, полагая снова $(\Sigma : \Sigma_0) = pf$, имеем $f \leq e$, а так как, с другой стороны, всегда $e \leq f$, то $e = f$. Отсюда и из равенства $n = n_0 p^f$ и следует условие (1).

¹⁾ Предыдущее (более длинное) доказательство путём последовательного продолжения изоморфизмов более поучительно, так как из него можно развить всю теорию несепарабельных расширений. Но для читателя, интересующегося, главным образом, сепарабельными расширениями, как наиболее важными и чаще всего встречающимися, предпочтительнее будет изложенное сейчас доказательство с помощью теоремы о примитивном элементе.

Обратно, пусть условие (1) выполнено. Σ_0 , как конечное сепарабельное расширение, является простым:

$$\Sigma_0 = \Delta(\alpha).$$

Пусть β — элемент из Σ , имеющий показателем как раз e . Тогда

$$\beta^{p^e} = \mu_0 \in \Sigma_0$$

и полином $x^{p^e} - \mu_0$ неприводим в Σ_0 , так как иначе уже $\beta^{p^{e-1}}$ лежало бы в Σ_0 (§ 38, задача 3). Таким образом, $\Sigma_0(\beta)$ — степени p^e над Σ_0 , и следовательно — степени $n = n_0 p^e$ над Δ . Так как Σ — также степени n над Δ , то заключаем, что $\Sigma_0(\beta) = \Sigma$ или $\Sigma = \Delta(\alpha, \beta)$. Но α сепарабельно; поэтому из теоремы о примитивном элементе следует, что расширение Σ — простое, что и требовалось доказать.

Задача 1. Если x и y неизвестны, то расширение $\Delta(x^{\frac{1}{p}}, y^{\frac{1}{p}})$ поля $\Delta(x, y)$, где Δ — поле характеристики p , уже не является простым.

Задача 2. Для характеристики $\neq 2$ всегда

$$\Delta(\sqrt{x}, \sqrt{y}) = \Delta(x, y, \sqrt{x} + \sqrt{y}),$$

а для характеристики 2 это соотношение уже не имеет места.

§ 41. Нормы и следы.

Пусть сначала Σ — конечное коммутативное расширение поля Δ . Относительные изоморфизмы поля Σ , переводящие Σ в сопряжённые поля, переводят также каждый элемент η поля Σ в сопряжённые с ним элементы. Если мы для простоты примем, что Σ — простое расширение: $\Sigma = \Delta(\vartheta)$, то

$$\eta = \psi(\vartheta) = a_0 + a_1 \vartheta + \dots + a_{n-1} \vartheta^{n-1},$$

и, осуществляя изоморфные отображения путём замены ϑ на сопряжённые элементы, мы получим:

$$\eta_v = \psi(\vartheta_v) = a_0 + a_1 \vartheta_v + \dots + a_{n-1} \vartheta_v^{n-1}.$$

При этом сопряжённые элементы ϑ_v снабжены номерами от 1 до n и каждый засчитывается столько раз, сколько раз он встречается в разложении на линейные множители неприводимого в $\Delta[t]$ полинома $\varphi(t)$, корнем которого служит ϑ . Таким образом, при сепарабельном ϑ каждый изоморфизм считается один раз, а при несепарабельном ϑ — несколько раз.

Рассмотрим теперь элементарные симметрические функции от $\eta_1, \dots, \eta_n$, в частности сумму

$$\sum_{v=1}^n \eta_v = S(\eta),$$

называемую следом элемента η , и произведение

$$\prod_{v=1}^n \eta_v = N(\eta),$$

называемое нормой элемента η .

Построение следа и нормы мы распространим также на полиномы с коэффициентами из Σ , условившись при этом, что под действие изоморфных отображений $\vartheta \rightarrow \vartheta$, попадают лишь коэффициенты этих полиномов, но не неизвестные. Так, например,

$$(1) \quad N(z - \eta) = \prod_{v=1}^n (z - \eta_v).$$

Коэффициентами этого полинома $G(z) = N(z - \eta)$ служат как раз элементарные симметрические функции от $\eta_1, \dots, \eta_n$. Таким образом, за основу достаточно принять одно понятие нормы: след и остальные элементарные симметрические функции могут быть определены с помощью нормы $N(z - \eta)$.

Данное выше, обычное в теории алгебраических чисел, определение нормы имеет то преимущество, что из него с очевидностью вытекают два основных свойства нормы и следа, а именно:

$$(2) \quad \begin{cases} N(\alpha\beta) = N(\alpha)N(\beta), \\ S(\alpha + \beta) = S(\alpha) + S(\beta). \end{cases}$$

Недостатком его является, однако, то, что оно непосредственно не переносится на непростые расширения поля и вовсе не переносится на произвольные алгебры с делением, как и вообще на другие алгебры. Поэтому мы дадим ниже некоторые другие определения нормы, более доступные обобщению.

Полином (1) после подстановки в него выражений $\eta_v = \psi(\vartheta_v)$ становится симметрической функцией корней ϑ_v и потому выражается целым рациональным образом через элементарные симметрические функции от ϑ_v , т. е. через коэффициенты полинома $\varphi(t)$. Корнями полинома $G(z) = N(z - \eta)$ служат сопряжённые с η величины η_v . Если $g(z)$ — неприводимый полином с корнем η_1 , то $G(z)$, имея с $g(z)$ общий корень η_1 , делится на $g(z)$. Пусть $(g(z))^r$ — наивысшая степень полинома $g(z)$, содержащаяся в $G(z)$, и

$$G(z) = (g(z))^r h(z).$$

Второй множитель $h(z)$ не имеет никаких линейных множителей, отличных от множителей вида $z - \eta_v$, входящих также в $g(z)$. Если бы $h(z)$ не был константой, то он имел бы с $g(z)$ общий корень η_v и, значит, должен был бы делиться на $g(z)$. Таким образом, $h(z)$ есть константа. Нормируя $g(z)$ так, чтобы старший коэффициент был $= 1$, получаем:

$$G(z) = (g(z))^r,$$

и те величины, вида $T. \text{ ф. алгебр. сопряженные}$
 η_v , являются корнями одного

и корни и из $\varphi(t)$, это
 раз ϑ и ϑ^2 . В $\varphi(t)$
 мы имеем ϑ и ϑ^2
 Т. ф.
 не
 водит
 то е
 при
 (ли
 η_2
 ср 13

Полагая

$$g(z) = z^m + b_1 z^{m-1} + \dots + b_m,$$

будем иметь:

$$G(z) = (g(z))^r = z^{mr} + r b_1 z^{mr-1} + \dots + b_m^r,$$

и тем самым

$$(3) \quad \begin{cases} S(\eta) = -r b_1, \\ N(\eta) = (-1)^{mr} b_m^r. \end{cases}$$

Степень n полинома $G(z)$ равна mr , и, следовательно,

$$(4) \quad r = \frac{n}{m} = \frac{(\Sigma : \Delta)}{(\Delta(\eta) : \Delta)} = (\Sigma : \Delta(\eta)).$$

Формулы (3), (4) содержат определение следа и нормы, сохраняющее смысл для произвольного тела конечного ранга над Δ , в предположении, что Δ лежит в центре тела. Но при этом определении свойства (2) уже не очевидны. Мы дадим поэтому ещё третье равносильное определение нормы, имеющее, кроме того, то преимущество, что оно сохраняет смысл в произвольных алгебрах.

Пусть $(\omega_1, \dots, \omega_n)$ — базис поля Σ над Δ . Выразим линейно через базис все произведения

$$(5) \quad \eta \omega_j = \sum_k c_{jk} \omega_k,$$

и образуем определитель D коэффициентов c_{jk} . Мы утверждаем теперь, что $D = N(\eta)$.

Покажем сначала, что D не зависит от выбора базиса. Если $(\omega'_1, \dots, \omega'_n)$ — другой базис и

$$(6) \quad \omega'_i = \sum_j a_{ij} \omega_j,$$

$$(7) \quad \omega_k = \sum_i b_{ki} \omega'_i,$$

то из (5), (6) и (7) находим:

$$\eta \omega'_i = \sum_j \sum_k \sum_l a_{ij} c_{jk} b_{kl} \omega'_l;$$

таким образом, новые коэффициенты задаются формулой

$$c_{il}' = \sum_j \sum_k a_{ij} c_{jk} b_{kl}.$$

Отсюда для определителей D' , A , B элементов c_{ij}' , a_{ij} , b_{kl} , по теореме умножения определителей, следует равенство

$$(8) \quad D' = ABD.$$

Если мы, в частности, выберем $\eta = 1$, то коэффициенты c_{jk} и c_{jk}' будут равны 1 при $j = k$ и равны 0 при $j \neq k$, так что $D = D' = 1$; таким образом, в качестве частного случая равенства (8) получим:

$$(9) \quad 1 = AB.$$

Но из (8) и (9) следует, что $D' = D$, т. е. определитель D действительно не зависит от выбора базиса.

Рассмотрим теперь, как ведёт себя определитель D при расширении поля Σ . Пусть Ω — расширение поля Σ и пусть $(\sigma_1, \dots, \sigma_n)$ — базис для Σ над Δ и $(\omega_1, \dots, \omega_s)$ — базис для Ω над Σ , стало быть $(\sigma_1\omega_1, \sigma_2\omega_1, \dots, \sigma_n\omega_1, \dots, \sigma_1\omega_s, \sigma_2\omega_s, \dots, \sigma_n\omega_s)$ — базис для Ω над Δ . Определитель D_Σ элемента η поля Σ найдётся из равенств

$$\eta\sigma_j = \sum_k c_{jk}\sigma_k.$$

Умножая эти равенства на ω_l , получим:

$$(10) \quad \eta\sigma_j\omega_l = \sum_k c_{jk}\sigma_k\omega_l.$$

Определитель D_Ω коэффициентов правой части равенств (10) состоит поэтому из s одинаковых блоков (c_{jk}) , расположенных вдоль главной диагонали:

$$D_\Omega = \begin{vmatrix} \boxed{\begin{matrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{n1} & \dots & c_{nn} \end{matrix}} & & 0 \\ & \boxed{\begin{matrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{n1} & \dots & c_{nn} \end{matrix}} & \\ & & \dots & \dots & \dots \end{vmatrix}$$

Таким образом, определитель элемента η , образованный в поле Ω , равен

$$(11) \quad D_\Omega = D_\Sigma^s; \quad s = (\Omega : \Sigma).$$

Вследствие формулы (11), можно для вычисления определителя D_{Σ} элемента η ограничиться наименьшим полем, содержащим этот элемент, т. е. полем $\Delta(\eta)$ с базисом $(1, \eta, \eta^2, \dots, \eta^{m-1})$. Относительно этого базиса, принимая во внимание определяющее уравнение $g(\eta) = 0$, имеем:

$$\eta \cdot 1 = \eta,$$

$$\eta \cdot \eta = \eta^2,$$

$$\eta \cdot \eta^2 = \eta^3,$$

$$\dots$$

$$\eta \cdot \eta^{m-1} = \eta^m = -b_m - b_{m-1}\eta - \dots - b_1\eta^{m-1}.$$

Следовательно, определитель элемента η в поле $\Delta(\eta)$ будет

$$D_{\Delta(\eta)} = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -b_m & -b_{m-1} & -b_{m-2} & \dots & -b_1 \end{vmatrix} = (-1)^m b_m.$$

В силу формулы (11), отсюда следует:

$$(12) \quad D_{\Sigma} = D'_{\Delta(\eta)} = (-1)^{mr} b_m^r, \quad r = (\Sigma: \Delta(\eta)).$$

Сравнение формул (3) и (4) с (12) показывает, что D_{Σ} действительно есть норма элемента η в поле Σ :

$$(13) \quad N(\eta) = D_{\Sigma}.$$

Если η — не элемент поля, а полином из $\Sigma[x_1, x_2, \dots]$, то сохраняют силу те же рассуждения, с тем лишь отличием, что неизвестные $x_1, x_2, \dots$ считаются присоединёнными к основному полю. Если η — полином степени h , то норма D_{Σ} будет полиномом степени nh . Рассматривая, например, вместо элемента η полином $z - \eta$, будем иметь из (5):

$$(z - \eta) \omega_j = z \omega_j - \sum_k c_{jk} \omega_k,$$

и

$$(14) \quad N(z - \eta) = \begin{vmatrix} z - c_{11} & -c_{12} & \dots & -c_{1n} \\ -c_{21} & z - c_{22} & \dots & -c_{2n} \\ \dots & \dots & \dots & \dots \\ -c_{n1} & -c_{n2} & \dots & z - c_{nn} \end{vmatrix}.$$

Коэффициент при z^{n-1} в $N(z - \eta)$, взятый с обратным знаком, есть снова след элемента η :

$$(15) \quad S(\eta) = c_{11} + c_{22} + \dots + c_{nn}.$$

Мы докажем теперь, что из определений (13) и (15) нормы и следа уже вытекают формулы (2).

Пусть $(\omega_1, \dots, \omega_n)$ — базис поля и

$$(16) \quad \alpha \omega_j = \sum_k a_{jk} \omega_k,$$

$$(17) \quad \beta \omega_j = \sum_k b_{jk} \omega_k.$$

Умножая левую и правую части равенства (17) на α и пользуясь равенством (16), получаем:

$$\alpha \beta \omega_j = \sum_k \sum_l b_{jk} a_{kl} \omega_l.$$

Таким образом, произведению $\alpha \beta$ соответствуют коэффициенты

$$c_{jl} = \sum_k b_{jk} a_{kl}.$$

Отсюда по теореме умножения определителей и следует, что

$$N(\alpha \beta) = N(\alpha) N(\beta).$$

Ещё легче доказательство соотношения для следов. Сложение формул (16) и (17) даёт:

$$(\alpha + \beta) \omega_j = \sum_k (a_{jk} + b_{jk}) \omega_k,$$

$$S(\alpha + \beta) = \sum_j (a_{jj} + b_{jj}) = \sum_j a_{jj} + \sum_j b_{jj} = S(\alpha) + S(\beta).$$

Норма и след зависят не только от η и основного поля Δ , но также и от надполя Σ . Желая подчеркнуть это, вместо N пишут N_Σ или $N_{\Sigma/\Delta}$. По формуле (11),

$$(18) \quad N_\Sigma(\eta) = N_\Sigma(\eta)^s; \quad s = (\Sigma : \Delta).$$

Заменяя здесь η на z — η и сравнивая коэффициенты при степенях z , непосредственно следующих за старшими, получаем, что

$$(19) \quad S_\Sigma(\eta) = s \cdot S_\Sigma(\eta).$$

Докажем теперь ещё две теоремы, которые понадобятся в следующем параграфе.

1. Соотношение вида

$$Nf(x_1, x_2, \dots) = F(x_1, x_2, \dots)$$

сохраняет силу, если заменить неизвестные $x_1, x_2, \dots$ элементами основного поля Δ (или какими-нибудь полиномами над Δ).

2. Если η — полином с коэффициентами из Σ , то $N(\eta)$ делится на η .

Первая из этих теорем непосредственно следует из определения нормы (13).

Вторая доказывается следующим образом: так как $N(z - \eta) = (g(z))^r$ и $g(\eta) = 0$, то $N(z - \eta)$ делится на $z - \eta$:

$$N(z - \eta) = (z - \eta) h(z);$$

полагая здесь $z = 0$, мы и получаем утверждение теоремы.

Задача 1. Вычислить норму элемента $a + b\sqrt{d}$ в квадратичном поле $\Delta(\sqrt{d})$. $N = a^2 - b^2 d$

Задача 2. Вычислить норму элемента $1 + \theta^2$ в поле $\Delta(\theta)$, где Δ — поле рациональных чисел и θ удовлетворяет неприводимому уравнению $\theta^3 + \theta + 1 = 0$. $N = 1$

Сколько ни изящны свойства определённой здесь нормы и сколько ни полезна она в коммутативных случаях, тем не менее не это есть норма, применяемая большей частью при изучении тел и матричных колец. Так, например, в случае тела кватернионов норма элемента $a + bj + ck + dl$ при нашем определении равна $(a^2 + b^2 + c^2 + d^2)^2$, тогда как обычно нормой кватерниона считают просто $a^2 + b^2 + c^2 + d^2$. Поэтому мы введём понятие *приведённой нормы*, определяемой следующим образом.

Пусть $(\omega_1, \dots, \omega_n)$ — базис рассматриваемой алгебры с делением (или вообще некоторой алгебры) Σ . Присоединим к основному полю Δ n неизвестных $u_1, \dots, u_n$ и образуем «общий элемент» алгебры Σ

$$\eta_u = u_1 \omega_1 + \dots + u_n \omega_n.$$

Общий элемент η_u является алгебраическим над $\Delta(u_1, \dots, u_n)$ и потому удовлетворяет некоторому уравнению наименьшей степени $g_u(\eta_u) = 0$. Как и выше, имеем:

$$(20) \quad N(z - \eta_u) = (g_u(z))^r.$$

Так как $N(z - \eta_u)$, в силу равенства (14), есть однородная форма относительно $z, u_1, \dots, u_n$, то и $g_u(z)$ есть такая форма (с коэффициентами из Δ). Расположим $g_u(z)$ по степеням z :

$$g_u(z) = z^m + b_1(u) z^{m-1} + \dots + b_m(u)$$

и назовём — $b_1(u)$ *приведённым следом*, $(-1)^m b_m(u)$ — *приведённой нормой* общего элемента η_u . Если теперь

$$\eta = a_1 \omega_1 + \dots + a_n \omega_n$$

— произвольный элемент из Σ , то, произведя замену $u_k \rightarrow a_k$, назовём — $b_1(a)$ *приведённым следом* и $(-1)^m b_m(a)$ — *приведённой нормой* элемента η . Мы будем обозначать их, соответственно, через $s(\eta)$ и $n(\eta)$. Положив в (20) $u_k = a_k$ и $z = 0$, получим:

$$(21) \quad N(\eta) = (n(\eta))^r.$$

Таким образом, «регулярная норма» $N(\eta)$ является степенью приведённой нормы $n(\eta)$. В случае простого (коммутативного) расширения поля Δ нормы $N(\eta)$ и $n(\eta)$ совпадают.

Аналогичным образом для следов получаем соотношение

$$(22) \quad S(\eta) = r \cdot s(\eta).$$

В силу однородности формы $g_u(z)$ приведённый след $s(\eta_u)$ является линейной формой относительно $u_1, \dots, u_n$. Отсюда непосредственно вытекает аддитивность этого следа:

$$s(\alpha + \beta) = s(\alpha) + s(\beta).$$

Для доказательства соответствующего свойства нормы образуем, вводя новые неизвестные $v_1, \dots, v_n$, второй общий элемент

$$\eta_v = v_1 \omega_1 + \dots + v_n \omega_n.$$

Тогда $n(\eta_u \eta_v)$ есть форма относительно неизвестных u и v , и имеет место соотношение

$$N(\eta_u \eta_v) = N(\eta_u) N(\eta_v)$$

или, в силу (21),

$$n(\eta_u \eta_v)^r = n(\eta_u)^r n(\eta_v)^r.$$

Отсюда

$$n(\eta_u \eta_v) = \gamma n(\eta_u) n(\eta_v),$$

где γ — корень r -той степени из единицы и, значит, не зависит от u и v . Придавая теперь неизвестным u и v такие значения, чтобы было $\eta_u = \eta_v = 1$, получим:

$$1 = \gamma \cdot 1 \cdot 1,$$

т. е. $\gamma = 1$. Тем самым

$$n(\eta_u) n(\eta_v) = n(\eta_u \eta_v),$$

и это свойство сохраняет силу при любом выборе значений для u и v .

Таким образом, формулы (2) верны также для приведённых следов и норм.

Задача 3. Доказать, что приведённая норма кватерниона $a + bj + ck + dl$ действительно равна $a^2 + b^2 + c^2 + d^2$.

Задача 4. Приведённая норма (в коммутативных расширениях) равна регулярной норме тогда и только тогда, когда расширение простое.

§ 42. Выполнение конструкций теории полей с помощью конечного числа шагов.

В этой главе мы провели ряд различных доказательств существования полей: существования полей рациональных функций $\Delta(x, y, \dots)$, существования простого алгебраического расширения $\Delta(\vartheta)$ (где ϑ удовлетворяет заданному неприводимому уравнению), существования поля разложения $\Delta(\alpha_1, \dots, \alpha_n)$ полинома $f(x)$. Возникает теперь вопрос, можно ли все эти поля эффективно построить и можно ли заменить данные нами доказательства существования конструктивными (конечными, интуиционистскими).

Мы назовём поле Δ явно заданным, если элементы этого поля однозначно изображены различными символами, которые можно складывать, вычитать, умножать и делить путём конечного числа операций.

Покажем сначала, что:

Если поле Δ явно задано, то явно задано также каждое простое трансцендентное его расширение $\Delta(f)$, равно как и каждое простое алгебраическое расширение $\Delta(\vartheta)$, определяющее уравнение

которого $\varphi = 0$, предполагаемое, разумеется, неприводимым, известно.

Доказательство. Элементами поля $\Delta(t)$ являются отношения $\frac{f(t)}{g(t)}$, $g(t) \neq 0$, правила действий над которыми были уже установлены в § 18. Для достижения единственности представления можно ещё потребовать, чтобы f и g были взаимно простыми и чтобы старший коэффициент знаменателя $g(t)$ был равен единице. При заданных f и g нахождение их наибольшего общего делителя, а тем самым приведение дроби к несократимому виду, выполняется с помощью алгоритма Евклида (§ 18) действительно явно.

В случае $\Delta(\theta)$ элементы поля однозначно представимы выражениями $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$, причём операции над этими выражениями производятся по правилам действий над полиномами, с той лишь разницей, что результат вычисления всегда приводится к наименьшему вычету по модулю φ (§ 32). Как выполнить деление двух таких выражений, было уже указано в § 19 (решение уравнения $\bar{a}x = \bar{b}$ в кольце классов вычетов по простому элементу).

Попытка аналогичного построения, с помощью методов § 35, поля разложения полинома $f(x)$ упирается в проблему разложения полинома на множители в заданном или уже построенном поле. Мы не обладаем никаким общим методом, который бы для каждого явно заданного поля K позволял выполнять разложение полиномов из $K[z]$ на простые множители с помощью конечного числа операций, и имеются основания предполагать, что такой общий метод вообще невозможен¹⁾. Тем не менее, мы видели, что для специальных полей (поля рациональных чисел, поля гауссовских чисел, поля рациональных функций от n неизвестных с рациональными коэффициентами, поля классов вычетов по модулю p и т. д.) такие методы разложения на простые множители существуют. Мы покажем теперь, что:

1) Если в поле Δ разложение полиномов от одного неизвестного выполнимо с помощью конечного числа операций, то это же имеет место и для полиномов от n неизвестных.

2) Если в поле Δ разложение полиномов (от одного или нескольких неизвестных) выполнимо с помощью конечного числа операций, то это же имеет место и для каждого простого трансцендентного расширения $\Delta(t)$, равно как и для каждого сепарабельного простого алгебраического расширения $\Delta(\theta)$, определяющее уравнение которого $\varphi(\theta) = 0$ известно.

Доказательство утверждения 1) основывается на одном приёме, предложенном Кронекером. Пусть $f(x_1, \dots, x_n)$ — заданный

¹⁾ См. B. L. van der Waerden, Eine Bemerkung über die Unzerlegbarkeit von Polynomen. *Math. Ann.*, 102 (1930), 738—739.

полином. Выберем тогда целое число m , большее степени полинома, и сделаем подстановку

$$x_v = t^{m^{v-1}}.$$

При этом член $a_p x_1^{p_1} x_2^{p_2} \dots x_n^{p_n}$ перейдет в $a_p t^{p_1 + p_2 m + \dots + p_n m^{n-1}}$, следовательно, различные произведения степеней x перейдут в различные степени t (ибо каждое целое число может быть записано в виде $p_1 + p_2 m + \dots + p_n m^{n-1}$ с $0 \leq p_v < m$ не более чем одним способом). Если теперь заданный полином $f(x_1, \dots)$ разложим:

$$f = g_1 g_2,$$

то разложение сохраняется и после указанной выше подстановки; пусть оно примет при этом вид

$$f^*(t) = g_1^*(t) g_2^*(t).$$

Тогда по полиномам g_1^* , g_2^* можно будет восстановить первоначальные полиномы g_1 , g_2 , так как каждому члену в g_v^* может соответствовать лишь один член в g_v . Итак, разложим $f^*(t)$ всеми возможными способами на два множителя (это выполнимо, если известно разложение $f^*(t)$ на простые множители) и установим для каждого разложения, какие полиномы g_1 , g_2 соответствуют данным множителям g_1^* , g_2^* . Тогда в каждом случае можно будет проверить, удовлетворяют ли эти полиномы g_1 , g_2 равенству

$$f = g_1 g_2.$$

Если это не имеет места ни в одном случае, то, значит, f неразложим; если же это равенство удовлетворяется для некоторых g_1 и g_2 , то подвергнем g_1 и g_2 такому же исследованию, как ранее f , и так до тех пор, пока — не более чем в m приёмов — не будет найдено полное разложение полинома f на простые множители.

Доказательство утверждения 2) в случае трансцендентного расширения $\Delta(t)$ совсем просто. Каждый полином $f(t, z)$ из $\Delta(t)[z]$ может быть сделан путём умножения на некоторый полином от одного t целым рациональным относительно t . Тогда, согласно § 23, каждому разложению полинома $f(t, z)$, рациональному относительно t , будет соответствовать целое рациональное разложение, и обратно. Тем самым задача приведена к разложению полиномов в $\Delta[t, z]$. *и членами 1-й степени. В будущем*

В случае алгебраического расширения $\Delta(\vartheta)$, где ϑ удовлетворяет сепарабельному неприводимому уравнению $\varphi(\vartheta) = 0$, дело обстоит не столь просто. Пусть задан полином $f(\vartheta, z)$ из $\Delta(\vartheta)[z]$. Во избежание многозначности в разложении на множители будем предполагать как сам полином, так и все его делители (если таковые имеются) нормированными так, чтобы старший коэффициент был равен 1. образуем теперь, вводя новое неизвестное u , полином $f(\vartheta, z - u\vartheta)$

и рассмотрим его норму, определённую как указано в § 41. Эта последняя является снова нормированным полиномом:

$$Nf(\vartheta, z - u\vartheta) = F(z, u).$$

Он может быть разложен в $\Delta[z, u]$ на нормированные неприводимые множители:

$$(1) \quad F(z, u) = F_1(z, u) F_2(z, u) \dots F_r(z, u).$$

Разыщем теперь в $\Delta(\vartheta)[z]$ наибольший общий делитель каждого множителя $F_k(z, u)$ с $f(\vartheta, z - u\vartheta)$. Если такой наибольший общий делитель не равен ни $f(\vartheta, z - u\vartheta)$, ни 1, то он является собственным делителем полинома $f(\vartheta, z - u\vartheta)$; в этом случае $f(\vartheta, z - u\vartheta)$, а потому также $f(\vartheta, z)$, разложимо в произведение двух множителей. Тогда мы возьмём один из этих множителей, скажем f_1 , и исследуем его таким же способом путём разложения нормы $Nf_1(\vartheta, z - u\vartheta)$. Этот процесс закончится тогда, когда каждый из множителей $F_k(z, u)$ будет либо делиться на $f(\vartheta, z - u\vartheta)$, либо взаимно просто с $f(\vartheta, z - u\vartheta)$. При этом все множители произведения (1) не могут быть взаимно просты с $f(\vartheta, z - u\vartheta)$, ибо в таком случае и всё произведение $F(z, u)$ было бы взаимно просто с $f(\vartheta, z - u\vartheta)$, что невозможно, так как норма полинома делится на сам этот полином. Таким образом, один из множителей полинома $F(z, u)$, скажем F_1 , делится на $f(\vartheta, z - u\vartheta)$.

В этом предположении мы утверждаем теперь, что полином $f(\vartheta, z)$ сам неприводим, и тем самым разложение уже закончено. Действительно, предположим, что $f(\vartheta, z)$ разложим:

$$f(\vartheta, z) = f_1(\vartheta, z) f_2(\vartheta, z).$$

Тогда замена z на $z - u\vartheta$ и построение норм дают:

$$(2) \quad F(z, u) = Nf(\vartheta, z - u\vartheta) = Nf_1(\vartheta, z - u\vartheta) Nf_2(\vartheta, z - u\vartheta).$$

Сравнивая это разложение с (1), мы видим, что одна из двух норм в правой части равенства (2), скажем $Nf_1(\vartheta, z - u\vartheta)$, делится на $F_1(z, u)$, а тем самым и на $f(\vartheta, z - u\vartheta)$:

$$Nf_1(\vartheta, z - u\vartheta) = f(\vartheta, z - u\vartheta) g(\vartheta, z, u).$$

Сравнивая члены левой и правой частей, имеющие высшие степени относительно z и u , и принимая во внимание, что f_1 и f нормированы, начинаясь, таким образом, с членов $(z - u\vartheta)^{m_1}$, соответственно, $(z - u\vartheta)^m$, получаем, что

$$[N(z - u\vartheta)]^{m_1} = N[(z - u\vartheta)^{m_1}] = (z - u\vartheta)^m g_1(\vartheta, z, u).$$

Так как $m > m_1$ ($f = f_1 f_2$ имеет высшую степень, чем f_1), то вхо-

дающая в левую часть норма $N(z - u\vartheta)$ содержит $z - u\vartheta$ в степени, большей, чем первая:

$$N(z - u\vartheta) = (z - u\vartheta)^2 h(\vartheta, z, u).$$

Полагая $u = 1$, получаем:

$$N(z - \vartheta) = (z - \vartheta)^2 h(\vartheta, z, 1).$$

Но $N(z - \vartheta) = \varphi(z)$, как определяющий полином сепарабельного поля $\Delta(\vartheta)$, не должен содержать кратных множителей. Тем самым мы пришли к противоречию, и, значит, полином $f(\vartheta, z)$ при указанных предположениях неприводим.

Таким образом, указанным методом действительно возможно найти неприводимые множители полинома $f(\vartheta, z)$ с помощью конечного числа операций [по крайней мере теоретически: на практике вычисление и разложение на множители нормы $Nf(\vartheta, z - u\vartheta)$ уже в простейших случаях наталкивается на почти непреодолимые трудности вычислительного характера].

Изложенное выше доказательство построено таким образом, что в нём не предполагается существование поля разложения.

Если теперь поле Δ последовательно расширяется путём присоединения (трансцендентных или сепарабельных алгебраических) величин $\vartheta_1, \vartheta_2, \dots, \vartheta_n$, то в силу предыдущих теорем разложение на множители полиномов в поле $\Delta(\vartheta_1, \vartheta_2, \dots, \vartheta_n)$ можно шаг за шагом свести к разложению полиномов в Δ .

Тем самым мы получили и средство, дающее в важнейших случаях возможность заменять доказательства существования, изложенные в этой главе, конструктивными доказательствами, например, построением поля разложения полинома $f(x)$, построением соответствующего нормального поля для поля $\Delta(\vartheta_1, \dots, \vartheta_n)$, построением примитивного элемента ϑ , равно как и изоморфизмов поля $\Delta(\vartheta_1, \dots, \vartheta_n) = \Delta(\vartheta)$ в соответствующем нормальном поле.

ГЛАВА ШЕСТАЯ.

ПРОДОЛЖЕНИЕ ТЕОРИИ ГРУПП.

Содержание. В §§ 43 и 44 рассматривается одно дальнейшее развитие понятия группы. §§ 45—47 содержат важные общие теоремы о нормальных делителях и «композиционных рядах», тогда как §§ 48 и 49 содержат специальные теоремы о группах подстановок, используемые дальше лишь в теории Галуа.

§ 43. Группы с операторами.

В этом параграфе понятие группы будет подвергнуто дальнейшему развитию, которое придаст всем рассмотренным большую общность, необходимую для последующих применений (в главах 15—17). Читатель, интересующийся пока только теорией Галуа, может спокойно пропустить этот и следующий параграфы; всюду, где в дальнейших параграфах будет идти речь о группах, он сможет разуть (скажем, конечные) группы в ранее установленном смысле.

Пусть заданы: во-первых, группа (в обычном смысле) $\mathfrak{G}$, с элементами $a, b, \dots$; во-вторых, множество Ω новых объектов $\eta, \theta, \dots$, которые мы будем называть *операторами*. При этом пусть для каждого θ и каждого a определено произведение θa («результат применения оператора θ к элементу a группы»), снова принадлежащее к группе $\mathfrak{G}$. Далее, будем предполагать, что каждый оператор θ «дистрибутивен», т. е. что

$$(1) \quad \theta(ab) = \theta a \cdot \theta b.$$

Иными словами: «умножение» на оператор θ должно быть эндоморфизмом группы $\mathfrak{G}$ ¹⁾. Если все эти условия выполнены, то $\mathfrak{G}$ называется *группой с операторами*, а Ω — её *областью операторов*.

Допустимой подгруппой группы $\mathfrak{G}$ (относительно области операторов Ω) будет называться подгруппа $\mathfrak{H}$, выдерживающая действие всех операторов из Ω , т. е. такая, что для всякого элемента a подгруппы $\mathfrak{H}$ также все θa лежат в $\mathfrak{H}$. Допустимая подгруппа, являющаяся одновременно нормальным делителем, будет называться *допустимым нормальным делителем*.

¹⁾ Отсюда следует, что при «умножении» на θ единица группы переходит в единицу, а обратный элемент — в обратный.

Пример 1. Пусть операторами будут внутренние автоморфизмы группы $\mathfrak{G}$:

$$\theta a = sac^{-1}.$$

Допустимыми будут те подгруппы, которые вместе с каждым a содержат и все sac^{-1} , т. е. нормальные делители.

Пример 2. Пусть операторами будут все автоморфизмы группы $\mathfrak{G}$. Допустимыми будут те подгруппы, которые переходят в себя при каждом автоморфизме; их называют характеристическими подгруппами.

Пример 3. Пусть $\mathfrak{G}$ — кольцо, рассматриваемое как группа относительно сложения. Область операторов $\mathfrak{Q}$ пусть служит само же кольцо, а произведением θa — произведение θ и a как элементов кольца. Тогда (1) есть обычный закон дистрибутивности:

$$r(a + b) = ra + rb.$$

Допустимыми подгруппами являются *левые идеалы*, т. е. подгруппы, содержащие вместе с каждым a также все ra .

Пример 4. Иногда оказывается более предпочтительным записывать операторы θ справа от элементов группы, т. е. вместо θa писать $a\theta$. Тогда (1) запишется так:

$$(ab)\theta = a\theta \cdot b\theta.$$

Если, например, разумеет под такими правыми операторами элементы кольца (рассматриваемого как группа относительно сложения), причём снова считать $a\theta$ произведением a и θ как элементов кольца, то в качестве допустимых подгрупп получим *правые идеалы*.

Пример 5. Наконец, часть операторов можно записывать слева, другую часть — справа. Если, например, взять в качестве операторов, действующих в кольце как в группе по сложению, сами элементы этого кольца, рассматриваемые как левые мультипликаторы, и те же элементы, рассматриваемые как правые мультипликаторы, то в качестве допустимых подгрупп мы получим *двусторонние идеалы*.

Пример 6. Как уже указывалось, *модулем* называют каждую аддитивно записанную абелеву группу. Модуль тоже может обладать областью операторов; в этом случае она называется также *областью мультипликаторов*. Тогда имеем:

$$\theta(a + b) = \theta a + \theta b.$$

Большей частью принимают, что область мультипликаторов образует кольцо, причём

$$(2) \quad \begin{cases} (\eta + \theta)a = \eta a + \theta a, \\ (\eta\theta)a = \eta(\theta a), \end{cases}$$

[а если мультипликаторы записываются справа, то, соответственно, $a(\eta\theta) = (a\eta)\theta$]. Тогда легко устанавливается, что $(\eta - \theta)a = \eta a - \theta a$

и $0 \cdot a = 0$ (где первый нуль есть нуль кольца, а второй — нуль модуля). Модуль с кольцом мультипликаторов $\mathfrak{o}$ называют *o-модулем* или *модулем относительно кольца $\mathfrak{o}$* . Если кольцо мультипликаторов обладает единицей e , то очень часто принимают, что она является одновременно «единичным оператором», т. е. что $e \cdot a = a$ для всех a из $\mathfrak{G}$.

Пример 7. Каждый модуль допускает в качестве мультипликаторов обыкновенные целые числа n в смысле обыкновенного умножения, ибо

$$n(a + b) = na + nb.$$

При этом допустимыми являются все подмодули.

Пример 8. Совокупность всех эндоморфизмов абелевой группы (т. е. всех ее гомоморфных отображений на себя или на собственные подмножества) является областью операторов, которую можно сделать кольцом, определив сумму и произведение двух эндоморфизмов формулами (2) (в первой из которых плюс в правой части обозначает композицию элементов группы). Это кольцо называется *кольцом эндоморфизмов* ¹⁾ абелевой группы.

Из этих примеров ясно, сколь широка область применения групп с операторами. Дальнейшие примеры см. в главе «Линейная алгебра» (часть II).

Задача 1. Пересечение двух допустимых подгрупп есть снова допустимая подгруппа. Аналогичное утверждение верно и для допустимых нормальных делителей.

Задача 2. Произведение AB двух перестановочных друг с другом допустимых подгрупп есть снова допустимая подгруппа. В специальном случае модулей: сумма $(\mathfrak{A}, \mathfrak{B})$ двух допустимых подмодулей есть снова допустимый подмодуль.

§ 44. Операторные изоморфизм и гомоморфизм.

Пусть $\mathfrak{G}$ и $\overline{\mathfrak{G}}$ — группы с общей областью операторов $\mathfrak{Q}$. Отображение группы $\mathfrak{G}$ на подмножество группы $\overline{\mathfrak{G}}$, относящее каждому элементу a из $\mathfrak{G}$ некоторый элемент $\bar{a}$ из $\overline{\mathfrak{G}}$ так, что произведению ab отвечает произведение $\bar{a}\bar{b}$ и каждому θa — соответствующее $\theta \bar{a}$, называется *операторным гомоморфизмом*. Если образом группы $\mathfrak{G}$ является вся группа $\overline{\mathfrak{G}}$, т. е. если каждый элемент из $\overline{\mathfrak{G}}$ отвечает по меньшей мере одному элементу из $\mathfrak{G}$, то имеем гомоморфное отображение $\mathfrak{G}$ на $\overline{\mathfrak{G}}$, в общем же случае, напротив, отображение $\mathfrak{G}$ в $\overline{\mathfrak{G}}$. Если каждое $\bar{a}$ отвечает только одному a , то имеем *операторный изоморфизм*.

¹⁾ Раньше употреблялся менее точный термин «кольцо автоморфизмов».

Для операторного гомоморфизма мы будем пользоваться обозначением $\mathfrak{G} \sim \overline{\mathfrak{G}}$, для операторного изоморфизма — обозначением $\mathfrak{G} \cong \overline{\mathfrak{G}}$.

Если $\mathfrak{N}$ — допустимый нормальный делитель группы $\mathfrak{G}$, то элементы ab смежного класса $\overline{a} = a\mathfrak{N}$ под действием оператора θ переходят в элементы $\theta a \cdot \theta b$, т. е. в элементы смежного класса $\theta a \cdot \mathfrak{N}$. Этот смежный класс $\overline{\theta a}$ мы будем называть произведением оператора θ на смежный класс $\overline{a}$. Тем самым факторгруппа $\mathfrak{G}/\mathfrak{N}$ становится группой с той же областью операторов Ω , причём соответствие $a \rightarrow \overline{a}$ является операторным гомоморфизмом.

Исходя, обратно, от операторного гомоморфизма, мы, как в § 10, получим теорему о гомоморфизмах:

Если $\mathfrak{G} \sim \overline{\mathfrak{G}}$, то множество $\mathfrak{N}$ тех элементов группы $\mathfrak{G}$, которым соответствует единица в $\overline{\mathfrak{G}}$, является допустимым нормальным делителем в $\mathfrak{G}$, и смежным классам по $\mathfrak{N}$ взаимно однозначно и операторно изоморфно соответствуют элементы из $\overline{\mathfrak{G}}$:

$$\mathfrak{G}/\mathfrak{N} \cong \overline{\mathfrak{G}}.$$

Что $\mathfrak{N}$ есть нормальный делитель — мы знаем уже из § 10. Что этот нормальный делитель $\mathfrak{N}$ является допустимым — ясно, ибо если a отображается в единицу $\overline{e}$ из $\overline{\mathfrak{G}}$, то θa отображается в $\overline{\theta e} = \overline{e}$, т. е. вместе с a также θa принадлежит к $\mathfrak{N}$. Что соответствие между смежными классами из $\mathfrak{G}$ и элементами из $\overline{\mathfrak{G}}$ взаимно однозначно, — мы уже знаем; то же, что это соответствие является операторным изоморфизмом, следует из того, что заданное соответствие $\mathfrak{G} \rightarrow \overline{\mathfrak{G}}$ было операторным гомоморфизмом.

В случае аддитивно записываемых групп с областью операторов $\mathfrak{o}$ ($\mathfrak{o}$ -модулей, в частности идеалов в $\mathfrak{o}$) операторный гомоморфизм называют также *модулярным гомоморфизмом*. Заметим, что при таком гомоморфизме θa переходит в $\overline{\theta a}$, т. е. θ не подвергается преобразованию; в этом — различие между гомоморфизмом модулей и гомоморфизмом колец, при котором ab переходит в $\overline{a\overline{b}}$. Приведём пример. Два левых идеала из кольца $\mathfrak{o}$ можно рассматривать как $\mathfrak{o}$ -модули; тогда операторный гомоморфизм между ними относит каждому a из одного идеала некоторое $\overline{a}$ из другого и произведению ga — произведению $\overline{ga}$ (для всех g из $\mathfrak{o}$). Но эти идеалы можно также рассматривать как кольца; при гомоморфизме же этих колец произведению ga (для всех g из идеала) будет соответствовать не $\overline{ga}$, а $\overline{g\overline{a}}$.

Все дальнейшие рассмотрения, где речь идёт просто о «группах», будут относиться также к группам с операторами. Под «подгруппами» и «нормальными делителями» будем тогда подразумевать допустимые подгруппы и допустимые нормальные делители, а под «изо-» и «гомоморфизмами» — операторные изо- и гомоморфизмы. В двух

ближайших параграфов мы будем опираться исключительно на теорему о гомоморфизмах и на то, что пересечение двух допустимых подгрупп, равно как и произведение двух перестановочных друг с другом допустимых подгрупп (в частности, произведение нормального делителя и подгруппы) снова являются допустимыми подгруппами.

Задача 1. Идеалы (1) и (2) в кольце целых чисел изоморфны как модули, но не изоморфны как кольца.

Задача 2. В кольце числовых пар (a_1, a_2) (§ 11, задача 1) идеалы, порождённые парами $(1, 0)$ и $(0, 1)$, изоморфны как кольца, но не изоморфны операторно.

§ 45. Две теоремы об изоморфизмах.

При гомоморфизме $\mathfrak{G} \sim \overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ каждая подгруппа $\mathfrak{H}$ группы $\mathfrak{G}$ гомоморфно отображается на некоторую подгруппу $\overline{\mathfrak{H}}$ группы $\overline{\mathfrak{G}}$. Если же мы теперь, наоборот, будем исходить из $\overline{\mathfrak{H}}$ и образуем совокупность $\mathfrak{H}$ всех тех элементов, образы которых (или смежные классы) принадлежат к $\overline{\mathfrak{H}}$, то при известных условиях $\mathfrak{H}$ сможет содержать больше элементов, чем $\mathfrak{H}$, поскольку в $\mathfrak{H}$ вместе с каждым элементом a из $\mathfrak{H}$ должны содержаться и все элементы смежного класса $a\mathfrak{N}$. Обозначив через $\mathfrak{H}\mathfrak{N}$ группу, образованную всеми произведениями ab элементов a из $\mathfrak{H}$ и элементов b из $\mathfrak{N}$ (см. задачу 2, § 43), будем иметь: $\mathfrak{H} = \mathfrak{H}\mathfrak{N}$ и, далее, $\overline{\mathfrak{H}} = \overline{\mathfrak{H}\mathfrak{N}/\mathfrak{N}}$. С другой стороны, $\mathfrak{H}$ гомоморфно отображается на $\overline{\mathfrak{H}}$, так что $\overline{\mathfrak{H}}$ изоморфна факторгруппе группы $\mathfrak{H}$ по её нормальному делителю, образованному теми элементами из $\mathfrak{H}$, которые переходят в единицу из $\overline{\mathfrak{H}}$, т. е. теми элементами из $\mathfrak{H}$, которые одновременно содержатся в $\mathfrak{N}$. Это даёт первую теорему об изоморфизмах:

Если $\mathfrak{N}$ — нормальный делитель и $\mathfrak{H}$ — подгруппа группы $\mathfrak{G}$, то пересечение $\mathfrak{H} \cap \mathfrak{N}$ является нормальным делителем в $\mathfrak{H}$, и¹⁾.

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N} \cong \mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N}).$$

Совокупность элементов, отображающихся на $\overline{\mathfrak{H}}$, будет совпадать с $\mathfrak{H}$ тогда и только тогда, когда $\mathfrak{H}$ вместе с каждым a содержит также весь смежный класс $a\mathfrak{N}$, т. е. когда $\mathfrak{H} \supseteq \mathfrak{N}$. Тем самым этим подгруппам $\mathfrak{H} \supseteq \mathfrak{N}$ взаимно однозначно соответствуют некоторые подгруппы $\overline{\mathfrak{H}} = \mathfrak{H}/\mathfrak{N}$ в $\overline{\mathfrak{G}}$. При этом каждая подгруппа $\overline{\mathfrak{H}}$ из $\overline{\mathfrak{G}}$ определяет одну подгруппу $\mathfrak{H} \supseteq \mathfrak{N}$, а именно, образованную всеми элементами всех входящих в $\overline{\mathfrak{H}}$ смежных классов по $\mathfrak{N}$. Наконец, правым и левым смежным классам группы $\mathfrak{G}$ по подгруппе $\mathfrak{N}$ соответствуют правые, соответственно левые, смежные классы группы $\overline{\mathfrak{G}}$.

¹⁾ Разумеется, для модулей вместо $\mathfrak{H}\mathfrak{N}$ следует писать $(\mathfrak{H}, \mathfrak{N})$.

по указанной полной подгруппе $\mathfrak{H}$. Таким образом, если $\overline{\mathfrak{H}}$ — нормальный делитель в $\overline{\mathfrak{G}}$, то и $\mathfrak{H}$ есть нормальный делитель в $\mathfrak{G}$, и обратно. Это же получается иным путём также при доказательстве второй теоремы об изоморфизмах.

Если $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ и $\overline{\mathfrak{H}}$ — нормальный делитель в $\overline{\mathfrak{G}}$, то соответствующая ему полная подгруппа $\mathfrak{H}$ является нормальным делителем в $\mathfrak{G}$, и

$$(1) \quad \mathfrak{G}/\mathfrak{H} \cong \overline{\mathfrak{G}}/\overline{\mathfrak{H}}.$$

Доказательство. Имеем $\mathfrak{G} \sim \overline{\mathfrak{G}}$ и $\overline{\mathfrak{G}} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$, следовательно, $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{H}$. Таким образом, $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ изоморфно факторгруппе группы $\mathfrak{G}$ по нормальному делителю, образованному теми элементами из $\mathfrak{G}$, которым при гомоморфизме $\mathfrak{G} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ соответствует единица, т. е. при первом гомоморфизме $\mathfrak{G} \sim \overline{\mathfrak{G}}$ — элементы из $\overline{\mathfrak{H}}$. Но этим нормальным делителем является $\mathfrak{H}$, что и требовалось доказать.

Изоморфизм (1) можно записать также следующим образом:

$$\mathfrak{G}/\mathfrak{H} \cong (\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}).$$

Задача 1. Показать с помощью первой теоремы об изоморфизмах, что факторгруппа симметрической группы $\mathfrak{S}_4$ по четверной группе $\mathfrak{B}_4$ (§ 9, задача 4) изоморфна симметрической группе $\mathfrak{S}_3$.

Задача 2. С помощью той же теоремы показать, что в каждой группе подстановок, содержащей хотя бы одну нечётную подстановку, чётные подстановки образуют нормальный делитель индекса 2.

Задача 3. С помощью той же теоремы показать, что факторгруппа группы евклидовых движений по нормальному делителю, образованному параллельными переносами, изоморфна группе поворотов вокруг одной точки.

§ 46. Нормальные и композиционные ряды.

Группа $\mathfrak{G}$ называется *простой*, если она не обладает нормальными делителями, отличными от неё самой и от единичной подгруппы.

Примеры. Группы простого порядка являются простыми, так как порядок подгруппы должен служить делителем порядка всей группы, так что кроме неё самой и единичной подгруппы у неё нет вообще никаких подгрупп, а потому и нормальных делителей. Позже будет показано, что также знакопеременные группы $\mathfrak{A}_n$ при $n > 4$ являются простыми (§ 48); далее, простой группой является каждый одночленный модуль, имеющий областью мультипликаторов поле, и т. д.

Конечный ряд подгрупп группы $\mathfrak{G}$:

$$(1) \quad \{\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \dots \supseteq \mathfrak{G}_r = \mathfrak{E}\},$$

где каждая подгруппа $\mathbb{G}_v$, $v=1, \dots, l$, является нормальным делителем предшествующей подгруппы $\mathbb{G}_{v-1}$, называется *нормальным рядом*. Число l называется *длиной* нормального ряда; факторгруппы $\mathbb{G}_{v-1}/\mathbb{G}_v$ называются *факторами* нормального ряда. Отметим, что длиной ряда (1) является не число его членов, а число факторов $\mathbb{G}_{v-1}/\mathbb{G}_v$.

Нормальный ряд

$$(2) \quad \{\mathbb{G} \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_m = \mathbb{E}\}$$

называется *уплотнением* нормального ряда (1), если все $\mathbb{G}_i$ из (1) содержатся также в (2). Так, например, для группы $\mathbb{S}_4$ (§ 6) ряд

$$\{\mathbb{S}_4 \supset \mathbb{A}_4 \supset \mathbb{V}_4 \supset \mathbb{E}\}$$

(ср. § 9, задача 4) есть уплотнение ряда

$$\{\mathbb{S}_4 \supset \mathbb{V}_4 \supset \mathbb{E}\}.$$

Члены в нормальном ряду могут, вообще говоря, повторяться сколько угодно раз подряд: $\mathbb{G}_i = \mathbb{G}_{i+1} = \dots = \mathbb{G}_k$. Нормальные ряды, в которых это не имеет места, называют нормальными рядами *без повторений*. Ряд без повторений, который нельзя уже далее уплотнить без повторений, называется композиционным рядом. Так, например, в симметрической группе $\mathbb{S}_3$ ряд

$$\{\mathbb{S}_3 \supset \mathbb{A}_3 \supset \mathbb{E}\},$$

равно как и в симметрической группе $\mathbb{S}_4$ ряд

$$\{\mathbb{S}_4 \supset \mathbb{A}_4 \supset \mathbb{V}_4 \supset \{1, (12)(34)\} \supset \mathbb{E}\},$$

являются композиционными рядами. В обоих случаях невозможность дальнейшего уплотнения следует из того, что индексом каждого нормального делителя в предшествующем является простое число. Существуют, однако, и такие группы, в которых каждый нормальный ряд может быть уплотнён (без повторений); эти группы, таким образом, вовсе не обладают композиционными рядами. Примером может служить бесконечная циклическая группа $\{a\}$; действительно, если в ней задан нормальный ряд без повторений

$$\{\mathbb{G} \supset \mathbb{G}_1 \supset \dots \supset \mathbb{G}_{l-1} \supset \mathbb{E}\}$$

и $\mathbb{G}_{l-1}$ имеет, скажем, индекс m , так что $\mathbb{G}_{l-1} = \{a^m\}$, то между $\mathbb{G}_{l-1}$ и $\mathbb{E}$ всегда можно вставить ещё подгруппу $\{a^{2m}\}$ индекса $2m$.

Нормальный ряд является композиционным тогда и только тогда, если, какие бы мы ни взяли соседние его члены $\mathbb{G}_{v-1}$ и $\mathbb{G}_v$, между ними нельзя вставить отличного от них нормального делителя члена $\mathbb{G}_{v-1}$, или, что, согласно § 45, сводится к тому же, если все факторы $\mathbb{G}_{v-1}/\mathbb{G}_v$ являются простыми. Простые факторы $\mathbb{G}_{v-1}/\mathbb{G}_v$ композиционного ряда называются *композиционными факторами*. В обоих

у $\mathbb{G}_{v-1}/\mathbb{G}_v \cong \mathbb{Z}_m$
 $\mathbb{Z}_m$ — простое
 $\mathbb{Z}_m$ — простое
 $\mathbb{Z}_m$ — простое
 $\mathbb{Z}_m$ — простое
 $\mathbb{Z}_m$ — простое

т.е. $\mathbb{Z}_m$ — простое делитель $\mathbb{Z}_m$

приведённых выше композиционных рядах все композиционные факторы суть циклические группы порядков 2, 3, соответственно 2, 3, 2, 2.

Два нормальных ряда называются *изоморфными*, если все факторы $\mathbb{G}_{\nu-1}/\mathbb{G}_{\nu}$ одного ряда изоморфны, в каком-то (произвольном) порядке, факторам другого ряда. Так, например, в циклической группе $\{a\}$ шестого порядка ряды

$$\{\{a\}, \{a^2\}, \mathbb{E}\}$$

и

$$\{\{a\}, \{a^3\}, \mathbb{E}\}$$

изоморфны, ибо факторами первого ряда служат циклические группы порядков 2, 3, а факторами второго ряда — циклические группы порядков 3, 2.

Для обозначения изоморфизма нормальных рядов мы будем в дальнейшем ради удобства пользоваться тем же символом $\cong$.

Последовательность подгрупп

$$\{\mathbb{G} \cong \mathbb{G}_1 \cong \dots\},$$

каждая из которых является нормальным делителем предыдущей, заканчивающуюся каким-либо нормальным делителем $\mathcal{A}$ группы $\mathbb{G}$, который может и не совпадать с $\mathbb{G}$, называют *нормальным рядом $\mathbb{G}$ по $\mathcal{A}$* . Ему соответствует нормальный ряд

$$\{\mathbb{G}/\mathcal{A} \cong \mathbb{G}_1/\mathcal{A} \cong \dots \cong \mathcal{A}/\mathcal{A} = \mathbb{E}\}$$

факторгруппы $\mathbb{G}/\mathcal{A}$, и обратно. При этом факторы второго ряда, по второй теореме об изоморфизмах, изоморфны факторам первого ряда.

Если два нормальных ряда

$$\{\mathbb{G} \cong \mathbb{G}_1 \cong \dots \cong \mathbb{G}_r = \mathbb{E}\}$$

и

$$\{\mathbb{G} \cong \mathbb{G}_1 \cong \dots \cong \mathbb{G}_r = \mathbb{E}\}$$

изоморфны, то для каждого уплотнения первого ряда можно найти изоморфное ему уплотнение второго ряда. Действительно, каждый фактор $\mathbb{G}_{\nu-1}/\mathbb{G}_{\nu}$ изоморфен некоторому вполне определённому фактору $\mathbb{G}_{\mu-1}/\mathbb{G}_{\mu}$; тем самым каждому нормальному ряду для $\mathbb{G}_{\nu-1}/\mathbb{G}_{\nu}$ соответствует изоморфный нормальный ряд для $\mathbb{G}_{\mu-1}/\mathbb{G}_{\mu}$, и потому также каждому нормальному ряду $\mathbb{G}_{\nu-1}$ по $\mathbb{G}_{\nu}$ — изоморфный ряд $\mathbb{G}_{\mu-1}$ по $\mathbb{G}_{\mu}$.

Мы можем теперь доказать следующую, принадлежащую О. Шрайеру, основную теорему о нормальных рядах:
Любые два нормальных ряда произвольной группы $\mathbb{G}$:

$$\{\mathbb{G} \cong \mathbb{G}_1 \cong \mathbb{G}_2 \cong \dots \cong \mathbb{G}_r = \mathbb{E}\}$$

и

$$\{\mathbb{G} \cong \mathbb{G}_1 \cong \mathbb{G}_2 \cong \dots \cong \mathbb{G}_r = \mathbb{E}\}$$

обладают изоморфными уплотнениями:

$$\{\mathbb{G} \supseteq \dots \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}\} \cong \{\mathbb{G} \supseteq \dots \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}\}.$$

Доказательство. Для $r=1$ или $s=1$ теорема очевидна; действительно, тогда одним из рядов является $\{\mathbb{G} \supseteq \mathbb{G}\}$, а второй ряд уже сам есть его уплотнение.

Мы сначала докажем теорему для $s=2$ полной индукцией по r , а затем для произвольного s полной индукцией по s .

При $s=2$ второй ряд имеет вид

$$\{\mathbb{G} \supseteq \mathbb{H} \supseteq \mathbb{G}\}.$$

Положим $\mathbb{D} = \mathbb{G}_1 \cap \mathbb{H}$ и $\mathbb{P} = \mathbb{G}_1 \mathbb{H}$. Очевидно, $\mathbb{P}$ и $\mathbb{D}$ — нормальные делители в $\mathbb{G}$; при этом, конечно, может случиться, что $\mathbb{P} = \mathbb{G}$ или $\mathbb{D} = \mathbb{G}$. Теперь, согласно предположению индукции, ряды

$$\{\mathbb{G}_1 \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}_r = \mathbb{G}\} \quad \text{и} \quad \{\mathbb{G}_1 \supseteq \mathbb{D} \supseteq \mathbb{G}\},$$

длины которых суть, соответственно, $r-1$ и 2, обладают изоморфными уплотнениями

$$(3) \quad \left\{ \begin{array}{l} \{\mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}\} \cong \\ \cong \{\mathbb{G}_1 \supseteq \dots \supseteq \mathbb{D} \supseteq \dots \supseteq \mathbb{G}\}. \end{array} \right.$$

Далее, на основании первой теоремы об изоморфизмах,

$$\mathbb{P}/\mathbb{H} \cong \mathbb{G}_1/\mathbb{D} \quad \text{и} \quad \mathbb{P}/\mathbb{G}_1 \cong \mathbb{H}/\mathbb{D},$$

и тем самым

$$(4) \quad \{\mathbb{P} \supseteq \mathbb{G}_1 \supseteq \mathbb{D} \supseteq \mathbb{G}\} \cong \{\mathbb{P} \supseteq \mathbb{H} \supseteq \mathbb{D} \supseteq \mathbb{G}\}.$$

Правая часть соотношения (3) определяет уплотнение левой части соотношения (4); для этого уплотнения существует изоморфное уплотнение правой части соотношения (4):

$$(5) \quad \left\{ \begin{array}{l} \{\mathbb{P} \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{D} \supseteq \dots \supseteq \mathbb{G}\} \cong \\ \cong \{\mathbb{P} \supseteq \dots \supseteq \mathbb{H} \supseteq \mathbb{D} \supseteq \dots \supseteq \mathbb{G}\}. \end{array} \right.$$

Из (3) и (5) следует:

$$\left\{ \begin{array}{l} \{\mathbb{G} \supseteq \mathbb{P} \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}\} \cong \\ \cong \{\mathbb{G} \supseteq \mathbb{P} \supseteq \dots \supseteq \mathbb{H} \supseteq \mathbb{D} \supseteq \dots \supseteq \mathbb{G}\}, \end{array} \right.$$

чем теорема и доказана для случая $s=2$.

Пусть теперь s произвольно, и теорема уже доказана для меньших значений s . По только что доказанному можно найти такое уплотнение первого ряда $\{\mathbb{G} \supseteq \mathbb{G}_1 \supseteq \dots\}$, которое было бы изоморфно некоторому уплотнению ряда $\{\mathbb{G} \supseteq \mathbb{H}_1 \supseteq \mathbb{G}\}$:

$$(6) \quad \left\{ \begin{array}{l} \{\mathbb{G} \supseteq \dots \supseteq \mathbb{G}_1 \supseteq \dots \supseteq \mathbb{G}_2 \supseteq \dots \supseteq \mathbb{G}\} \cong \\ \cong \{\mathbb{G} \supseteq \dots \supseteq \mathbb{H}_1 \supseteq \dots \supseteq \mathbb{G}\}. \end{array} \right.$$

По предположению индукции, часть $\{\mathfrak{G}_1 \cong \dots \cong \mathfrak{G}\}$ ряда, стоящего справа, и ряд $\{\mathfrak{G}_1 \cong \mathfrak{G}_2 \cong \dots \cong \mathfrak{G}_s = \mathfrak{G}\}$ обладают изоморфными уплотнениями:

$$(7) \quad \{\mathfrak{G}_1 \cong \dots \cong \mathfrak{G}\} \cong \{\mathfrak{G}_1 \cong \dots \cong \mathfrak{G}_2 \cong \dots \cong \mathfrak{G}\}.$$

Но ~~новая~~ ~~соотношения~~ (7) определяет уплотнение правой части соотношения (6), а для этого последнего уплотнения можно найти изоморфное уплотнение левой части соотношения (6). Таким образом,

$$\begin{aligned} \{\mathfrak{G} \cong \dots \cong \mathfrak{G}_1 \cong \dots \cong \mathfrak{G}_2 \cong \dots \cong \mathfrak{G}\} &\cong \\ &\cong \{\mathfrak{G} \cong \dots \cong \mathfrak{G}_1 \cong \dots \cong \mathfrak{G}\} \cong \\ &\cong \{\mathfrak{G} \cong \dots \cong \mathfrak{G}_1 \cong \dots \cong \mathfrak{G}_2 \cong \dots \cong \mathfrak{G}\} \text{ [в силу (7)].} \end{aligned}$$

Тем самым теорема полностью доказана ¹⁾.

Если в двух изоморфных рядах вычеркнуть все повторения, то останутся снова изоморфные ряды. Поэтому мы можем всегда считать уплотнения, о которых говорится в основной теореме, уплотнениями без повторений.

Из основной теоремы о нормальных рядах непосредственно вытекают следующие две теоремы для групп, обладающих композиционными рядами:

1. Теорема Жордана-Гельдера. Любые два композиционных ряда одной и той же группы $\mathfrak{G}$ изоморфны.

Действительно, эти ряды совпадают со своими уплотнениями, свободными от повторений.

2. Если группа $\mathfrak{G}$ обладает композиционным рядом, то каждый нормальный ряд этой группы может быть уплотнён до композиционного ряда; в частности, в этом случае через каждый нормальный делитель группы $\mathfrak{G}$ проходит композиционный ряд.

Группа, обладающая нормальным рядом, в котором все факторы абелевы, называется разрешимой. (Примеры: рассмотренные выше группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$.)

Из основной теоремы следует, что каждый нормальный ряд разрешимой группы может быть уплотнён до нормального ряда с абелевыми факторами. В частности, если разрешимая группа обладает композиционным рядом, то все композиционные факторы являются простыми абелевыми группами, т. е. в случае обыкновенных конечных групп — циклическими группами простого порядка (см. ниже задачу 3).

Задача 1. Каждая конечная группа обладает композиционным рядом.

Задача 2. Образовать все композиционные ряды циклической группы порядка 20. *(20, 10, 5, 4) и еще одна (20, 4)*

¹⁾ Другое доказательство теоремы дал Н. Zassenhaus, Abh. Math. Sem., Hamburg, 10 (1934), 106—108. Ред.

Задача 3. Абелева группа (без операторов) является простой лишь в том случае, если она циклическая простого порядка.

Задача 4. Группа порядка p^n является простой лишь при $n = 1$ [см. § 9; задача 9].

Задача 5. Каждая группа порядка p^n разрешима. [Образовать композиционный ряд и применить задачу 4.]

§ 47. Прямые произведения.

Группа $\mathfrak{G}$ называется прямым произведением её подгрупп $\mathfrak{A}$ и $\mathfrak{B}$, если выполнены следующие условия:

I. 1. $\mathfrak{A}$ и $\mathfrak{B}$ суть нормальные делители группы $\mathfrak{G}$.

I. 2. $\mathfrak{G} = \mathfrak{AB}$.

I. 3. $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{E}$.

Эти условия равносильны следующим:

II. 1. Каждый элемент группы $\mathfrak{G}$ может быть представлен в виде произведения

$$(1) \quad g = ab, \quad a \in \mathfrak{A}, \quad b \in \mathfrak{B}.$$

II. 2. Множители a и b однозначно определяются элементом g .

II. 3. Каждый элемент из $\mathfrak{A}$ перестановочен с каждым элементом из $\mathfrak{B}$.

Из I следует II. А именно, II. 1 следует из I. 2. II. 2 получается так: если $g = a_1 b_1 = a_2 b_2$, то $a_2^{-1} a_1 = b_2 b_1^{-1}$; таким образом, элемент $a_2^{-1} a_1$ должен принадлежать и к $\mathfrak{A}$, и к $\mathfrak{B}$, и потому, в силу I. 3, он должен быть равен единице; отсюда $a_1 = a_2$, $b_1 = b_2$, т. е. представление (1) однозначно. II. 3 следует из того, что элемент $aba^{-1}b^{-1}$, в силу I. 1, принадлежит и к $\mathfrak{A}$, и к $\mathfrak{B}$, и потому, в силу I. 3, равен единице.

Из II следует I. То, что $\mathfrak{A}$ есть нормальный делитель, получается из II. 1-и II. 3 так:

$$g \mathfrak{A} g^{-1} = ab \mathfrak{A} b^{-1} a^{-1} = ab b^{-1} \mathfrak{A} a^{-1} = a \mathfrak{A} a^{-1} = \mathfrak{A}.$$

I. 2 следует из II. 1. Наконец, I. 3 получается следующим образом. Элемент c пересечения $\mathfrak{A} \cap \mathfrak{B}$ можно представить в виде произведения элемента из $\mathfrak{A}$ и элемента из $\mathfrak{B}$ двумя способами:

$$c = c \cdot 1 = 1 \cdot c;$$

отсюда, вследствие единственности [II. 2], вытекает, что $c = 1$. Тем самым I. 3 доказано.

Произведение $\mathfrak{AB}$, когда оно является прямым, обозначают также символом $\mathfrak{A} \times \mathfrak{B}$. В случае аддитивных групп (модулей) пользуются обозначением $(\mathfrak{A}, \mathfrak{B})$ для суммы и $\mathfrak{A} + \mathfrak{B}$ для прямой суммы.

Если известна структура прямых множителей $\mathcal{A}$ и $\mathcal{B}$, то тем самым известна и структура их прямого произведения $\mathcal{G}$, ибо перемножение любых двух элементов $g_1 = a_1 b_1$ и $g_2 = a_2 b_2$ сводится к перемножению в отдельности их компонент:

$$g_1 g_2 = a_1 a_2 \cdot b_1 b_2.$$

Группа $\mathcal{G}$ называется *прямым произведением своих подгрупп* $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n$: $\mathcal{G} = \mathcal{A}_1 \times \mathcal{A}_2 \times \dots \times \mathcal{A}_n$, если выполнены следующие условия:

I'.1. Все $\mathcal{A}_i$ суть нормальные делители группы $\mathcal{G}$;

I'.2. $\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_n = \mathcal{G}$;

I'.3. $(\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{v-1}) \cap \mathcal{A}_v = \mathcal{E}$ ($v = 2, 3, \dots, n$).

При выполнении этих условий группы $\mathcal{A}_1, \dots, \mathcal{A}_{n-1}$ являются также нормальными делителями в их произведении $\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{n-1}$, и значит, это произведение по тому же самому определению — прямое; далее, $\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{n-1}$, как произведение нормальных делителей, в свою очередь есть нормальный делитель в $\mathcal{G}$, причём $(\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{n-1}) \cap \mathcal{A}_n = \mathcal{E}$, так что

$$(2) \quad \mathcal{G} = (\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{n-1}) \times \mathcal{A}_n = \mathcal{B}_n \times \mathcal{A}_n,$$

где

$$\mathcal{B}_n = \mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{n-1} = \mathcal{A}_1 \times \mathcal{A}_2 \times \dots \times \mathcal{A}_{n-1}.$$

Формула (2) может быть положена в основу рекуррентного определения прямого произведения n множителей. Применяя к $\mathcal{G} = \mathcal{B}_n \times \mathcal{A}_n$ эквивалентное с I' определение II, полной индукцией по n немедленно получаем:

II'. *Каждый элемент из $\mathcal{G}$ однозначно представим в виде произведения*

$$g = a_1 a_2 \dots a_n \quad (a_i \in \mathcal{A}_i),$$

причём каждый элемент из $\mathcal{A}_\mu$ перестановочен с каждым элементом из $\mathcal{A}_\nu$; $\mu, \nu = 1, 2, \dots, n$; $\mu \neq \nu$.

Обратно, из II' следует I'. Действительно, полагая

$$\mathcal{A}_1 \mathcal{A}_2 \dots \mathcal{A}_{v-1} \mathcal{A}_{v+1} \dots \mathcal{A}_n = \mathcal{B}_v,$$

получаем из II', что, для каждого v ,

$$(3) \quad \mathcal{G} = \mathcal{A}_v \times \mathcal{B}_v.$$

Тем самым каждое $\mathcal{A}_i$ является нормальным делителем группы $\mathcal{G}$ и

$$\mathcal{A}_i \cap \mathcal{B}_v = \mathcal{E}.$$

Последнее даёт даже несколько больше, чем условие I'.3.

Из (3) по первой теореме об изоморфизмах следует, что

$$\mathcal{G}/\mathcal{A}_v \cong \mathcal{B}_v, \quad \mathcal{G}/\mathcal{B}_v \cong \mathcal{A}_v.$$

делителем в $\mathcal{A}_k$ и, следовательно, либо $= \mathcal{A}_k$, либо $= \mathcal{G}$. В первом случае $\mathcal{A}_k \subset \Pi$ и, значит, множитель $\mathcal{A}_k$ в произведении $\Pi \cdot \mathcal{A}_k$ излишен. Во втором же случае $\Pi \cdot \mathcal{A}_k$ есть прямое произведение: $\Pi \cdot \mathcal{A}_k = \Pi \times \mathcal{A}_k$. Таким образом, произведение (5), после вычёркивания всех лишних $\mathcal{A}$, примет вид:

$$\mathcal{G} = \mathcal{G} \times \mathcal{A}_{i_1} \times \mathcal{A}_{i_2} \times \dots \times \mathcal{A}_{i_r}.$$

Отсюда и следует утверждение теоремы.

§ 48. Простота знакопеременной группы.

В § 46 мы видели, что симметрические группы $\mathcal{S}_3$, $\mathcal{S}_4$ разрешимы. В противоположность этому, все следующие симметрические группы $\mathcal{S}_n$ ($n > 4$) уже неразрешимы. Правда, они всегда имеют нормальный делитель индекса 2, а именно, знакопеременную группу $\mathcal{A}_n$, однако, композиционный ряд каждой из них переходит от $\mathcal{A}_n$ прямо к $\mathcal{G}$, ибо имеет место следующая

Теорема. Знакопеременная группа $\mathcal{A}_n$ ($n > 4$) является простой.

В основе доказательства этой теоремы лежит следующая

Лемма. Если нормальный делитель $\mathcal{N}$ группы $\mathcal{A}_n$ ($n > 2$) содержит трёхчленный цикл, то $\mathcal{N} = \mathcal{A}_n$.

Доказательство леммы. Если $n = 3$, то утверждение очевидно. Пусть поэтому $n > 3$ и пусть $\mathcal{N}$ содержит, скажем, цикл (123). Тогда в $\mathcal{N}$ должны содержаться как его квадрат (123)(123) = (213), так и все сопряжённые с ним (т.е. $\mathcal{N} \mathcal{N}^{-1}$).

$$\sigma \cdot (213) \cdot \sigma^{-1} \quad (\sigma \in \mathcal{A}_n).$$

Взяв $\sigma = (12)(3k)$, где $k > 3$, получим:

$$\sigma \cdot (213) \cdot \sigma^{-1} = (12k).$$

Таким образом, $\mathcal{N}$ содержит все циклы вида (12k). Но эти циклы порождают группу $\mathcal{A}_n$ (§ 7, задача 4). Следовательно, $\mathcal{N} = \mathcal{A}_n$.

Доказательство теоремы. Пусть $\mathcal{N}$ — отличный от $\mathcal{G}$ нормальный делитель группы $\mathcal{A}_n$. Мы покажем, что $\mathcal{N} = \mathcal{A}_n$.

Выберем в $\mathcal{N}$ подстановку τ , которая, не будучи тождественной, оставляет на месте наибольшее возможное при этом число номеров. Покажем, что τ переставляет точно три номера, оставляя все прочие на месте.

Действительно, предположим, что, в противоречие с нашим утверждением, τ переставляет больше чем три номера; тогда в разложении τ на циклы фактически фигурирует не менее четырёх номеров. При этом либо τ содержит цикл по меньшей мере из трёх номеров, либо τ состоит из одних лишь двухчленных циклов. В первом случае мы можем положить:

$$\tau = (123 \dots) \dots$$

Тогда τ переставляет по меньшей мере номера 1, 2, 3, 4, 5, поскольку подстановка (1234), как нечётная, не содержится в знакопеременной группе. Во втором случае положим

$$\tau = (12)(34) \dots$$

Трансформируя теперь τ с помощью подстановки $\sigma = (345)$, мы получим в первом случае

$$\tau_1 = \sigma\tau\sigma^{-1} = (124\dots) \dots;$$

во втором случае

$$\tau_1 = \sigma\tau\sigma^{-1} = (12)(45) \dots,$$

т. е. в обоих случаях $\tau_1 \neq \tau$ и тем самым $\tau^{-1}\tau_1 \neq 1$. Подстановка $\tau^{-1}\tau_1$ оставляет все номера $k > 5$ на месте, так как для них $\tau_1 k = \tau k$. Но эта подстановка оставляет на месте также номер 1, а во втором случае, кроме того, — и номер 2. Таким образом, в обоих случаях она оставляет на месте большее количество номеров, чем подстановка τ , что, однако, противоречит определению последней подстановки. Итак, τ может переставлять лишь три номера. Но тогда τ есть трёхчленный цикл, и в силу леммы $\mathcal{M} = \mathcal{M}_n$. Тем самым теорема доказана.

Задача. Доказать, что для $n \neq 4$ знакопеременная группа $\mathcal{M}_n$ является единственным нормальным делителем симметрической группы $\mathcal{S}_n$, отличным от самой $\mathcal{S}_n$ и $\mathcal{E}$. Если $n \neq 4$, то $\mathcal{M}_n = K \times \mathcal{E}$.

это и. г. $\mathcal{M}_n$ и $\mathcal{E}$. $\mathcal{M}_n$ — это не делитель $\mathcal{S}_n$.

§ 49. Транзитивность и примитивность.

Группа подстановок множества $\mathcal{M}$ называется транзитивной над $\mathcal{M}$, если в $\mathcal{M}$ существует элемент a , который с помощью подстановок этой группы переводится во все элементы x множества $\mathcal{M}$, иными словами, если для каждого x из $\mathcal{M}$ существует в группе такая подстановка σ , что $\sigma a = x$.

Если это условие выполнено, то и для любых двух элементов x, y из $\mathcal{M}$ существует в группе подстановка τ , переводящая x в y . Действительно, из

$$pa = x, \quad \sigma a = y$$

следует, что

$$(\sigma p^{-1})x = \sigma a = y.$$

Таким образом, для вопроса о транзитивности безразлично, от какого элемента a отправляться.

Если группа $\mathcal{G}$ не транзитивна над $\mathcal{M}$ (интранзитивная группа) то множество $\mathcal{M}$ распадается на «области транзитивности», т. е. на подмножества, которые рассматриваемой группой преобразуются, каждое, в себя и над которыми группа уже транзитивна. Это разбиение на подмножества производится по следующему принципу: два

элемента a, b множества M относятся в одно подмножество тогда и только тогда, когда в G существует подстановка σ , переводящая a в b .

Это свойство 1) рефлексивно, 2) симметрично и 3) транзитивно; действительно:

$$1) \sigma a = a \text{ для } \sigma = 1.$$

$$2) \text{ Из } \sigma a = b \text{ следует } \sigma^{-1} b = a.$$

$$3) \text{ Из } \sigma a = b, \tau b = c \text{ следует } (\tau\sigma) a = c.$$

Таким образом, указанный принцип действительно определяет разбиение множества M на классы.

Если группа G транзитивна над M и G_a — подгруппа тех элементов группы G , которые оставляют элемент a множества M на месте, то каждый левый смежный класс τG_a по подгруппе G_a переводит элемент a в единственный элемент τa . Как непосредственно видно из транзитивности группы G , таким путём определяется взаимно однозначное соответствие между этими левыми смежными классами и элементами множества M . Таким образом, число смежных классов (индекс подгруппы G_a) равно числу элементов множества M . Группой элементов из G , оставляющих инвариантным элемент a , служит

$$G_a = \tau G_a \tau^{-1}.$$

Транзитивная группа подстановок множества M называется импримитивной, если M можно разбить по крайней мере на два взаимно простых подмножества $M_1, M_2, \dots$, из которых хотя бы в одном содержится более одного элемента, таким образом, чтобы любая подстановка группы переводила каждое подмножество M_i в некоторое подмножество M_j . Множества $M_1, M_2, \dots$ называются тогда областями импримитивности. Если подобное разбиение

$$M = \{M_1, M_2, \dots\}$$

невозможно, то группа называется примитивной.

Примеры. Четверная группа Клейна импримитивна, с подмножествами

$$\{1, 2\}, \{3, 4\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}$$

в качестве областей импримитивности. (Возможны, впрочем, ещё два других разбиения на области импримитивности.) Напротив, полная (равно как и знакопеременная) группа подстановок n -й степени всегда примитивна; действительно, при любом разбиении множества M на подмножества, скажем,

$$M = \{\{1, 2, \dots, k\}, \{\dots\}, \dots\} \quad (1 < k < n)$$

существует подстановка, переводящая $\{1, 2, \dots, k\}$ в $\{1, 2, \dots, k-1, k+1\}$, т. е. в множество, не взаимно простое и не совпадающее с $\{1, 2, \dots, k\}$.

При разбиении $\mathcal{M} = \{M_1, \dots, M_r\}$, обладающем указанным свойством, т. е. таким, что группа $\mathcal{G}$ переставляет между собой множества M_i , для каждого v существует в группе подстановка, переводящая M_1 в M_v . А именно, для её нахождения достаточно, пользуясь транзитивностью группы, найти подстановку, переводящую произвольно выбранный элемент из M_1 в некоторый элемент из M_v ; эта подстановка может тогда перевести M_1 только в M_v . Отсюда, в частности, следует, что множества $M_1, M_2, \dots$ состоят все из одинакового числа элементов.

Для любой транзитивной группы $\mathcal{G}'$ подстановок множества $\mathcal{M}$ справедлива следующая теорема:

Пусть g — подгруппа, образованная всеми элементами группы $\mathcal{G}$, оставляющими инвариантным некоторый элемент a из M . Если группа $\mathcal{G}$ импримитивна, то существует группа h , заключённая между группами g и $\mathcal{G}$ и отличная от них:

$$g \subset h \subset \mathcal{G};$$

и обратно, если такая промежуточная группа h существует, то $\mathcal{G}$ импримитивна. Группа h оставляет инвариантной некоторую область импримитивности M_1 , а левые смежные классы группы $\mathcal{G}$ по подгруппе h переводят M_1 в другие области импримитивности M_v .

Доказательство. Пусть сперва $\mathcal{G}$ импримитивна, $\mathcal{M} = \{M_1, M_2, \dots\}$ — разбиение множества M на области импримитивности и a — какой-нибудь элемент из M_1 . Рассмотрим подгруппу h элементов из $\mathcal{G}$, оставляющих инвариантным множество M_1 . Согласно сделанному выше замечанию, h содержит все подстановки, переводящие a в себя или в другие элементы из M_1 ; следовательно, $g \subset h$ и $h \neq g$. Так как, вместе с тем, в $\mathcal{G}$ существуют также подстановки, переводящие M_1 , скажем, в M_2 , то $h \neq \mathcal{G}$. Наконец, если τ переводит M_1 в M_v , то и весь смежный класс τh переводит M_1 в M_v .

Пусть теперь, обратно, дана группа h , отличная от g и $\mathcal{G}$ и заключённая между ними:

$$g \subset h \subset \mathcal{G}.$$

$\mathcal{G}$ полностью распадается на смежные классы τh , а каждый из них, в свою очередь, — на смежные классы σg . Каждый из этих последних смежных классов σg переводит a в некоторый другой элемент σa ; следовательно, объединив эти классы в смежные классы τh , мы и элементы σa объединим по меньшей мере в два попарно взаимно простых множества $M_1, M_2, \dots$, каждое из которых будет состоять по меньшей мере из двух элементов. Таким образом, M , определяются как множества вида

(1)

$$M_i = \tau h a.$$

Каждая подстановка σ переводит $M_1 = \tau\eta a$ в $\sigma\tau\eta a$, т. е. снова в некоторое множество того же вида, чем и доказана импримитивность группы. Если мы обозначим через M_1 множество, получающееся из (1), скажем, при $\tau = 1$, то η будет оставлять область импримитивности M_1 неизменной (ибо $\eta M_1 = \eta\eta a = \eta a = M_1$), а смежные классы $\tau\eta$ будут переводить M_1 в остальные области импримитивности M , (ибо $\tau\eta M_1 = \tau\eta\eta a = \tau\eta a$).

Задача 1. Если число элементов множества M простое, то каждая транзитивная группа подстановок множества M примитивна.

Задача 2. Определённая выше группа η транзитивна над M_1 .

Задача 3. Пусть множество M разбито на три области импримитивности по два элемента в каждой, порядок же группы равен 12. Каков

a) индекс η в G ,

b) индекс g в η ,

c) порядок g ?

Задача 4. Порядок транзитивной группы подстановок конечного множества объектов делится на число этих объектов.

Замечание. Число переставляемых объектов называют также степенью группы подстановок; этот термин уже употреблялся выше для случая симметрических и знакопеременных групп.

Зад. 1. Раз M из простого числа, то ~~группа~~ ~~такая~~ ~~группа~~ ее нельзя разбить на подмножества из одинакового числа элементов, а это значит, что в случае импримитивности, образы импримитивности составляющие M , по числу элементов равны.

Зад. 2. η содержит все подстановки перемещающие a в a и такие a в любой другой элемент M . Но это значит, что вообще содержит все подстановки перемещающие любой элемент M , в любой другой элемент M , т. е. транзитивна.

ГЛАВА СЕДЬМАЯ.

ТЕОРИЯ ГАЛУА.

Теория Галуа занимается конечными сепарабельными расширениями поля K и особенно их изоморфизмами и автоморфизмами. Ею устанавливается связь между расширениями поля K , содержащимися в заданном нормальном поле над K , и подгруппами некоторой конечной группы. В этой теории находят ответ различные вопросы, относящиеся к решению алгебраических уравнений.

Всюду в этой главе поле K будет называться *основным* полем.

§ 50. Группа Галуа.

Согласно § 40, каждое конечное сепарабельное расширение Σ основного поля K порождается «примитивным элементом» ϑ : $\Sigma = K(\vartheta)$. Согласно § 38, Σ обладает в надлежаще выбранном расширении Ω столькими «относительными», т. е. оставляющими все элементы поля K на месте, изоморфизмами, какова степень n поля Σ относительно K . В качестве этого расширения Ω можно взять поле разложения неприводимого полинома $f(x)$, имеющего своим корнем ϑ . Это поле разложения является наименьшим нормальным относительно K полем, содержащим Σ , или, как мы будем также говорить, — *нормальным полем, соответствующим полю Σ* . Относительные изоморфизмы поля $K(\vartheta)$ характеризуются тем, что они переводят в поле Ω величину ϑ в сопряжённые величины $\vartheta_1, \dots, \vartheta_n$ ¹⁾. Каждый элемент $\varphi(\vartheta) = \sum a_\lambda \vartheta^\lambda$ ($a_\lambda \in K$) переходит при этом в $\varphi(\vartheta_i) = \sum a_\lambda \vartheta_i^\lambda$, так что вместо того, чтобы говорить об относительном изоморфизме, можно также говорить о *подстановке* $\vartheta \rightarrow \vartheta_i$.

Однако, следует отметить, что величины ϑ и ϑ_i суть лишь удобные вспомогательные средства для описания изоморфизмов, само же понятие изоморфизма совершенно не зависит от специального выбора ϑ . Изоморфизмы, как мы это ниже ещё увидим, можно строить и при задании поля несколькими образующими.

Если Σ само есть нормальное поле, то все сопряжённые поля $K(\vartheta_i)$ совпадают с Σ .

¹⁾ Разумеется, среди $\vartheta_1, \dots, \vartheta_n$ содержится и само ϑ .

Действительно, прежде всего, в этом случае все θ , содержащиеся в $K(\theta)$. Но поля $K(\theta_i)$ эквивалентны полю $K(\theta)$ и, значит, сами нормальны. Следовательно, и θ , в свою очередь, содержится в каждом $K(\theta_i)$.

Верно и обратное предложение:

Если Σ совпадает со всеми сопряжёнными полями $K(\theta_i)$, то Σ нормально.

Действительно, при этом предположении Σ совпадает с полем разложения $K(\theta_1, \dots, \theta_n)$ полинома $f(x)$ и, следовательно, является нормальным полем над K .

Отныне мы будем предполагать, что $\Sigma = K(\theta)$ — нормальное поле. Тогда изоморфизмы, переводящие Σ в сопряжённые поля $K(\theta_i)$, будут автоморфизмами поля Σ . Эти автоморфизмы поля Σ (оставляющие все элементы из K на месте), очевидно, образуют группу из n элементов, если в качестве умножения автоморфизмов принять их последовательное выполнение; её называют группой Галуа поля Σ относительно K . Эта группа будет играть основную роль в дальнейших наших рассуждениях. Обозначим её через G . Отметим, что порядок группы Галуа равен степени поля, $n = (\Sigma : K)$.

Если, как это иногда встречается, говорят о группе Галуа в случае конечного сепарабельного расширения Σ' , не являющегося нормальным, то под этим всегда подразумевается группа Галуа соответствующего нормального поля $\Sigma \supset \Sigma'$.

Для нахождения автоморфизмов отнюдь не требуется отыскивать сначала примитивный элемент θ поля Σ . Можно строить Σ также путём нескольких последовательных присоединений, скажем, в виде $\Sigma = K(\alpha_1, \dots, \alpha_m)$, и находить сначала изоморфизмы поля $K(\alpha_1)$, переводящие α_1 в сопряжённые величины, затем продолжать эти изоморфизмы до изоморфизмов поля $K(\alpha_1, \alpha_2)$, и т. д.

Важным частным случаем является тот, когда $\alpha_1, \dots, \alpha_m$ суть все корни уравнения $f(x) = 0^1$. Под группой Галуа уравнения $f(x) = 0$ или также полинома $f(x)$ понимают группу Галуа поля разложения $K(\alpha_1, \dots, \alpha_m)$ этого уравнения. Каждый относительный автоморфизм переводит систему корней саму в себя, т. е. каждый такой автоморфизм переставляет корни. Если эта перестановка известна, то известен также автоморфизм; действительно, если, например, $\alpha_1, \dots, \alpha_m$ переходят соответственно в $\alpha'_1, \dots, \alpha'_m$, то каждый элемент поля $K(\alpha_1, \dots, \alpha_m)$, как рациональная функция $\varphi(\alpha_1, \dots, \alpha_m)$, переходит в соответствующую функцию $\varphi(\alpha'_1, \dots, \alpha'_m)$. Таким образом, группой Галуа уравнения можно считать также некоторой группой подстановок его корней. Так мы и будем поступать всюду, где будет идти речь о группах Галуа уравнений.

Пусть Δ — «промежуточное поле»: $K \subseteq \Delta \subseteq \Sigma$. Согласно одной теореме § 35, каждый (относительный) изоморфизм поля Δ , перево-

¹⁾ $f(x)$ должен быть полиномом без кратных линейных множителей.

дающий Δ внутри Σ в сопряжённое поле Δ' , может быть продолжен до изоморфизма всего поля Σ , т. е. до элемента группы Галуа. Отсюда следует:

Два промежуточных поля Δ , Δ' тогда и только тогда сопряжены относительно основного поля K , если они могут быть переведены одна в другую с помощью некоторой подстановки из группы Галуа.

Таким же образом, взяв $\Delta = K(\alpha)$, получим:

Два элемента α , α' поля Σ тогда и только тогда сопряжены относительно основного поля K , если они могут быть переведены один в другой с помощью некоторой подстановки из группы Галуа поля Σ .

Число различных элементов, сопряжённых с величиной α поля Σ , равно степени неприводимого уравнения, корнем которого служит α . Если это число равно 1, то α есть корень линейного уравнения, т. е. содержится в K . Отсюда следует:

Если элемент α «выдерживает» все подстановки группы Галуа поля Σ , т. е. при всех этих подстановках переходит в себя, то α принадлежит основному полю K .

Из этих теорем уже видно, как велико значение группы автоморфизмов для изучения свойств поля. Эти теоремы, высказанные в целях удобства для конечных расширений, с помощью «трансфинитной индукции» без труда переносятся и на бесконечные расширения. Они сохраняют силу даже для несепарабельных расширений, если только степень поля заменить приведённой степенью поля, а утверждение последней теоремы заменить следующим: «то степень α^p , где p — характеристика, принадлежит основному полю K ». Напротив, «основная теорема теории Галуа», устанавливаемая в следующем параграфе, имеет место лишь для конечных сепарабельных расширений.

Расширение Σ основного поля K называют *абелевым*, если его группа Галуа абелева; *циклическим*, если группа циклична, и т. п. Равным образом и уравнение называют *абелевым*, *циклическим*, *примитивным*, если его группа Галуа, соответственно, абелева, циклична или (как группа подстановок корней) примитивна.

Особенно простой пример группы Галуа доставляет поле Галуа $GF(p^m)$ (§ 37), если в качестве основного поля взято содержащееся в нём простое поле Π . Рассмотренный в § 37 автоморфизм $s(\alpha \rightarrow \alpha^p)$ и степени его $s^2, s^3, \dots, s^m = 1$ оставляют все элементы из Π на месте и принадлежат поэтому к группе Галуа; а так как и степень поля равна m , то эти автоморфизмы исчерпывают всю группу Галуа. Таким образом, эта группа — циклическая порядка m .

Задача 1. Каждая рациональная функция корней уравнения, переходящая в себя при всех подстановках его группы Галуа, принадлежит основному полю, и обратно.

Задача 2. Группа Галуа уравнения $f(x) = 0$, не имеющего кратных корней, транзитивна (как группа подстановок корней; § 49)

тогда и только тогда, когда уравнение неприводимо в основном поле.

Задача 3. Какие возможности имеются для группы Галуа неприводимого уравнения третьей степени?

Задача 4. Группа Галуа уравнения в том и только в том случае состоит из одних лишь чётных подстановок, если квадратный корень из дискриминанта содержится в основном поле.

Задача 5. Установить группы Галуа уравнений

$$\begin{aligned}x^3 - 2 &= 0, \\ x^3 + 2x + 1 &= 0, \\ x^4 - 5x^2 + 6 &= 0,\end{aligned}$$

а также «уравнений деления круга»

$$\begin{aligned}x^4 + x^2 + 1 &= 0, \\ x^4 + 1 &= 0\end{aligned}$$

(во всех случаях — относительно поля рациональных чисел, как основного поля).

§ 51. Основная теорема теории Галуа.

«Основная теорема» гласит:

1) Каждому промежуточному полю Δ , $K \subseteq \Delta \subseteq \Sigma$, соответствует некоторая подгруппа $\mathfrak{g}$ группы Галуа $\mathfrak{G}$, а именно — совокупность тех автоморфизмов поля Σ , которые оставляют на месте все элементы из Δ . 2) Поле Δ однозначно определяется подгруппой $\mathfrak{g}$, а именно, Δ есть совокупность всех тех элементов поля Σ , которые «выдерживают» подстановки из $\mathfrak{g}$, т. е. остаются на месте при всех этих подстановках. 3) Каждой подгруппе $\mathfrak{g}$ группы $\mathfrak{G}$ соответствует поле Δ , связанное с $\mathfrak{g}$ указанным образом. 4) Порядок подгруппы $\mathfrak{g}$ равен степени поля Σ относительно Δ ; индекс подгруппы $\mathfrak{g}$ в $\mathfrak{G}$ равен степени поля Δ относительно основного поля K .

Доказательство. Совокупность автоморфизмов поля Σ , оставляющих на месте все элементы из Δ , представляет собой группу Галуа поля Σ относительно Δ и, значит, во всяком случае обладает групповыми свойствами. Тем самым утверждение 1) доказано. Утверждение 2) вытекает из последней теоремы § 50, применённой к Σ как надполю и Δ как основному полю. Несколько сложнее доказывается утверждение 3).

Пусть снова $\Sigma = K(\mathfrak{g})$ и $\mathfrak{g}$ — заданная подгруппа группы $\mathfrak{G}$. Обозначим через Δ совокупность всех элементов поля Σ , переходящих в себя при всех подстановках σ из $\mathfrak{g}$. Очевидно, Δ есть поле; действительно, если α и β остаются на месте при подстановке σ , то то же имеет место и для $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, а также, в случае

$\theta \neq 0$, для $\frac{\alpha}{\theta}$. Далее, имеем $K \subseteq \Delta \subseteq \Sigma$. Группа Галуа поля Σ относительно Δ содержит группу g , поскольку подстановки из g во всяком случае обладают свойством оставлять на месте элементы поля Δ . Если бы группа Галуа поля Σ относительно Δ содержала ещё элементы, не входящие в g , то и степень $(\Sigma : \Delta)$ была бы больше порядка подгруппы g . Эта степень $(\Sigma : \Delta)$ равна степени элемента θ относительно поля Δ , так как, очевидно, $\Sigma = \Delta(\theta)$. Но θ есть корень уравнения h -той степени

$$(1) \quad (x - \sigma_1 \theta)(x - \sigma_2 \theta) \dots (x - \sigma_h \theta) = 0,$$

где $\sigma_1, \sigma_2, \dots, \sigma_h$ — все подстановки из g . Коэффициенты этого уравнения инвариантны относительно подстановок группы g и потому принадлежат полю Δ . Следовательно, степень элемента θ относительно поля Δ не превышает порядка группы g .

Таким образом, остаётся заключить, что g есть вся группа Галуа поля Σ относительно Δ . Тем самым утверждение 3) доказано. (Причём попутно мы обнаружили неприводимость уравнения (1) в $\Delta[x]$.)

Наконец, если n — порядок группы $\mathfrak{G}$, h — снова порядок группы g , а j — индекс g в $\mathfrak{G}$, то имеем:

$$n = (\Sigma : K), \quad h = (\Sigma : \Delta), \quad n = h \cdot j,$$

$$(\Sigma : K) = (\Sigma : \Delta) \cdot (\Delta : K),$$

откуда

$$(\Delta : K) = j.$$

Тем самым доказано и утверждение 4).

По доказанной теперь основной теореме связь между подгруппами g группы Галуа и промежуточными полями взаимно однозначна. Возникает вопрос: как найти g по заданному Δ или Δ по заданной g ?

Первое сделать легко. Пусть уже найдены выражения для величин $\theta_1, \dots, \theta_n$, сопряжённых с θ , через θ ; тогда найдены и автоморфизмы $\theta \rightarrow \theta_i$, составляющие группу $\mathfrak{G}$. Если затем задано подполе $\Delta = K(\beta_1, \dots, \beta_k)$, где $\beta_1, \dots, \beta_k$ — известные выражения от θ , то g состоит просто из тех подстановок группы $\mathfrak{G}$, которые оставляют инвариантными $\beta_1, \dots, \beta_k$; действительно, эти подстановки будут оставлять инвариантными и все рациональные функции от $\beta_1, \dots, \beta_k$.

Пусть теперь, обратно, задана g ; образуем соответствующее произведение

$$(x - \sigma_1 \theta)(x - \sigma_2 \theta) \dots (x - \sigma_h \theta).$$

Как было выяснено при доказательстве основной теоремы, коэффициенты этого полинома должны лежать в Δ . Они даже порождают Δ ; действительно, они порождают поле, относительно которого элемент θ , как корень уравнения (1), уже имеет степень h , и потому оно не может быть собственным подполем поля Δ . Таким образом,

образующими поля Δ служат просто элементарные симметрические функции от $\sigma_1\theta, \dots, \sigma_h\theta$.

Другой метод построения поля Δ по подгруппе g состоит в том, что разыскивают величину $\chi(\theta)$, которая оставалась бы инвариантной при подстановках из g , но уже не выдерживала бы никакой другой подстановки из G . Эта величина $\chi(\theta)$, принадлежащая полю Δ , но уже не принадлежащая никакому его собственному подполю, и будет порождать поле Δ . Что такая величина всегда существует — следует, например, из теоремы о примитивном элементе (§ 40).

Основная теорема теории Галуа даёт возможность, как только известна группа Галуа, получить полный перечень всех промежуточных полей, заключённых между K и Σ . Число их, очевидно, конечно, ибо конечная группа обладает лишь конечным числом подгрупп. Но по группам можно узнать также, какие поля содержатся в каких, ибо имеет место следующая теорема:

Если Δ_1 — подполе поля Δ_2 , то группа g_2 , соответствующая полю Δ_2 , является подгруппой группы g_1 , соответствующей полю Δ_1 , и обратно.

Доказательство. Пусть сперва $\Delta_1 \subseteq \Delta_2$. Тогда каждая подстановка, оставляющая на месте все элементы из Δ_2 , оставляет на месте также все элементы из Δ_1 . *и. е. $g_2 \subseteq g_1$*

Пусть, с другой стороны, $g_1 \subseteq g_2$. Тогда каждый элемент поля, выдерживающий все подстановки из g_1 , выдерживает также все подстановки из g_2 . *$\Delta_1 \subseteq \Delta_2$*

В заключение рассмотрим ещё следующий вопрос: что произойдёт с группой Галуа поля $K(\theta)$ относительно K , если основное поле K расширить до некоторого поля Δ и соответственно расширить $K(\theta)$ до $\Delta(\theta)$? (При этом мы, разумеется, предполагаем, что поле $\Delta(\theta)$ имеет смысл, т. е. что Δ и θ содержатся в некотором общем надполе Ω .)

Подстановки $\theta \rightarrow \theta_i$, дающие после расширения автоморфизмы поля $\Delta(\theta)$, дают также изоморфизмы поля $K(\theta)$, и тем самым, так как $K(\theta)$ нормально, — автоморфизмы этого поля. Поэтому группа подстановок, получающаяся после расширения основного поля, является подгруппой первоначальной группы. Что эта подгруппа может быть собственной, мы усматриваем сразу, беря в качестве Δ поле, заключённое между K и $K(\theta)$. Но она может также совпадать с первоначальной группой; в этом случае говорят, что расширение основного поля не приводит группу поля $K(\theta)$.

Задача 1. Пересечению двух подгрупп группы Галуа G отвечает объединение соответствующих им полей, а объединению этих подгрупп — пересечение соответствующих полей¹⁾.

¹⁾ Объединение двух групп означает группу, порождённую объединением множеств элементов этих групп. Аналогично определяется понятие объединения полей.

Задача 2. Если поле Σ — циклическое степени n над K , то каждому делителю d числа n отвечает точно одно промежуточное поле Δ степени d , и из двух промежуточных полей тогда и только тогда одно содержится в другом, когда степень одного делится на степень другого (см. § 8, задача 6).

Задача 3. С помощью теории Галуа заново найти все подполя поля $GF(p^n)$ (§ 37).

Задача 4. Пусть $K \subseteq \Delta$ и $K(\theta)$ нормально над K . Показать, что группа Галуа поля $K(\theta)$ относительно K тогда и только тогда совпадает с группой Галуа поля $\Delta(\theta)$ относительно Δ , когда $K(\theta) \cap \Delta = K$.

Задача 5. С помощью теоремы § 49 показать, что поле $K(\alpha_1)$, получающееся путём присоединения корня неприводимого алгебраического уравнения, тогда и только тогда обладает подполем Δ таким, что

$$K \subset \Delta \subset K(\alpha_1),$$

когда группа Галуа уравнения, как группа подстановок корней, импримитивна. Тогда можно определить Δ , в частности, так, что степень поля $(\Delta:K)$ будет равна числу областей импримитивности и определяющее уравнение поля $K(\alpha_1)$ будет распадаться в Δ на неприводимые множители, соответствующие областям импримитивности.

Задача 6. Показать, что основная теорема имеет место также для несепарабельных расширений характеристики p , но со следующими изменениями. Утверждение 2) будет гласить: совокупность элементов поля Σ , выдерживающих подстановки из g , является «корневым полем поля Δ в поле Σ », т. е. совокупностью элементов поля Σ , обладающих тем свойством, что результат возведения их в некоторую степень p^r содержится в Δ . Утверждение 3) будет гласить: для каждой подгруппы g группы G можно найти точно одно поле Δ , инвариантное относительно операции извлечения корня p -той степени и выдерживающее подстановки из g и только их. Утверждение 4) верно с заменой степени приведённой степени.

В дополнении Р. Бэра и Х. Хассе к отмеченной во введении книге Штейнница доказано, что конечность, нормальность и сепарабельность поля Σ над K не только достаточны, но и необходимы для справедливости всех утверждений основной теоремы теории Галуа. Обобщение основной теоремы на случай бесконечных расширений даёт W. Kruil, *Math. Ann.*, 100 (1928), 687—698, на случай ненормальных и несепарабельных расширений — N. Jacobson, *Amer. J. Math.*, 66 (1944), 1—29, на случай модулей над полями (в смысле § 33) — R. Baer, *Amer. J. Math.*, 62 (1940), 551—588.

§ 52. Сопряжённые группы, поля и элементы полей.

Пусть снова $\mathfrak{G}$ — группа Галуа поля Σ относительно K и β — элемент из Σ . Подгруппа $\mathfrak{g}$ группы $\mathfrak{G}$, соответствующая промежуточному полю $K(\beta)$, состоит из всех подстановок, оставляющих β на месте. Остальные подстановки из $\mathfrak{G}$ преобразуют β в сопряжённые величины, причём каждая из этих величин может быть получена таким способом (§ 50). Мы утверждаем теперь далее:

Подстановки группы $\mathfrak{G}$, переводящие β в заданный сопряжённый с β элемент, образуют смежный класс $\tau\mathfrak{g}$ по подгруппе $\mathfrak{g}$, и каждый смежный класс переводит β в один и тот же сопряжённый элемент.

Доказательство. Если ρ и τ — подстановки, переводящие β в один и тот же сопряжённый элемент:

$$\rho(\beta) = \tau(\beta),$$

то

$$\tau^{-1}\rho(\beta) = \tau^{-1}\tau(\beta) = \beta;$$

следовательно $\tau^{-1}\rho = \sigma$ есть элемент из $\mathfrak{g}$, и $\rho = \tau\sigma$; тем самым ρ и τ лежат в одном и том же смежном классе $\tau\mathfrak{g}$. Обратно, если ρ и τ лежат в одном и том же смежном классе, т. е. оба в $\tau\mathfrak{g}$, то $\rho = \tau\sigma$, где σ лежит в $\mathfrak{g}$; тем самым

$$\rho(\beta) = \tau\sigma(\beta) = \tau(\sigma(\beta)) = \tau(\beta).$$

Из этой теоремы снова следует, что степень элемента β (= числу сопряжённых с β элементов) равна индексу подгруппы $\mathfrak{g}$ (= числу смежных классов).

Аutomорфизм τ , переводящий β в $\tau\beta$, переводит $K(\beta)$ в сопряжённое поле $K(\tau\beta)$. Мы утверждаем, что поле $K(\tau\beta)$ соответствует подгруппе $\tau\mathfrak{g}\tau^{-1}$.

Действительно, подгруппа, соответствующая полю $K(\tau\beta)$, состоит из подстановок σ' , оставляющих $\tau\beta$ на месте, так что

$$\sigma' = \tau\beta\tau^{-1},$$

или

$$\tau^{-1}\sigma'\tau = \beta,$$

или

$$\tau^{-1}\sigma'\tau = \sigma \in \mathfrak{g},$$

или

$$\sigma' = \tau\sigma\tau^{-1},$$

т. е. это и есть группа $\tau\mathfrak{g}\tau^{-1}$.

Таким образом, сопряжённым полям соответствуют сопряжённые группы.

Согласно § 50, поле Δ тогда и только тогда нормально относительно K , когда оно совпадает со всеми сопряжёнными полями. Отсюда теперь следует:

Поле Δ , $K \subseteq \Delta \subseteq \Sigma$, нормально тогда и только тогда, когда соответствующая ему группа $\mathfrak{G}$ совпадает со всеми сопряжёнными с ней в $\mathfrak{S}$ группами $\tau \mathfrak{G} \tau^{-1}$, т. е. когда $\mathfrak{g}$ является нормальным делителем в $\mathfrak{S}$.

Если теперь Δ нормально, то возникает вопрос: какова группа Галуа поля Δ относительно K ?

Каждый автоморфизм из $\mathfrak{S}$ преобразует Δ в себя и порождает, таким образом, некоторый автоморфизм из искомой группы Галуа поля Δ относительно K . При этом произведению двух автоморфизмов из $\mathfrak{S}$ отвечает снова произведение соответствующих автоморфизмов поля Δ , т. е. $\mathfrak{S}$ гомоморфно отображается на группу Галуа поля Δ . Элементами из $\mathfrak{S}$, которым отвечает тождественная подстановка в Δ , являются как раз элементы из $\mathfrak{g}$; отсюда по теореме о гомоморфизмах (§ 10) следует, что искомая группа изоморфна факторгруппе $\mathfrak{S}/\mathfrak{g}$. Итак:

Группа Галуа поля Δ относительно K изоморфна факторгруппе $\mathfrak{S}/\mathfrak{g}$.

Задача 1. Все подполя абелева поля нормальны и сами абелевы. Все подполя циклического поля сами цикличны.

Задача 2. Если $K \subseteq \Delta \subseteq \Sigma$ и Δ — наименьшее поле, содержащее Δ и нормальное относительно K , то группа, соответствующая полю Δ , является пересечением группы, соответствующей полю Δ , со всеми сопряжёнными с ней группами.

Задача 3. Определить подполя поля $\Gamma(\rho, \sqrt[3]{2})$, где Γ — поле рациональных чисел, принимаемое за основное поле, $\rho = \frac{-1 - \sqrt{-3}}{2}$ — первообразный корень третьей степени из единицы. Каковы степени этих подполей? Какие подполя являются сопряжёнными, какие нормальны?

Задача 4. Те же вопросы для поля $\Gamma(\sqrt{2}, \sqrt{5})$.

§ 53. Поля деления круга.

Пусть Γ — поле рациональных чисел, т. е. простое поле характеристики нуль. В этом случае уравнение

$$\Phi_h(x) = 0,$$

корнями которого служат все первообразные корни h -той степени из единицы, каждый с кратностью 1, и только они (см. § 36), называется уравнением деления круга, а поле, полученное путём присоединения к Γ корней h -той степени из единицы, называется полем деления круга или круговым полем. Введение этих терминов основывается на следующем. Комплексное число

$$\zeta_h = \cos \frac{2\pi}{h} + i \sin \frac{2\pi}{h}$$

является первообразным корнем h -той степени из единицы; из него равенством

$$2 \cos \frac{2\pi}{h} = \zeta + \zeta^{-1}$$

определяется $\cos \frac{2\pi}{h}$; а знание этого косинуса даёт возможность построить правильный h -угольник и, значит, разделить окружность на h равных дуг.

Излагаемая ниже теория полей деления круга, разумеется, не зависит от того, будем ли мы понимать под первообразным корнем из единицы ζ комплексное число или же простой символ.

Прежде всего нужно показать, что уравнение (1) неприводимо над Γ .

Пусть $f(x) = 0$ — неприводимое уравнение, которому удовлетворяет некоторый произвольно выбранный первообразный корень h -той степени из единицы ζ . При этом $f(x)$ можно считать целочисленным примитивным полиномом. Требуется показать, что $f(x) = \Phi_h(x)$.

Пусть p — простое число, не входящее в h . Тогда вместе с ζ также ζ^p является первообразным корнем h -той степени из единицы, удовлетворяя при этом некоторому целочисленному примитивному неприводимому уравнению $g(\zeta^p) = 0$. Покажем сперва, что $f(x) = \varepsilon g(x)$ где $\varepsilon = \pm 1$, т. е. ε — делитель единицы из кольца целых чисел.

Полином $x^h - 1$ имеет с $f(x)$ общий корень ζ и с $g(x)$ — общий корень ζ^p , а потому делится как на $f(x)$, так и на $g(x)$. Если бы $f(x)$ и $g(x)$ были существенно различны (т. е. отличались друг от друга не только делителем единицы), то $x^h - 1$ должен был бы делиться на произведение $f(x)g(x)$:

$$(2) \quad x^h - 1 = f(x)g(x)h(x),$$

где $h(x)$, согласно § 23, — снова целочисленный полином. Далее, полином $g(x^p)$, имеющий корнем ζ , должен делиться на $f(x)$:

$$(3) \quad g(x^p) = f(x)k(x),$$

где $k(x)$ — снова целочисленный полином.

Будем теперь рассматривать (2) и (3) как сравнения по модулю p .

$$g(x^p) \equiv \{g(x)\}^p$$

по модулю p . Действительно, если записать $g(x)$ в виде суммы степеней x без коэффициентов (заменяя, скажем, $2x^3$ на $x^3 + x^3$) и затем произвести возвышение $g(x)$ в степень p по правилам задачи § 30, т. е. путём возведения в p -тую степень каждого члена в отдельности, то мы получим как раз $g(x^p)$. Из формулы (3) следует поэтому:

$$\{g(x)\}^p \equiv f(x)k(x) \pmod{p}.$$

Представим себе теперь, что обе части формулы (4) разложены на неразложимые множители по модулю p . На основании теоремы об однозначном разложении полиномов с коэффициентами из поля $\mathbb{C}/(p)$ на простые множители (см. § 19), каждый простой множитель $\varphi(x)$ полинома $f(x)$ должен входить также в $\{g(x)\}^p$, а значит, и в $g(x)$. Поэтому правая часть формулы (2) делится по модулю p на $\{\varphi(x)\}^2$, следовательно, левая часть $x^h - 1$ и её производная hx^{h-1} обе должны делиться по модулю p на $\varphi(x)$. Но так как, по предположению, $h \not\equiv 0 \pmod{p}$, то hx^{h-1} имеет неприводимым множителем лишь x , который, однако, не входит в $x^h - 1$. Полученное противоречие и доказывает наше утверждение.

Таким образом, действительно, $f(x) = \pm g(x)$ и ζ^p есть корень полинома $f(x)$.

Покажем, далее, что все первообразные корни h -той степени из единицы являются корнями полинома $f(x)$. Пусть ζ^v такой первообразный корень, и

$$v = p_1 \dots p_n,$$

где p_i — простые множители числа v , одинаковые или различные, но во всяком случае взаимно простые с h .

Так как ζ удовлетворяет уравнению $f(x) = 0$, то по только что доказанному и ζ^{p_1} удовлетворяет этому уравнению. Повторяя то же рассуждение для простого множителя p_2 , заключаем, что и $\zeta^{p_1 p_2}$ удовлетворяет указанному уравнению. Продолжая этот процесс, получим (полная индукция!), что ζ^v удовлетворяет уравнению $f(x) = 0$.

Итак, все корни полинома $\Phi_h(x)$ удовлетворяют уравнению $f(x) = 0$; а так как полином $f(x)$ по предположению неприводим, полином же $\Phi_h(x)$ не имеет кратных корней, то заключаем, что

$$\Phi_h(x) = f(x).$$

Тем самым доказана неприводимость уравнения деления круга¹⁾.

Основываясь уже на одном этом обстоятельстве, можно без труда построить группу Галуа поля деления круга $\Gamma(\zeta)$.

Прежде всего, степень этого поля равна степени полинома $\Phi_h(x)$, т. е. равна $\varphi(h)$ (см. § 36). Автоморфизм поля $\Gamma(\zeta)$ задаётся указанием того корня полинома $\Phi_h(x)$, в который должен перейти ζ . Но корнями полинома $\Phi_h(x)$ являются все степени ζ^λ , где λ взаимно просто с h . Пусть σ_λ — автоморфизм, переводящий ζ в ζ^λ . Мы имеем

$$\sigma_\lambda = \sigma_\mu$$

тогда и только тогда, когда

$$\zeta^\lambda = \zeta^\mu$$

¹⁾ Другие простые доказательства см., например, в статье E. Landau и непосредственно за ней следующей статье I. Schur'a в *Math. Zeitschr.*, 29 (1929), 462—463.

или

$$\lambda \equiv \mu \pmod{h}.$$

Далее,

$$\sigma_{\lambda} \sigma_{\mu} (\zeta) = \sigma_{\lambda} (\zeta^{\mu}) = \{\sigma_{\lambda} (\zeta)\}^{\mu} = \zeta^{\mu \lambda}$$

и, значит,

$$\sigma_{\lambda} \sigma_{\mu} = \sigma_{\lambda \mu}.$$

Таким образом, группа автоморфизмов поля деления круга $\Gamma(\zeta)$ изоморфна группе классов вычетов по модулю n взаимно простых с n (см. § 19, задача 6).

Эта группа, в частности, абелева. Таким образом, все её подгруппы суть нормальные делители, а следовательно, все подполя поля $\Gamma(\zeta)$ — нормальны и абелевы.

Пример: корни двенадцатой степени из единицы. Классы вычетов, взаимно простые с 12, представляются числами

$$1, 5, 7, 11.$$

Мы можем поэтому обозначить автоморфизмы через $\sigma_1, \sigma_5, \sigma_7, \sigma_{11}$, причём автоморфизм σ_{λ} переводит ζ в ζ^{λ} . Таблица умножения такова:

σ_1	σ_5	σ_7	σ_{11}
σ_5	σ_1	σ_{11}	σ_7
σ_7	σ_{11}	σ_1	σ_5
σ_{11}	σ_7	σ_5	σ_1

Каждый элемент имеет порядок 2. Таким образом, кроме самой группы и единичной подгруппы имеются ещё три подгруппы:

$$1. \{ \sigma_1, \sigma_5 \},$$

$$2. \{ \sigma_1, \sigma_7 \},$$

$$3. \{ \sigma_1, \sigma_{11} \}.$$

Этим трём группам соответствуют квадратичные поля, порождаемые квадратными корнями. Нахождение этих полей основывается на следующих соображениях.

Корни четвёртой степени из единицы $\omega, \omega^3, \omega^5, \omega^6$ являются так же корнями двенадцатой степени из единицы и потому лежат в рассматриваемом поле. Таким образом, $\Gamma(\zeta)$ есть квадратичное подполе.

Точно так же и корни третьей степени из единицы лежат в поле. Так как

$$\rho = -\frac{1}{2} + \frac{1}{2} \sqrt{-3}$$

есть корень третьей степени из единицы, то и $\Gamma(\sqrt{-3})$ есть квадратичное подполе.

Перемножая квадратные корни l и $\sqrt{-3}$, получаем $\sqrt{3}$. Таким образом $\Gamma(\sqrt{3})$ есть третье квадратичное подполе.

Определим теперь, какие подгруппы соответствуют этим трём полям.

Так как $\sigma_6 \zeta^3 = \zeta^{15} = \zeta^3$, то $l = \zeta^3$ выдерживает автоморфизм σ_6 . Следовательно, поле $\Gamma(l)$ соответствует группе $\{\sigma_1, \sigma_6\}$.

Так как $\sigma_7 \zeta^4 = \zeta^{28} = \zeta^4$, то $\rho = \zeta^4$ выдерживает автоморфизм σ_7 . Следовательно, поле $\Gamma(\sqrt{-3})$ соответствует группе $\{\sigma_1, \sigma_7\}$.

Оставшееся ещё поле $\Gamma(\sqrt{3})$ должно соответствовать группе $\{\sigma_1, \sigma_{11}\}$.

Каждые два из этих трёх подполей порождают всё поле. Поэтому первообразный корень двенадцатой степени из единицы ζ должен выражаться через два квадратных корня. И действительно,

$$\zeta = \zeta^{-3} \zeta^4 = l^{-1} \rho = -l \frac{-1 + \sqrt{-3}}{2} = \frac{l - \sqrt{3}}{2}.$$

В следующем параграфе мы увидим, как можно определить все подполя поля деления круга с простым показателем и построить из этих подполей путём последовательных присоединений само поле.

Задача 1. Величина $\zeta + \zeta^{-1}$ при $h > 2$ порождает всегда подполе степени $\frac{1}{2} \varphi(h)$.

Задача 2. Определить группу и подполя поля корней пятой степени из единицы и выразить эти корни с помощью квадратных корней. То же для корней восьмой степени из единицы.

Задача 3. Определить группу и подполя поля корней седьмой степени из единицы. Каково определяющее уравнение поля $\Gamma(\zeta + \zeta^{-1})$?

§ 54. Периоды уравнения деления круга.

Пусть теперь показателем рассматриваемых корней из единицы будет простое число q . В этом случае уравнением деления круга будет

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \dots + x + 1 = 0.$$

Степень его $n = q - 1$.

Пусть ζ — первообразный корень q -той степени из единицы.

Группа классов вычетов, взаимно простых с q , циклическа (§ 37) и состоит поэтому из $\varphi(q)$ классов вычетов

$$1, g, g^2, \dots, g^{n-1},$$

где g — «первообразный корень по модулю q », т. е. примитивный корень сравнения $g^n \equiv 1 (q)$. Поэтому и группа Галуа циклическа.

и порождается тем автоморфизмом σ , который переводит ζ в ζ^q . Первообразные корни q -той степени из единицы могут быть представлены в виде

$$\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{n-1}}, \text{ где } \zeta^{q^n} = \zeta.$$

Положим

$$\zeta^{q^v} = \zeta_v;$$

числа v можно будет при вычислениях приводить по модулю n , так как

$$\zeta^{q^{v+n}} = \zeta^{q^v}.$$

Имеем:

$$\sigma(\zeta_i) = \sigma(\zeta^{q^i}) = \{\sigma(\zeta)\}^{q^i} = (\zeta^q)^{q^i} = \zeta^{q^{i+1}} = \zeta_{i+1}.$$

Таким образом автоморфизм σ увеличивает каждый индекс на 1. v -кратное применение автоморфизма σ даёт:

$$\sigma^v(\zeta_i) = \zeta_{i+v}.$$

Величины ζ_i ($i=0, 1, \dots, n-1$) образуют базис поля. Чтобы убедиться в этом, достаточно показать, что они линейно независимы. Но, действительно, ζ_i совпадают с точностью до порядка следования с $\zeta, \dots, \zeta^{q^{n-1}}$; таким образом, наличие линейного соотношения между ними означало бы, что

$$a_1\zeta + \dots + a_{q-1}\zeta^{q-1} = 0$$

или, по сокращении на ζ :

$$a_1 + a_2\zeta + \dots + a_{q-1}\zeta^{q-2} = 0.$$

Но так как ζ не может удовлетворять никакому уравнению степени $q-2$, то должно следовать, что

$$a_1 = a_2 = \dots = a_{q-1} = 0;$$

т. е. ζ_i линейно независимы.

Периоды уравнения деления круга непосредственно определяют структуру циклической группы; последние же задаются следующим образом (см. конец § 7):

Есть

$$n = ef$$

разложение n на взаимно простые множители e и f . Тогда элементы

$$\sigma^e, \sigma^{2e}, \dots, \sigma^{(f-1)e}, \sigma^e,$$

образуют подгруппу g порядка f . Каждая из них может быть получена таким способом.

Теперь элементы α , выдерживающие автоморфизм σ^e (а значит, и все автоморфизмы из подгруппы g). Если

$$\alpha = a_0\zeta_0 + a_1\zeta_1 + \dots + a_{n-1}\zeta_{n-1},$$

ТО

$$\sigma^e(\alpha) = a_0 \zeta_e + a_1 \zeta_{e+1} + \dots + a_{n-1} \zeta_{e+n-1}.$$

Для того чтобы последнее выражение было равно α , должны выполняться условия

$$a_0 = a_e,$$

$$\dots\dots\dots$$

$$a_v = a_{v+e},$$

$$\dots\dots\dots$$

$$a_{n-1} = a_{e+n-1}.$$

индексы следует брать по модулю n . Следовательно,

$$a_v = a_{v+e} = a_{v+2e} = \dots,$$

что члены выражения (1) можно объединить в группы

$$a_v (\zeta_v + \zeta_{v+e} + \dots).$$

В соответствии с этим положим

$$\eta_v = \zeta_v + \zeta_{v+e} + \zeta_{v+2e} + \dots + \zeta_{v+(f-1)e} \quad (v = 0, \dots, e-1),$$

после чего каждый элемент (1), выдерживающий автоморфизм σ^e , запишется в виде

$$\alpha = a_0 \eta_0 + a_1 \eta_1 + \dots + a_{e-1} \eta_{e-1}.$$

Это показывает, что η_i образуют базис подполя, соответствующего подгруппе g .

Так как

$$\sigma(\eta_0) = \eta_1,$$

$$\dots\dots\dots$$

$$\sigma^v(\eta_0) = \eta_v,$$

$$\dots\dots\dots$$

$\eta_0, \eta_1, \dots$ сопряжены и полином

$$f(x) = (x - \eta_0)(x - \eta_1) \dots (x - \eta_{e-1})$$

является

Но поле $\Gamma(\eta_0)$, как и всякое подполе поля $\Gamma(\zeta)$, нормально, так что полином (3) целиком распадается в нём на линейные множители. Следовательно,

$$\Gamma(\eta_0) = \Gamma(\eta_0, \dots, \eta_{e-1}),$$

т. е. требуемое подполе порождается уже элементом η_0 .

Величины $\eta_0, \dots, \eta_{e-1}$, определяемые формулами (2), называются Гауссу, f -членными периодами поля деления круга.

Гаусс предложил удобную формулу для вычисления произведения $\eta_i \eta_k$. Он ввёл новое обозначение:

$$\eta(r) = \zeta^r + \zeta^{rg^e} + \dots + \zeta^{r g^{(f-1)e}} = \sum_{v \bmod f} \zeta^{r g^{ve}}$$

(где запись « $v \bmod f$ » выражает, что v пробегает полную систему вычетов по модулю f). Таким образом, $\eta(r)$ при $r \not\equiv 0 \pmod{q}$ есть то η_i , в котором содержится член ζ^r . Заметим, что

$$\eta(r g^e) = \eta(r)$$

и

$$\eta(0) = 1 + \dots + 1 = f.$$

Перемножение двух $\eta(r)$ даёт теперь:

$$\eta(r) \eta(s) = \sum_{v \bmod f} \left(\sum_{\mu \bmod f} \zeta^{r g^{ve} + s g^{\mu e}} \right)$$

или, если положить $\mu = \mu' + v$:

$$\begin{aligned} \eta(r) \eta(s) &= \sum_{v \bmod f} \left(\sum_{\mu' \bmod f} \zeta^{r g^{ve} + s g^{(\mu'+v)e}} \right) = \\ &= \sum_{\mu' \bmod f} \left(\sum_{v \bmod f} \zeta^{r g^{ve} + s g^{(\mu'+v)e}} \right). \end{aligned}$$

Величина, стоящая в скобках, равна $\eta(r + s g^{\mu'e})$. Следовательно, заменяя μ на $\mu + s g^{\mu'e}$, имеем:

$$\eta(r) \eta(s) = \sum_{\mu \bmod f} \eta(r + s g^{\mu e}) \quad (\text{формула Гаусса})$$

Видно, что в этой сумме совпадают с показателями, которые получают, если первый член суммы $\eta(r)$ помножить на все члены суммы $\eta(s)$.

Из равенства

$$\zeta + \zeta^2 + \dots + \zeta^{q-1} = -1$$

следует ещё, что

$$\eta_0 + \eta_1 + \dots + \eta_{e-1} = -1,$$

и тем самым

$$\eta(0) = f = -f(\eta_0 + \eta_1 + \dots + \eta_{e-1}).$$

Это позволяет выразить все $\eta(0)$, входящие в правую часть формулы Гаусса, через $\eta_0, \eta_1, \dots, \eta_{e-1}$. Замечая, что остальные $\eta(i)$ с точностью до порядка нумерации совпадают с величинами $\eta_0, \eta_1, \dots, \eta_{e-1}$, мы получаем из формулы Гаусса для каждого произведения $\eta_i \eta_k$ представление в виде суммы целочисленных кратных от величин η_i .

Пример: $q = 17$. Число 3 является первообразным корнем, так как степени его по модулю 17 таковы:

Показатели:	0	1	2	3	4	5	6	7	8
Степени:	1	3	-8	-7	-4	5	-2	-6	-1
Показатели:	9	10	11	12	13	14	15	16	
Степени:	-3	8	7	4	-5	2	6	1	

Вычислим сначала *восьмичленные периоды* ($e=2, f=8$):

$$\begin{aligned}\eta_0 &= \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2, \\ \eta_1 &= \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5} + \zeta^6.\end{aligned}$$

Имеем: $\eta_0 + \eta_1 = -1$, и по формуле Гаусса (принимая во внимание, что $\eta_0 = \eta^{(1)}$, $\eta_1 = \eta^{(3)}$):

$$\eta_0 \eta_1 = \eta^{(4)} + \eta^{(-6)} + \eta^{(6)} + \eta^{(-5)} + \eta^{(-2)} + \eta^{(8)} + \eta^{(-4)} + \eta^{(7)}.$$

Но $\eta^{(r)}$ есть всегда то η , в которое входит ζ^r . Таким образом,

$$\begin{aligned}\eta^{(4)} &= \eta^{(-2)} = \eta^{(8)} = \eta^{(-4)} = \eta_0, \\ \eta^{(-6)} &= \eta^{(6)} = \eta^{(-5)} = \eta^{(7)} = \eta_1,\end{aligned}$$

и тем самым

$$\eta_0 \eta_1 = 4\eta_0 + 4\eta_1 = -4.$$

Итак, η_0 и η_1 суть корни уравнения

$$(4) \quad y^2 + y - 4 = 0;$$

решение его есть

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

Четырёхчленные периоды ($e=4, f=4$) суть:

$$\begin{aligned}\xi_0 &= \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4, \\ \xi_1 &= \zeta^3 + \zeta^5 + \zeta^{-8} + \zeta^{-5}, \\ \xi_2 &= \zeta^{-8} + \zeta^{-2} + \zeta^8 + \zeta^2, \\ \xi_3 &= \zeta^{-7} + \zeta^{-6} + \zeta^7 + \zeta^6.\end{aligned}$$

Имеем:

$$\begin{aligned}\xi_0 + \xi_2 &= \eta_0, \\ \xi_1 + \xi_3 &= \eta_1.\end{aligned}$$

Чтобы получить уравнение для ξ_0 и ξ_2 , вычислим $\xi_0 \xi_2$:

$$\xi_0 \xi_2 = \xi^{(-7)} + \xi^{(-1)} + \xi^{(-8)} + \xi^{(3)} = \xi_3 + \xi_0 + \xi_2 + \xi_1 = -1.$$

Следовательно, ξ_0 и ξ_2 удовлетворяют уравнению

$$(5) \quad x^2 - \eta_0 x - 1 = 0.$$

Аналогично, ξ_1 и ξ_3 удовлетворяют уравнению

$$(6) \quad x^2 - \eta_1 x - 1 = 0.$$

Эти уравнения выражают известное нам уже заранее обстоятельство, что поле $\Gamma(\xi_0)$ квадратично относительно $\Gamma(\eta_0)$.

Суммы

$$\lambda^{(1)} = \zeta + \zeta^{-1},$$

$$\lambda^{(4)} = \zeta^4 + \zeta^{-4}$$

представляют *двучленные периоды*. Сложение и перемножение их дают:

$$\lambda^{(1)} + \lambda^{(4)} = \xi_0,$$

$$\lambda^{(1)}\lambda^{(4)} = \zeta^5 + \zeta^{-5} + \zeta^3 + \zeta^{-3} = \xi_1.$$

Следовательно, $\lambda^{(1)}$ и $\lambda^{(4)}$ удовлетворяют уравнению

$$(7) \quad \Delta^2 - \xi_0\Delta + \xi_1 = 0.$$

Наконец, само ζ удовлетворяет уравнению

$$\zeta + \zeta^{-1} = \lambda^{(1)}$$

или

$$\zeta^2 - \lambda^{(1)}\zeta + 1 = 0.$$

Тем самым корни 17-й степени из единицы могут быть вычислены путём решения цепи квадратных уравнений.

Рассматривая, в частности, корни 17-й степени из единицы как числа, можно положить:

$$\zeta = e^{\frac{2\pi i}{17}},$$

$$\lambda^{(1)} = \zeta + \zeta^{-1} = 2 \cos \frac{2\pi}{17}.$$

Уравнение (4) имеет один положительный и один отрицательный корень. При этом, так как теперь

$$\eta_0 = (\zeta + \zeta^{-1}) + (\zeta^3 + \zeta^{-3}) + (\zeta^4 + \zeta^{-4}) + (\zeta^2 + \zeta^{-2}) =$$

$$= 2 \left(\cos \frac{2\pi}{17} + \cos \frac{16\pi}{17} + \cos \frac{8\pi}{17} + \cos \frac{4\pi}{17} \right) > 2 \left(\frac{1}{2} - 1 + 0 + \frac{1}{2} \right) = 0,$$

то η_0 есть положительный корень:

$$\eta_0 = -\frac{1}{2} + \frac{1}{2} \sqrt{17}.$$

Точно так же и уравнения (5) и (6) имеют по одному положительному и одному отрицательному корню; так как

$$\xi_0 = 2 \left(\cos \frac{2\pi}{17} + \cos \frac{8\pi}{17} \right) > 0,$$

$$\xi_9 = 2 \left(\cos \frac{14\pi}{17} + \cos \frac{12\pi}{17} \right) < 0,$$

то ξ_0 и ξ_1 суть положительные корни, соответственно, уравнений (5) и (6). Наконец,

$$\lambda^{(1)} = 2 \cos \frac{2\pi}{17} > 2 \cos \frac{8\pi}{17} = \lambda^{(4)},$$

т. е. $\lambda^{(1)}$ — наибольший из двух (положительных) корней уравнения (7). Опираясь на формулу $\lambda^{(1)} = \zeta + \zeta^{-1}$ и применяя к ней возведение в степень

правильного семнадцатиугольника с помощью циркуля и линейки (см. § 59).

Задача 1. Выполнить фактически построение правильного семнадцатиугольника.

Задача 2. Доказать для $\frac{p-1}{2}$ -членных периодов η_0 и η_1 в общем случае соотношения

$$\eta_0 + \eta_1 = -1,$$

$$\eta_0 \eta_1 = \frac{1+p}{4} \quad \text{для } p \equiv -1 \pmod{4},$$

$$\eta_0 \eta_1 = \frac{1-p}{4} \quad \text{для } p \equiv 1 \pmod{4},$$

и вывести отсюда квадратное уравнение для η_0 .

Задача 3. Величина η_0 задачи 2 есть «сумма Гаусса»:

$$\eta_0 = \sum_{s=1}^{\frac{p-1}{2}} \zeta^{s^2}.$$

§ 55. Циклические поля и двучленные уравнения.

Пусть K — основное поле, содержащее корни n -ной степени из единицы, причём $n \cdot 1 \neq 0$ (т. е. n не делится на характеристику поля). Мы утверждаем тогда, что группа Галуа двучленного уравнения

$$x^n - a = 0 \quad (a \neq 0)$$

циклическа.

Доказательство. Если ϑ — какой-нибудь корень рассматриваемого уравнения и ζ — первообразный корень n -ной степени из единицы, то $\zeta\vartheta, \zeta^2\vartheta, \dots, \zeta^{n-1}\vartheta$ суть остальные корни того же уравнения¹⁾. Поэтому уже ϑ порождает всё поле корней, и каждая подстановка группы Галуа имеет вид

$$\vartheta \rightarrow \zeta^v \vartheta.$$

Перемножение двух подстановок $\vartheta \rightarrow \zeta^v \vartheta$ и $\vartheta \rightarrow \zeta^w \vartheta$ даёт $\vartheta \rightarrow \zeta^{v+w} \vartheta$. Таким образом каждой подстановке соответствует определённый корень n -ной степени из единицы ζ^v , а произведению подстановок — произведение этих корней. Следовательно, группа Галуа изоморфна некоторой подгруппе группы корней n -ной степени из единицы. А так как эта последняя группа циклическа, то циклическа и каждая её подгруппа, а тем самым и рассматриваемая группа Галуа.

¹⁾ Очевидно, все эти корни различны, и тем самым уравнение сепарабельно.

Если, в частности, уравнение $x^n - a = 0$ неприводимо, то все корни $\zeta\theta$ сопряжены с θ и потому группа Галуа изоморфна полной группе корней n -ной степени из единицы. Порядок её в этом случае равен n .

Покажем теперь, обратно, что каждое циклическое поле n -ной степени относительно K порождается корнями некоторого двучленного уравнения $x^n - a = 0$.

Пусть $L = K(\theta)$ — циклическое поле степени n , и σ — образующая автоморфизмов его группы Галуа, так что $\sigma^n = 1$. Мы снова принимаем, что основное поле K содержит корни n -ной степени из единицы.

Пусть ζ — такой корень; образуем «резольвенту Лагранжа»:

$$(1) \quad (\zeta, \theta) = \theta_0 + \zeta\theta_1 + \dots + \zeta^{n-1}\theta_{n-1},$$

где положено

$$\theta_i = \sigma^i \theta.$$

Подстановка σ циклически перемещает величины θ_i :

$$\sigma\theta_i = \theta_{i+1} \quad (\theta_n = \theta_0),$$

и тем самым переводит резольвенту (ζ, θ) в

$$\begin{aligned} \sigma(\zeta, \theta) &= \theta_1 + \zeta\theta_2 + \dots + \zeta^{n-2}\theta_{n-1} + \zeta^{n-1}\theta_0 = \\ &= \zeta^{-1}(\theta_0 + \zeta\theta_1 + \zeta^2\theta_2 + \dots + \zeta^{n-1}\theta_{n-1}) = \zeta^{-1}(\zeta, \theta). \end{aligned}$$

Поэтому n -ная степень $(\zeta, \theta)^n$ при подстановке σ остаётся неизменной, т. е. $(\zeta, \theta)^n$ принадлежит основному полю K .

Вычисляя $(\zeta, \theta)^n$ путём формального возведения суммы (1) в степень n , мы получим выражение вида

$$(2) \quad (\zeta, \theta)^n = P_0 + \zeta P_1 + \dots + \zeta^{n-1} P_{n-1},$$

где P_i суть полиномы n -ной степени от величин θ , не зависящие от того, какой был выбран корень ζ .

Умножая (1) на ζ^{-r} и суммируя по всем ζ , мы получим (принимая во внимание последнюю теорему § 36):

$$(3) \quad \sum_{\zeta} \zeta^{-r} (\zeta, \theta) = n\theta_r.$$

Так как, по предположению, n не делится на характеристику поля, то из (3), зная все (ζ, θ) , можно вычислить величины θ_r . Но в силу (2) (ζ, θ) получаются, каждая, путём извлечения корня n -ной степени из некоторой величины основного поля K . Отсюда и следует требуемый результат:

Если в основном поле содержатся все корни n -ной степени из единицы, и n не делится на его характеристику, то каждое циклическое поле n -ной степени может быть образовано путём присоединения корней n -ной степени из некоторого элемента основного поля.

Часто оказывается полезным замечание, что также $(\zeta, \vartheta) \cdot (\zeta^{-1}, \vartheta)$ не изменяется при подстановке σ , поскольку первый множитель умножается при этом на ζ^{-1} , а второй — на ζ . Таким образом, и

$$(\zeta, \vartheta) \cdot (\zeta^{-1}, \vartheta)$$

принадлежит основному полю. Поэтому из двух таких «сопряженных» резольвент достаточно присоединить уже одну.

Наконец, непосредственно ясно, что и

$$(1, \vartheta) = \vartheta_0 + \vartheta_1 + \dots + \vartheta_{n-1}$$

принадлежит основному полю K .

Если наше поле Σ получается путём присоединения всех корней уравнения $f(x) = 0$, то σ осуществляет подстановку этих корней, а следовательно, и их номеров $1, 2, \dots, m$; пусть

$$(12\dots j)(j+1\dots l)\dots$$

— разложение этой подстановки на циклы. Все подстановки группы Σ в n -й степени выписанной подстановки и переводят номер в $2, 3, \dots, j$. Если мы теперь предположим, что уравнение $f(x) = 0$ неприводимо, то все корни сопряжены; тем самым должна иметься возможность переводить корень ξ_1 во все остальные корни, т. е. уже цикл $(12\dots j)$ должен охватывать все корни. Так как образующая подстановка группы Галуа должна иметь порядок n , то $j = n$. Таким образом и степень m уравнения равна n , т. е. степени поля. Поэтому уже присоединение одного корня должно порождать всё поле. Занумеровывая корни числами $0, 1, \dots, n-1$ вместо $1, 2, \dots, n$, мы можем порождающий поле элемент $\vartheta = \vartheta_0$ взять равным ξ_0 ; тогда при подходящей нумерации остальных корней будем автоматически иметь: $\vartheta_1 = \sigma\vartheta = \sigma\xi_0 = \xi_1, \vartheta_2 = \sigma\vartheta_1 = \sigma\xi_1 = \xi_2$ и т. д. Поэтому в качестве величин ϑ_i в (1) можно взять соответствующим образом занумерованные корни полинома $f(x)$.

Если основное поле K не содержит корней n -й степени из единицы, то для того, чтобы можно было применить описанный метод решения с помощью корней n -й степени, нужно сперва присоединить к K корни n -й степени из единицы. При этом группа Галуа останется циклической, так как всякая подгруппа циклической группы циклическа.

Мы установим теперь ещё некоторые результаты, относящиеся к неприводимости двучленных уравнений простой степени p .

Прежде всего, если основное поле K снова содержит корни p -той степени из единицы, то, по доказанному в начале этого параграфа, группа Галуа является подгруппой циклической группы порядка p , т. е. либо всей этой группой, либо единичной группой. В первом случае все корни сопряжены и потому уравнение неприводимо. Во втором случае все корни остаются на месте при подстановках группы Галуа и тем самым уравнение распадается на линейные

множители уже в поле K . Итак: *полином $x^p - a$ — а либо полностью разложим, либо неприводим.*

Если K не содержит корней p -той степени из единицы, то утверждать столь многое нельзя. Однако имеет место следующая теорема:

Либо, полином $x^p - a$ неприводим, либо a является p -той степенью некоторого элемента из K , так что в K имеет место разложение

$$x^p - a = x^p - \beta^p = (x - \beta)(x^{p-1} + \beta x^{p-2} + \dots + \beta^{p-1}).$$

~~Доказательство. Пусть полином $x^p - a$ разложим:~~

$$x^p - a = \varphi(x) \cdot \psi(x).$$

В своём поле разложения $x^p - a$ разлагается на линейные множители следующим образом:

$$x^p - a = \prod_{v=0}^{p-1} (x - \zeta^v \theta) \quad (\theta^p = a).$$

Поэтому множитель $\varphi(x)$ должен быть произведением некоторых линейных множителей $x - \zeta^v \theta$, и независимый от x член $\pm b$ полинома $\varphi(x)$ должен иметь вид $\pm \zeta'^\mu \theta^\mu$, где ζ' — корень p -той степени из единицы:

$$b = \zeta'^\mu \theta^\mu,$$

$$b^p = \zeta'^{p\mu} \theta^{p\mu} = a^\mu.$$

Так как $0 < \mu < p$, то $(\mu, p) = 1$ и потому, при надлежащем выборе целых рациональных чисел ρ и σ , имеем:

$$\begin{aligned} \rho\mu + \sigma p &= 1, \\ a &= a^{\rho\mu} a^{\sigma p} = b^{\rho} a^{\sigma p} = (b^{\rho} a^{\sigma})^p. \end{aligned}$$

Следовательно, a есть p -тая степень.

Интересные теоремы относительно приводимости двучленных уравнений содержатся в работах: A. Capelli, Sulla riducibilità delle equazioni algebriche, Rendiconti Napoli, 1898, и G. Darbi, Sulla riducibilità delle equazioni algebriche, Annali di Mat. (4), (1927), 185 — 208.

Задача. Если основное поле K не предполагается содержащим корни n -ной степени из единицы, то группа двучленного уравнения $x^n - a = 0$ изоморфна группе линейных подстановок по модулю n :

$$x' \equiv cx + b.$$

[Соответствующим нормальным полем является $K(\theta, \zeta)$ и для каждой подстановки σ группы Галуа имеем:

$$\sigma\zeta = \zeta^c,$$

$$\sigma\theta = \zeta^{b\theta} \theta.$$

§ 56. Разрешимость уравнений в радикалах.

Как известно, корни уравнения второй, третьей или четвёртой степени могут быть выражены через коэффициенты с помощью рациональных операций и извлечения корней $\sqrt[n]{}$, $\sqrt[3]{}$, ... («радикалов») (см. § 58). Поставим теперь вопрос: какие вообще уравнения обладают тем свойством, что их корни могут быть выражены через величины основного поля K с помощью рациональных операций и радикалов? При этом мы можем, конечно, ограничиться неприводимыми уравнениями с коэффициентами из K . Задача заключается в том, чтобы путём последовательного присоединения величин $\sqrt[n]{a}$ (где a каждый раз принадлежит уже построенному полю) построить такое расширение поля K , которое содержало бы один или все корни предложенного уравнения.

Но эта постановка вопроса в одном пункте ещё не точна. Радикал $\sqrt[n]{a}$ является в поле, вообще говоря, многозначной функцией, и возникает вопрос, какое из этих значений следует понимать каждый раз под $\sqrt[n]{a}$. Так, например, если бы для представления первообразного корня шестой степени из единицы в радикалах мы воспользовались просто выражением $\sqrt[6]{1}$ или даже $\sqrt[12]{1}$, то такое решение следовало бы признать неудовлетворительным, тогда как решение $\zeta = \frac{1}{2} \pm \frac{1}{2} \sqrt{-3}$ было бы более удовлетворительным, поскольку выражение $\frac{1}{2} \pm \frac{1}{2} \sqrt{-3}$ при всяком выборе значения $\sqrt{-3}$ (т. е. решения уравнения $x^2 + 3 = 0$) представляет оба первообразных корня шестой степени из единицы.

Наиболее строгое требование, которое можно в этом отношении поставить, состоит в том, чтобы, во-первых, все решения рассматриваемого уравнения представлялись выражениями вида

$$(1) \quad \sqrt[n]{\dots \sqrt[m]{\dots} + \sqrt[r]{\dots} + \dots + \dots}$$

(или сходными выражениями) и чтобы, во-вторых, эти выражения при всяком выборе значений входящих в них радикалов давали решение рассматриваемого уравнения. (При этом, конечно, радикалу $\sqrt[n]{a}$, входящему в выражение (1) несколько раз, должно приписываться всюду одно и то же значение.)

Предположим, что первое требование выполнено. Тогда и второе будет выполнено, коль скоро мы проследим за тем, чтобы при последовательном присоединении радикалов $\sqrt[n]{a}$ соответствующее уравнение $x^n - a = 0$ было каждый раз неприводимо. Действи-

тельно, тогда все возможные значения корня $\sqrt[n]{a}$ будут всегда сопряжёнными величинами, переводимыми, таким образом, друг в друга с помощью изоморфизмов, и эти изоморфизмы при всех дальнейших присоединениях будут допускать продолжение до изоморфизмов расширенного поля (см. § 35). Поэтому, если при некотором значении радикала $\sqrt[n]{a}$ выражение (1) представляет корень рассматриваемого уравнения, то и при любом другом значении этого радикала оно должно будет представлять корень того же уравнения, так как каждый изоморфизм переводит корни полинома из $K[x]$ снова в корни того же полинома.

После этих предварительных замечаний мы в состоянии следующим образом формулировать основную теорему об уравнениях, разрешимых в радикалах:

1. Если хотя бы один корень неприводимого в K уравнения $f(x) = 0$ может быть представлен выражением вида (1), причём показатели входящих в него радикалов не делятся на характеристику поля K^1 , то группа Галуа этого уравнения разрешима (т. е. её композиционные факторы — циклические простых порядков). 2. Обратно, если группа Галуа уравнения разрешима, то все его корни можно представить в виде (1), и притом так, чтобы показатели последовательно присоединяемых радикалов $\sqrt[n]{a}$ были простыми числами, а соответствующие уравнения $x^n - a = 0$ были неприводимы; при этом мы предполагаем, что характеристика поля K равна нулю или же превосходит наибольшее простое число, содержащееся среди порядков композиционных факторов²⁾.

Таким образом, суть этой теоремы состоит в том, что разрешимость групп Галуа является решающим условием разрешимости уравнения в радикалах. Понятие разрешимости в радикалах сформулировано в первой части теоремы в наиболее слабом, а во второй части — в наиболее сильном виде, так что теорема утверждает возможно больше.

Доказательство. 1. Прежде всего, все показатели корней в (1) можно считать простыми числами, в силу того, что

$$\sqrt[r]{\sqrt[s]{a}} = \sqrt[r \cdot s]{a}.$$

¹⁾ Это предположение имеет своей целью устранить появление неспаряжённых расширений. От него можно было бы освободиться, однако нас это здесь не будет интересовать.

²⁾ Если допустить, чтобы в формулу решения, кроме радикалов указанного вида, входили ещё корни из единицы, то последнее условие можно заменить более слабым, а именно, чтобы среди порядков композиционных факторов не содержалась характеристика поля K .

Присоединим тогда к K все корни из единицы степеней p_1, p_2 и т. д., где $p_1, p_2, \dots$ — простые числа, входящие в качестве показателей корней в (1). Это сведётся, таким образом, к ряду последовательных циклических нормальных расширений, которые мы можем считать в свою очередь разложенными на расширения простых степеней. Но как только указанные корни из единицы будут уже содержаться в поле, так, согласно § 45, присоединение радикала $\sqrt[p]{a}$ либо вовсе не будет расширением, либо будет циклическим

нормальным расширением степени p . Присоединив уже $\sqrt[p]{a}$, мы присоединим теперь один за другим все корни p -той степени из величин, сопряжённых с a ; и это либо вовсе не будут расширения, либо будут циклические расширения простой степени; выполнением их мы достигнем того, что наше поле каждый раз будет оставаться нормальным относительно K . В итоге ряда циклических присоединений:

$$(2) \quad K \subset \Delta_1 \subset \Delta_2 \subset \dots \subset \Delta_\omega,$$

мы придём, наконец, к некоторому нормальному полю $\Delta_\omega = \Omega$, содержащему корень (1) полинома $f(x)$. Вследствие нормальности, поле Ω будет содержать все корни полинома $f(x)$, а значит, и его поле разложения Σ .

Пусть $\mathfrak{G}$ — группа Галуа поля Ω относительно K . Тогда ряду полей (2) соответствует ряд подгрупп

$$(3) \quad \mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \dots \supset \mathfrak{G}_\omega = \mathfrak{E},$$

причём каждая из этих групп служит нормальным делителем предыдущей, а факторгруппы циклически и простых порядков. Это означает, что группа $\mathfrak{G}$ разрешима и (3) есть её композиционный ряд.

Полю Σ соответствует некоторая подгруппа $\mathfrak{H}$, являющаяся нормальным делителем группы $\mathfrak{G}$. Согласно § 46, можно построить композиционный ряд группы $\mathfrak{G}$, содержащий $\mathfrak{H}$:

$$(4) \quad \mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \dots \supset \mathfrak{H} \supset \dots \supset \mathfrak{E},$$

причём этот ряд будет иметь, с точностью до изоморфизма, те же композиционные факторы, что и ряд (3), но, возможно, лишь в другом порядке. Группой Галуа поля Σ относительно K является факторгруппа $\mathfrak{G}/\mathfrak{H}$; для неё мы имеем теперь композиционный ряд

$$\mathfrak{G}/\mathfrak{H} \supset \mathfrak{H}_1/\mathfrak{H} \supset \mathfrak{H}_2/\mathfrak{H} \supset \dots \supset \mathfrak{H}/\mathfrak{H} = \mathfrak{E},$$

факторы которого, по второй теореме об изоморфизмах (§ 45), изоморфны соответствующим факторам ряда (4) и, значит, снова циклически и простых порядков. Тем самым утверждение 1 доказано.

Для доказательства утверждения 2 мы докажем сначала следующее предложение:

Лемма. Корни q -той степени из единицы (где q — простое число) представимы с помощью «неприводимых радикалов» (т. е.

корней неприводимых уравнений $x^p - a = 0$), в предположении, что характеристика поля K равна нулю или больше чем q .

Утверждение леммы в случае $q = 2$ тривиально (поскольку корни второй степени из единицы ± 1 рациональны), так что мы можем принять, что оно уже доказано для всех простых чисел, меньших чем q . Поле корней q -той степени из единицы циклично и имеет степень $q - 1$; разложив $q - 1$ на простые множители: $q - 1 = p_1 \dots p_r$, мы можем построить это поле с помощью ряда циклических расширений, имеющих степени p_i . Присоединяя предварительно корни степеней $p_1, \dots, p_r$ из единицы, которые, по предположению индукции, представимы с помощью радикалов, мы можем применить к циклическим расширениям со степенями p_i теорему § 55, устанавливающую представимость последовательных образующих элементов полей с помощью радикалов. Соответствующие уравнения $x^q - a = 0$ должны быть неприводимы, так как иначе числа p_i не могли бы служить степенями соответствующих полей.

Теперь мы в состоянии доказать утверждение 2. Пусть Σ — поле разложения полинома $f(x)$ и $\mathbb{G} \supset \mathbb{G}_1 \supset \dots \supset \mathbb{G}_r = \mathbb{C}$ — композиционный ряд группы Галуа поля Σ относительно K . Этому ряду групп соответствует ряд полей:

$$K \subset \Delta_1 \subset \dots \subset \Delta_r = \Sigma,$$

каждое из которых нормально и циклично относительно предыдущего. Если $q_1, q_2, \dots$ — относительные степени этих полей, то мы сначала присоединим к K корни степеней q_1, q_2 и т. д. из единицы, что, в силу леммы, возможно сделать путём присоединения неприводимых радикалов. Тогда, по теореме § 55, образующие полей $\Delta_1, \Delta_2, \dots, \Delta_r$ можно будет выразить с помощью радикалов, причём соответствующие уравнения $x^{q_i} - a = 0$ будут в каждом случае либо неприводимы, либо целиком распадаться (конец § 55); в последнем случае присоединение соответствующего радикала излишне. Тем самым доказано и утверждение 2.

Что утверждение 2 действительно неверно, если одна из степеней q_i равна характеристике поля p , показывает следующий пример. «Общее уравнение второй степени» $x^2 + ux + v$ (u, v — неизвестные, присоединённые к простому полю характеристики 2) неприводимо и сепарабельно и остаётся неприводимым при присоединении всех корней из единицы. Присоединение корня неприводимого двучленного уравнения нечётной степени не может привести к разложению общего уравнения, так как это присоединение порождает поле нечётной степени. Но и присоединение квадратного корня тоже не может вызвать разложения, поскольку при этом присоединении приведённая степень поля не изменяется. Таким образом, указанное уравнение не разрешимо в радикалах никаким способом.

Применение. Симметрические группы второй, третьей и четвёртой степени (и их подгруппы) разрешимы; этим объясняется возможность решения уравнений второй, третьей и четвёртой степеней в радикалах (вывод этих решений см. в § 58). Однако симметрические группы пятой и более высоких степеней уже не являются разрешимыми (§ 48), и, как мы скоро увидим, существуют уравнения любой степени, имеющие своей группой Галуа соответствующую симметрическую группу. Поэтому не существует никакой общей формулы решения уравнений пятой и более высоких степеней в радикалах. Лишь некоторые специальные типы этих уравнений (как, например, уравнения деления круга) допускают решение в радикалах.

Поля или уравнения, группы Галуа которых разрешимы, называются *метациклическими*. Иногда и соответствующую группу также называют метациклической (вместо разрешимой).

§ 57. Общее уравнение n -ной степени.

Под *общим уравнением n -ной степени* понимают уравнение

$$z^n - u_1 z^{n-1} + u_2 z^{n-2} - \dots + (-1)^n u_n = 0$$

с заданными коэффициентами $u_1, \dots, u_n$, присоединёнными к основному полю K . Если $v_1, \dots, v_n$ — корни этого уравнения, то

$$u_1 = v_1 + \dots + v_n,$$

$$u_2 = v_1 v_2 + v_1 v_3 + \dots + v_{n-1} v_n,$$

$$\dots$$

$$u_n = v_1 v_2 \dots v_n.$$

Сравним общее уравнение (1) с другим уравнением, корни которого $x_1, \dots, x_n$ являются *неопределёнными* и потому коэффициенты суть элементарные симметрические функции этих *неопределённых* корней:

$$(2) \quad \begin{cases} z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \dots + (-1)^n \sigma_n = \\ = (z - x_1)(z - x_2) \dots (z - x_n) = 0; \end{cases}$$

$$\begin{cases} \sigma_1 = x_1 + \dots + x_n, \\ \sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n, \\ \dots \\ \sigma_n = x_1 x_2 \dots x_n. \end{cases}$$

Уравнение (2) сепарабельно и имеет своей группой Галуа относительно поля $K(\sigma_1, \dots, \sigma_n)$ симметрическую группу всех подстановок корней x . Действительно, каждая такая подстановка представляет автоморфизм поля $K(x_1, \dots, x_n)$, оставляющий неизменными симметрические функции $\sigma_1, \dots, \sigma_n$, а тем самым и все элементы поля

$K(\sigma_1, \dots, \sigma_n)$. Таким образом, каждая функция от $x_1, \dots, x_n$, инвариантная относительно подстановок указанной группы, принадлежит полю $K(\sigma_1, \dots, \sigma_n)$, т. е. каждая симметрическая функция от x , может быть рационально выражена через $\sigma_1, \dots, \sigma_n$. Тем самым мы заново доказали, с помощью теории Галуа, часть «основной теоремы о симметрических функциях» из § 26.

Без труда получается снова также «теорема единственности» из § 26, утверждающая, что соотношение $f(\sigma_1, \dots, \sigma_n) = 0$ может иметь место лишь в том случае, если сим. полином f тождественно равен нулю. Действительно, если бы имело место соотношение

$$f(\sigma_1, \dots, \sigma_n) = f(\sum x_i, \sum x_i x_k, \dots, x_1 x_2 \dots x_n) = 0,$$

то оно осталось бы в силе и после подстановки вместо неизвестных x_i величин v_i . Мы имели бы таким образом:

$$f(\sum v_i, \sum v_i v_k, \dots, v_1 v_2 \dots v_n) = 0$$

или $f(u_1, \dots, u_n) = 0$; следовательно, полином f был бы тождественно равен нулю. (т. е. $u_1, \dots, u_n$ — независимы)

Из теоремы единственности следует, что соответствие

$$f(u_1, \dots, u_n) \rightarrow f(\sigma_1, \dots, \sigma_n)$$

является не только гомоморфизмом, но и изоморфизмом колец $K[u_1, \dots, u_n]$ и $K[\sigma_1, \dots, \sigma_n]$. Он может быть продолжен до изоморфизма полей отношений $K(u_1, \dots, u_n)$ и $K(\sigma_1, \dots, \sigma_n)$ и далее, согласно § 35, — до изоморфизма полей корней $K(v_1, \dots, v_n)$ и $K(x_1, \dots, x_n)$. При этом v_i переходят в каком-то порядке в x_k , но так как x_k перестановочны, то мы можем также перевести каждое v_i в соответствующее x_i . Тем самым доказано следующее предложение:

Существует изоморфизм

$$K(v_1, \dots, v_n) \cong K(x_1, \dots, x_n),$$

переводящий каждое v_i в x_i и каждое u_i в σ_i .

Вследствие этого изоморфизма все теоремы, относящиеся к уравнению (2), непосредственно переносятся на уравнение (1). В частности, получаем:

Общее уравнение (1) сепарабельно и имеет своей группой Галуа относительно поля коэффициентов $K(u_1, \dots, u_n)$ симметрическую группу. Степень его поля разложения равна $n!$.

Положим

$$K(u_1, \dots, u_n) = \Delta,$$

$$K(v_1, \dots, v_n) = \Sigma$$

и обозначим симметрическую группу через $\mathfrak{S}_n$. Она всегда обладает подгруппой индекса 2: знакопеременной группой $\mathfrak{A}_n$. Соответствующее

промежуточное поле Δ имеет степень 2 и порождается любой функцией от v_i , выдерживающей все подстановки из $\mathcal{A}_n$, но не все из $\mathcal{S}_n$. Такой функцией является, в случае, если характеристика поля K отлична от двух, *произведение разностей*

$$\prod_{i < k} (v_i - v_k) = \sqrt{D};$$

квадрат его есть *дискриминант* уравнения (1):

$$D = \prod_{i < k} (v_i - v_k)^2.$$

Дискриминант, как симметрическая функция, является полиномом от u_i . Таким образом, мы получаем поле Δ в форме

$$\Delta = \Delta(\sqrt{D}).$$

При $n > 4$ группа $\mathcal{A}_n$ — простая (§ 48), и потому

$$(3) \quad \mathcal{S}_n \supset \mathcal{A}_n \supset \mathcal{C}$$

— композиционный ряд. Таким образом, группа $\mathcal{S}_n$ при $n > 4$ не является разрешимой, а отсюда, согласно § 56, вытекает знаменитая теорема Абеля:

Общее уравнение n -ной степени при $n > 4$ неразрешимо в радикалах.

При $n = 2$ и $n = 3$ композиционные факторы в (3) циклически. При $n = 2$ имеем даже $\mathcal{A}_n = \mathcal{C}$; при $n = 3$ порядки факторов суть 2 и 3. При $n = 4$ имеем композиционный ряд

$$\mathcal{S}_4 \supset \mathcal{A}_4 \supset \mathcal{B}_4 \supset \mathcal{Z}_2 \supset \mathcal{C},$$

где $\mathcal{B}_4$ — «четверная группа Клейна»

$$\{1, (12)(34), (13)(24), (14)(23)\},$$

а $\mathcal{Z}_2$ — любая из её подгрупп второго порядка. Порядки композиционных факторов суть

$$2, 3, 2, 2.$$

Эти обстоятельства и лежат в основе формул решения уравнений второй, третьей и четвертой степеней, о которых будет идти речь в следующем параграфе.

§ 58. Уравнения второй, третьей и четвертой степеней.

Решение *общего уравнения второй степени*

$$x^2 + px + q = 0,$$

согласно общей теории, получается посредством присоединения одного квадратного корня; в качестве этого корня можно взять

(см. конец предыдущего параграфа) произведение разностей корней x_1, x_2 :

$$x_1 - x_2 = \sqrt{D}; \quad D = p^2 - 4q.$$

Отсюда и из равенства

$$x_1 + x_2 = -p$$

получаем известные формулы решения квадратного уравнения:

$$x_1 = \frac{-p + \sqrt{D}}{2}, \quad x_2 = \frac{-p - \sqrt{D}}{2}.$$

При этом предполагается лишь, что характеристика основного поля не равна 2.

Общее уравнение третьей степени

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

можно, прежде всего, привести с помощью подстановки

$$z = x - \frac{1}{3} a_1$$

к виду

$$x^3 + px + q = 0 \quad 1).$$

(В соответствии с общей теорией § 56 мы предполагаем, что характеристика основного поля отлична от 2 и 3.)

Руководствуясь композиционным рядом

$$\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{C},$$

$$\Delta \subset \Delta(13) \subset E$$

присоединим сначала произведение разностей корней:

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{D} = \sqrt{-4p^3 - 27q^2}.$$

(см. конец § 26, где следует положить $a_0 = 1$, $a_1 = 0$, $a_2 = p$, $a_3 = q$). В результате этого присоединения получится поле $\Delta(\sqrt{D})$, относительно которого рассматриваемое уравнение будет иметь группу Галуа $\mathfrak{A}_3$, т. е. циклическую группу третьего порядка. В соответствии с общей теорией § 55 присоединяем прежде всего кубические корни из единицы:

$$(1) \quad \rho = -\frac{1}{2} + \frac{1}{2} \sqrt{-3}, \quad \rho^2 = -\frac{1}{2} - \frac{1}{2} \sqrt{-3},$$

и рассматриваем затем резольвенты Лагранжа:

$$(1, x_1) = x_1 + x_2 + x_3 = 0,$$

$$(\rho, x_1) = x_1 + \rho x_2 + \rho^2 x_3,$$

$$(\rho^2, x_1) = x_1 + \rho^2 x_2 + \rho x_3.$$

1) Только для упрощения формул. Из доказательства легко установить, как выглядят формулы решения для первоначального уравнения

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0.$$

Третья степень каждой из этих величин должна рационально выражаться через $\sqrt{-3}$ и $\sqrt{D}$. Вычисление даёт:

$$\begin{aligned}(\rho, x_1)^3 &= x_1^3 + x_2^3 + x_3^3 + \\ &+ 3\rho x_1^2 x_2 + 3\rho x_2^2 x_3 + 3\rho x_3^2 x_1 + \\ &+ 3\rho^2 x_1 x_2^2 + 3\rho^2 x_2 x_3^2 + 3\rho^2 x_3 x_1^2 + \\ &+ 6x_1 x_2 x_3,\end{aligned}$$

и соответственно, заменой ρ на ρ^2 , получается $(\rho^2, x_1)^3$. Подставляя сюда выражения (1) и замечая, что

$$\begin{aligned}\sqrt{D} &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \\ &= x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - x_1 x_2^2 - x_2 x_3^2 - x_3 x_1^2,\end{aligned}$$

получаем:

$$(\rho, x_1)^3 = \sum x_1^3 - \frac{3}{2} \sum x_1^2 x_2 + 6x_1 x_2 x_3 + \frac{3}{2} \sqrt{-3} \sqrt{D}.$$

(Знаки суммирования имеют здесь тот же смысл, что и для симметрических функций, в § 26.) Входящие в эту формулу симметрические функции легко могут быть выражены, по § 26, через элементарные симметрические функции $\sigma_1, \sigma_2, \sigma_3$ и тем самым через коэффициенты нашего уравнения. Имеем:

$$\begin{aligned}\exists \sum x_1^3 &= 3 \sum x_1^2 x_2 + 6x_1 x_2 x_3 = 0, \text{ так как } \sigma_1 = 0, \\ -\frac{9}{2} \sigma_1 \sigma_2 &= -\frac{9}{2} \sum x_1^2 x_2 - \frac{27}{2} x_1 x_2 x_3 = 0, \text{ так как } \sigma_1 = 0, \\ \frac{27}{2} \sigma_3 &= \frac{27}{2} x_1 x_2 x_3 = -\frac{27}{2} q \\ \sum x_1^3 - \frac{3}{2} \sum x_1^2 x_2 + 6x_1 x_2 x_3 &= -\frac{27}{2} q;\end{aligned}$$

поэтому

$$(\rho, x_1)^3 = -\frac{27}{2} q + \frac{3}{2} \sqrt{-3} \sqrt{D},$$

и точно так же

$$(\rho^2, x_1)^3 = -\frac{27}{2} q - \frac{3}{2} \sqrt{-3} \sqrt{D}.$$

Кубические иррациональности (ρ, x_1) и (ρ^2, x_1) не независимы, а именно (см. § 55),

$$\begin{aligned}(\rho, x_1) \cdot (\rho^2, x_1) &= x_1^2 + x_2^2 + x_3^2 + (\rho + \rho^2) x_1 x_2 + \\ &+ (\rho + \rho^2) x_1 x_3 + (\rho + \rho^2) x_2 x_3 = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_1 x_3 - x_2 x_3 = \\ &= \sigma_1^2 - 3\sigma_2 = -3\rho.\end{aligned}$$

Таким образом, кубические корни

$$(2) \quad \begin{cases} (\rho, x_1) = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \\ (\rho^2, x_1) = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}} \end{cases}$$

следует определять так, чтобы их произведение подчинялось равенству

$$(3) \quad (\rho, x_1) \cdot (\rho^2, x_1) = -3\rho.$$

Корни x_1, x_2, x_3 определяются теперь с помощью формулы (3) § 55 следующим образом:

$$(4) \quad \begin{cases} 3 \cdot x_1 = \sum_{\zeta} (\zeta, x_1) = (\rho, x_1) + (\rho^2, x_1), \\ 3 \cdot x_2 = \sum_{\zeta} \zeta^{-1} (\zeta, x_1) = \rho^2 (\rho, x_1) + \rho (\rho^2, x_1), \\ 3 \cdot x_3 = \sum_{\zeta} \zeta^{-2} (\zeta, x_1) = \rho (\rho, x_1) + \rho^2 (\rho, x_1). \end{cases}$$

Формулы (2), (3), (4) суть «формулы Кардано». В силу своего вывода они верны не только для «общего», но и для каждого частного кубического уравнения.

Вопрос о вещественности корней. Если основным полем, которому принадлежат коэффициенты p, q , служит вещественное числовое поле K , то возможны два случая:

а) Уравнение имеет один вещественный и два сопряжённых комплексных корня.

Очевидно, тогда произведение $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ чисто мнимо и тем самым $D < 0$. Величины $\pm \sqrt{-3D}$ вещественны, и в (2) можно взять для (ρ, x_1) вещественный кубический корень. Тогда, вследствие соотношения (3), также (ρ^2, x_1) будет вещественным, и формулы (4) дадут $3x_1$ в виде суммы двух вещественных кубических корней, а $3x_2$ и $3x_3$ — как сопряжённые комплексные величины.

б) Уравнение имеет три вещественных корня.

Теперь $\sqrt{D}$ вещественно, и тем самым $D \geq 0$. В случае $D = 0$ (равенство двух корней) остаётся в силе всё сказанное выше. Но в случае $D > 0$ величины, стоящие в формулах (2) под знаками кубических радикалов, мнимы, и мы получаем тем самым три (вещественных) выражения (4) в виде сумм мнимых кубических корней, т. е. не в вещественной форме.

Это — так называемый «неприводимый случай» («casus irreducibilis») кубического уравнения. Покажем, что в этом случае действительно невозможно решить уравнение

$$x^3 + px + q = 0$$

с помощью вещественных радикалов, если только это уравнение не распадается уже в основном поле K .

Итак, пусть уравнение $x^3 + px + q = 0$ неприводимо над полем K и имеет три вещественных корня x_1, x_2, x_3 . Присоединим сначала $\sqrt{D}$. Это не вызовет распадаения уравнения [так как поле $K(\sqrt{D})$, являющееся, самое большее, квадратичным, не может содержать ни одного корня неприводимого кубического уравнения], а его группой Галуа будет теперь $\mathfrak{A}_3$. Если бы

оказалось возможным добиться разложения уравнения с помощью ряда присоединений вещественных радикалов, показатели которых, разумеется, можно считать простыми числами, то среди этих присоединений нашлось бы «критическое» присоединение $\sqrt[h]{a}$ (h — простое число), как раз и вызывающее разложение. тогда как до присоединения радикала $\sqrt[h]{a}$, скажем, в поле Δ , уравнение ещё неприводимо. Согласно § 55, либо полином $x^h - a$ неприводим в Δ , либо a есть h -тая степень некоторого числа из Δ . Последний случай отпадает, так как иначе вещественный корень h -той степени из a уже содержался бы в Δ и, значит, его присоединение не могло бы вызвать разложения уравнения. Таким образом, полином $x^h - a$ неприводим и степень поля $\Delta(\sqrt[h]{a})$ есть как раз h . По предположению, в $\Delta(\sqrt[h]{a})$ содержится корень уравнения $x^3 + px + q = 0$, ещё неприводимого в Δ ; тем самым h делится на 3, значит, $h = 3$ и, скажем, $\Delta(\sqrt[3]{a}) = \Delta(x_1)$. Степень поля разложения $\Delta(x_1, x_2, x_3)$ относительно поля Δ тоже равна 3; тем самым имеем также $\Delta(\sqrt[3]{a}) = \Delta(x_1, x_2, x_3)$. Но, будучи, как только что установлено, нормальным, поле $\Delta(\sqrt[3]{a})$ должно одновременно с $\sqrt[3]{a}$ содержать также сопряжённые величины $\rho\sqrt[3]{a}$ и $\rho^2\sqrt[3]{a}$, а значит, и кубические корни из единицы ρ и ρ^2 . Тем самым мы пришли к противоречию, так как поле $\Delta(\sqrt[3]{a})$ вещественно и потому не может содержать невещественного числа ρ .

Общее уравнение четвёртой степени

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0,$$

аналогично уравнению третьей степени, может быть преобразовано с помощью подстановки

$$z = x - \frac{1}{4} a_1$$

в уравнение

$$x^4 + px^2 + qx + r = 0.$$

Композиционному ряду

$$\mathfrak{G}_4 \supset \mathfrak{H}_4 \supset \mathfrak{B}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E}$$

соответствует ряд полей

$$\Delta \subset \Delta(\sqrt{D}) \subset \Delta_1 \subset \Delta_2 \subset \Sigma.$$

Мы будем снова предполагать, что характеристика поля Δ отлична от 2 и 3. Как мы увидим, находить развёрнутое выражение дискриминанта D не понадобится. Поле Δ_1 будет получаться из $\Delta(\sqrt{D})$ присоединением величины, выдерживающей все подстановки из $\mathfrak{B}_4$, но не все из $\mathfrak{H}_4$. Такой величиной является

$$\theta_1 = (x_1 + x_2)(x_3 + x_4).$$

Заметим попутно, что эта величина, кроме подстановок из $\mathfrak{B}_4$, выдерживает ещё следующие подстановки:

$$(12), (34), (1324), (1423)$$

(образующие вместе с $\mathfrak{B}_4$ группу восьмого порядка). Она обладает относительно Δ тремя различными сопряжёнными величинами, в которые переводится подстановками из $\mathfrak{B}_4$, а именно:

$$\theta_1 = (x_1 + x_2)(x_3 + x_4),$$

$$\theta_2 = (x_1 + x_3)(x_2 + x_4),$$

$$\theta_3 = (x_1 + x_4)(x_2 + x_3).$$

Эти величины являются корнями уравнения третьей степени

$$(5) \quad \theta^3 - b_1\theta^2 + b_2\theta - b_3 = 0,$$

где b_i — элементарные симметрические функции от $\theta_1, \theta_2, \theta_3$:

$$b_1 = \theta_1 + \theta_2 + \theta_3 = 2 \sum x_1 x_2 = 2p,$$

$$b_2 = \sum \theta_1 \theta_2 = \sum x_1^2 x_2^2 + 3 \sum x_1^2 x_2 x_3 + 6 x_1 x_2 x_3 x_4,$$

$$b_3 = \theta_1 \theta_2 \theta_3 = \sum x_1^3 x_2^2 x_3 + 2 \sum x_1^3 x_2 x_3 x_4 + 2 \sum x_1^2 x_2^2 x_3^2 + 4 \sum x_1^2 x_2^2 x_3 x_4.$$

b_2 и b_3 могут быть выражены через элементарные симметрические функции $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ от x_i . А именно (метод § 26):

$$\sigma_2^2 = \sum x_1^2 x_2^2 + 2 \sum x_1^2 x_2 x_3 + 6 x_1 x_2 x_3 x_4 = p^2,$$

$$\sigma_1 \sigma_3 = \sum x_1^3 x_2 x_3 + 4 x_1 x_2 x_3 x_4 = 0,$$

$$-4\sigma_4 = -4x_1 x_2 x_3 x_4 = -4r$$

$$b_2 = \sum x_1^2 x_2^2 + 3 \sum x_1^2 x_2 x_3 + 6 x_1 x_2 x_3 x_4 = p^2 - 4r;$$

$$\sigma_1 \sigma_2 \sigma_3 = \sum x_1^3 x_2^2 x_3 + 3 \sum x_1^3 x_2 x_3 x_4 + 3 \sum x_1^2 x_2^2 x_3^2 + 8 \sum x_1^2 x_2^2 x_3 x_4 = 0,$$

$$-\sigma_1^2 \sigma_4 = -\sum x_1^3 x_2 x_3 x_4 - 2 \sum x_1^2 x_2^2 x_3 x_4 = 0,$$

$$-\sigma_3^2 = -\sum x_1^2 x_2^2 x_3^2 - 2 \sum x_1^2 x_2^2 x_3 x_4 = -q^2$$

$$b_3 = \sum x_1^3 x_2^2 x_3 + 2 \sum x_1^3 x_2 x_3 x_4 + 2 \sum x_1^2 x_2^2 x_3^2 + 4 \sum x_1^2 x_2^2 x_3 x_4 = -q^2.$$

Тем самым уравнение (5) приводится к

$$(6) \quad \theta^3 - 2p\theta^2 + (p^2 - 4r)\theta + q^2 = 0.$$

Это уравнение называется *кубической резольвентой* уравнения четвёртой степени; корни её $\theta_1, \theta_2, \theta_3$ могут быть выражены в радикалах по «формулам Кардано». Каждая из величин θ выдерживает группу из восьми подстановок; однако в своей совокупности они выдерживают только группу $\mathfrak{B}_4$, и потому

$$K(\theta_1, \theta_2, \theta_3) = \Delta_1.$$

Поле Δ_2 получается из Δ_1 присоединением величины, выдерживающей не все четыре подстановки из $\mathfrak{B}_4$, а (скажем) только под-

становку (12) (34) и единичную. Такою величиной является $x_1 + x_2$.
Имеем:

$$(x_1 + x_2)(x_3 + x_4) = \theta_1 \quad \text{и} \quad (x_1 + x_2) + (x_3 + x_4) = 0,$$

откуда, скажем,

$$x_1 + x_2 = \sqrt{-\theta_1}, \quad x_3 + x_4 = -\sqrt{-\theta_1}.$$

Аналогично получаем:

$$x_1 + x_3 = \sqrt{-\theta_2}, \quad x_2 + x_4 = -\sqrt{-\theta_2};$$

$$x_1 + x_4 = \sqrt{-\theta_3}, \quad x_2 + x_3 = -\sqrt{-\theta_3}.$$

Однако, эти три иррациональности не являются независимыми, поскольку

$$\begin{aligned} \sqrt{-\theta_1} \cdot \sqrt{-\theta_2} \cdot \sqrt{-\theta_3} &= (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) = \\ &= x_1^3 + x_1^2(x_2 + x_3 + x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = \\ &= x_1^2(x_1 + x_2 + x_3 + x_4) + \sum x_1x_2x_3 = \\ &= \sum x_1x_2x_3 = \\ &= -q. \end{aligned}$$

Так как $\mathfrak{B}_4$ имеет порядок 4 и обладает подгруппой порядка 2, то двух квадратичных иррациональностей как раз достаточно, чтобы спуститься от $\mathfrak{B}_4$ к $\mathfrak{E}$ или, что то же, подняться от Δ до Σ . И действительно, корни x_i выражаются в радикалах через три величины θ (зависящие уже от двух из них); в самом деле, очевидно

$$\begin{cases} 2x_1 = \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}, \\ 2x_2 = \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2x_3 = -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2x_4 = -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}. \end{cases}$$

Это и суть формулы решения общего уравнения четвертой степени. В силу своего вывода они верны также для каждого частного уравнения четвертой степени.

Замечание. Так как

$$\theta_1 - \theta_2 = -(x_1 - x_4)(x_2 - x_3),$$

$$\theta_1 - \theta_3 = -(x_1 - x_3)(x_2 - x_4),$$

$$\theta_2 - \theta_3 = -(x_1 - x_2)(x_3 - x_4),$$

то дискриминант кубической резольвенты равен дискриминанту первоначального уравнения. Это доставляет простой способ вычисления дискриминанта уравнения четвертой степени, поскольку дискриминант кубического уравнения мы уже знаем; находим:

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

Задача 1. Группой Галуа кубической резольвенты каждого индивидуального уравнения четвертой степени является факторгруппа группы Галуа исходного уравнения по пересечению этой последней с четверной группой $\mathfrak{B}_4$.

Задача 2. Определить группу Галуа уравнения

$$x^4 + x^2 + x + 1 = 0.$$

[См. задачу 4 § 50 и предыдущую задачу 1.]

§ 59. Построения с помощью циркуля и линейки.

Обратимся теперь к рассмотрению следующего вопроса: *когда геометрическая задача на построение может быть решена с помощью циркуля и линейки?*

Пусть нам заданы некоторые образы элементарной геометрии (точки, прямые или круги). Задача состоит в том, чтобы, пользуясь ими, построить другие образы, удовлетворяющие известным условиям.

Присоединим к заданным образам декартову систему координат. Тогда все заданные образы можно будет представить с помощью чисел (координат), и то же будет верно для образов, которые требуется построить. Если удастся построить (как отрезки) числа, представляющие последние образы, то задача будет решена. Тем самым всё сводится к построению, исходя из заданных отрезков, некоторых новых отрезков. Пусть $a, b, \dots$ — заданные отрезки и x — один из искомым.

Мы можем теперь указать, прежде всего, достаточное условие возможности построения:

Если решение x задачи вещественно и может быть вычислено, исходя из заданных отрезков $a, b, \dots$, с помощью рациональных операций и извлечения (не обязательно вещественных) квадратных корней, то отрезок x может быть построен с помощью циркуля и линейки.

Эту теорему удобнее всего доказывать, изображая все комплексные числа $p + iq$, встречающиеся при вычислении x , известным способом ¹⁾ точками плоскости с прямоугольными координатами p, q и заменяя все производимые операции геометрическими построениями в этой плоскости. Как это делается — достаточно хорошо известно: сложение есть векторное сложение, вычитание — обратная операция. При умножении складываются аргументы и перемножаются модули; поэтому, если φ_1, φ_2 — аргументы и r_1, r_2 — модули перемножаемых чисел, то соответствующие величины φ, r

¹⁾ Комплексные числа, точный смысл которых в рамках абстрактной алгебры будет выяснен лишь в главе 9, мы будем предполагать здесь известными.

для произведения строятся на основании уравнений

$$\varphi = \varphi_1 + \varphi_2 \text{ и } r = r_1 r_2 \text{ или } 1 : r_1 = r_2 : r.$$

Деление выполняется снова как обратная операция. Наконец, для вычисления квадратного корня из числа, имеющего модуль r и аргумент φ , нужно построить r_1 , φ_1 на основании уравнений

$$\varphi = 2\varphi_1 \text{ или } \varphi_1 = \frac{1}{2}\varphi$$

и

$$r = r_1^2 \text{ или } 1 : r_1 = r_1 : r.$$

Тем самым всё сводится к известным построениям циркулем и линейкой¹⁾.

Оказывается, что верна также теорема, обратная только что доказанной:

Если отрезок x может быть построен из заданных отрезков $a, b, \dots$ с помощью циркуля и линейки, то x может быть выражено через $a, b, \dots$ с помощью рациональных операций и извлечения квадратных корней.

Для доказательства этого предложения рассмотрим подробнее операции, применяемые при построениях. Это суть: взятие произвольной точки (внутри заданной области); построение прямой по двум её точкам; построение окружности по центру и радиусу; наконец, построение точки пересечения двух прямых, прямой и окружности, или двух окружностей.

Но все эти операции могут быть сведены с помощью нашей системы координат к алгебраическим операциям. Если точка может быть взята внутри области произвольно, то мы можем, в частности, за её координаты принять рациональные числа. Все остальные построения приводят к рациональным операциям, за исключением двух последних (пересечения окружностей с прямыми или окружностями), приводящих к квадратным уравнениям и, значит, к извлечению квадратных корней. Тем самым утверждение доказано.

Остаётся ещё заметить, что в геометрических задачах речь идёт не о нахождении способов построения для каждого специального выбора заданных точек; напротив, требуется дать общий способ построения, который бы всегда (при некоторых ограничениях) давал решение. С алгебраической точки зрения это означает, что одна и та же формула (могущая содержать квадратные корни), должна для всех значений $a, b, \dots$, лежащих в известных грани-

¹⁾ Другое доказательство получим, разбивая все встречающиеся числа на их вещественную и мнимую части и сводя по § 69 комплексные квадратные корни к вещественным, которые тогда могут быть построены обычным способом.

цах, давая решение x , имеющее смысл и удовлетворяющее уравнениям геометрической задачи. Иными словами это можно выразить так: уравнения, которыми определяется x , и извлечения квадратных корней и другие операции, с помощью которых мы решаем эти уравнения, должны сохранять смысл при замене заданных элементов $a, b, \dots$ неопределёнными величинами. Так, например, если спрашивается, выполняли ли с помощью циркуля и линейки трисекция угла, — задача, которая вследствие соотношения

$$\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi$$

сводится к решению уравнения

$$(1) \quad 4x^3 - 3x = \alpha \quad (\alpha = \cos 3\varphi),$$

— то при этом имеется в виду не вопрос о том, можно ли для каждого частного значения α найти решение уравнения (1) с помощью извлечения квадратных корней, но спрашивается, существует ли общая формула решения уравнения (1), имеющая требуемый вид, т. е. формула решения, сохраняющая смысл при неопределённом α .

Итак, мы свели теперь геометрическую задачу о возможности построения с помощью циркуля и линейки к следующему алгебраическому вопросу: когда величина x может быть выражена через заданные величины $a, b, \dots$ с помощью рациональных операций и извлечения квадратных корней?

Ответить на этот вопрос нетрудно. Пусть $\mathfrak{K}$ — поле рациональных функций от заданных величин $a, b, \dots$. Если x выражается через $a, b, \dots$ с помощью рациональных операций и извлечения квадратных корней, то x во всяком случае должно принадлежать полю, получающемуся из $\mathfrak{K}$ путём последовательного присоединения конечного числа квадратных корней, т. е. путём конечного числа расширений степени 2. Если мы ещё будем присоединять вслед за каждым квадратным корнем также квадратные корни из сопряжённых элементов поля, то все новые расширения, как и прежние, будут квадратичными и в результате мы получим нормальное расширение степени 2^m , содержащее x . Итак:

Для того чтобы отрезок x можно было построить с помощью циркуля и линейки, необходимо, чтобы число x содержалось в нормальном расширении поля $\mathfrak{K}$, имеющем степень 2^m .

Но это условие также достаточно. Действительно, группа Галуа поля степени 2^m есть группа порядка 2^m и, следовательно, как всякая группа, порядок которой равен степени простого числа, — разрешимая группа (§ 46, задача 5). Таким образом, существует композиционный ряд, все композиционные факторы которого — второго порядка. По основной теореме теории Галуа, ему соответствует возрастающий ряд полей, в котором каждое следующее имеет по отношению к предыдущему степень 2. Но всякое расширение второй степени может быть достигнуто путём присое-

динения некоторого квадратного корня. Тем самым величина x может быть выражена с помощью квадратных корней, откуда и следует наше утверждение.

Применим теперь эти общие теоремы к некоторым классическим задачам.

Делийская задача об удвоении куба приводит к кубическому уравнению

$$x^3 = 2.$$

Согласно признаку Эйзенштейна, это уравнение неприводимо, так что каждый его корень порождает расширение третьей степени. Но такое поле не может быть подполем поля степени 2^m . Следовательно, *удвоение куба невыполнимо с помощью циркуля и линейки.*

Проблема *трисекции угла*, как мы уже видели, приводит к уравнению

$$4x^3 - 3x - \alpha = 0,$$

где α — неопределённая величина. Неприводимость этого уравнения над полем рациональных функций от α легко устанавливается: если бы левая часть содержала множитель, рациональный относительно α , то она содержала бы и множитель, целый рациональный относительно α ; однако линейный полином от α , коэффициенты которого не имеют общего множителя, очевидно, неприводим. Отсюда, как и выше, заключаем, что *трисекция угла невыполнима с помощью циркуля и линейки.*

Алгебраически более удобная форма уравнения трисекции угла получится, если к полю рациональных функций от $\alpha = \cos 3\varphi$ присоединить ещё величину

$$i \sin 3\varphi = \sqrt{-(1 - \cos^2 3\varphi)}$$

и написать уравнение для

$$y = \cos \varphi + i \sin \varphi,$$

а именно

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

или, короче,

$$y^3 = \beta.$$

То, что трисекция угла 3φ может быть сведена к этому двучленному уравнению, легко также следует из геометрической интерпретации комплексных чисел.

Величины x и y могут быть выражены одна через другую с помощью квадратных корней.

Квадратура круга приводит к проблеме построения числа π . Невозможность этого построения вытекает из того, что π , как известно, не удовлетворяет вообще никакому алгебраическому уравне-

нию с рациональными коэффициентами, иными словами, — что π трансцендентно. Действительно, тогда π не может принадлежать никакому конечному расширению поля рациональных чисел.

Задача построения правильного n -угольника, вписанного в заданную окружность, приводит, в случае n -угольника, к задаче построения величины

$$2 \cos \frac{2\pi}{h} = \zeta + \zeta^{-1},$$

где ζ — первообразный корень h -той степени из единицы $e^{\frac{2\pi i}{h}}$. Но эта величина преобразуется в себя лишь при подстановках $\zeta \rightarrow \zeta$ и $\zeta \rightarrow \zeta^{-1}$ группы Галуа поля деления круга и, значит, порождает вещественное подполе степени $\frac{\varphi(h)}{2}$. Следовательно, условием воз-

можности построения этой величины является, чтобы $\frac{\varphi(h)}{2}$, а потому и $\varphi(h)$, было степенью двойки. Но при $h = 2^{\nu} q_1^{\nu_1} \dots q_r^{\nu_r}$ (q_i — нечётные простые числа) имеем:

$$(2) \quad \varphi(h) = 2^{\nu-1} q_1^{\nu_1-1} \dots q_r^{\nu_r-1} (q_1-1) \dots (q_r-1)$$

(где при $\nu=0$ первый множитель $2^{\nu-1}$ отпадает). Таким образом, указанное условие сводится к требованию, чтобы нечётные простые множители могли входить в h лишь в первых степенях ($\nu_i=1$) и чтобы, кроме того, для каждого входящего в h нечётного простого числа q_i число q_i-1 было степенью двойки, так что каждое q_i должно иметь вид

$$q_i = 2^k + 1.$$

Какие же простые числа имеют такой вид?

k не может делиться на нечётное число $\mu > 2$; действительно, из

$$k = \mu \nu, \quad \mu \not\equiv 0 \pmod{2}, \quad \mu > 2$$

следовало бы, что $(2^{\nu})^{\mu} + 1$ делится на $2^{\nu} + 1$ и, значит, не простое.

Таким образом, должно быть $k \equiv 2^{\lambda}$ и

$$q_i = 2^{2^{\lambda}} + 1.$$

Значения $\lambda = 0, 1, 2, 3, 4$ действительно дают простые числа q_i , а именно

$$3, 5, 17, 257, 65537.$$

Но для $\lambda = 5$ и некоторых больших λ (как далеко — неизвестно) числа $2^{2^{\lambda}} + 1$ уже не являются простыми; например, $2^{2^5} + 1$ имеет делителем 641.

Таким образом, каждый правильный h -угольник, где h , кроме степени двойки, содержит лишь указанные простые множители 3,

Рай

х² и делится на х² + 1
если
х не
делится
на 2
то
х² + 1
делится
на х² + 1
х² + 1
делится
на х² + 1

5, 17, ... и притом не выше чем в первой степени, может быть построен с помощью циркуля и линейки (Гаусс). Пример семнадцатиугольника был рассмотрен нами в § 54. Известны также способы построения правильных трёх-, четырёх-, пяти-, шести-, восьми- и десятиугольников. Правильные семи- и девятиугольники уже не могут быть построены с помощью циркуля и линейки; они приводят к кубическим подполям поля деления круга шестой степени.

Задача. Показать, что кубическое уравнение

$$x^3 + px + q = 0$$

в «неприводимом случае» всегда может быть преобразовано некоторой подстановкой $x = \beta x'$ в уравнение (1) трисекции угла, и вывести отсюда для этого кубического уравнения формулу решения в тригонометрических функциях.

§ 60. Метациклические уравнения простой степени.

Неприводимому уравнению простой степени q соответствует транзитивная группа подстановок «степени» q , т. е. транзитивная группа $\mathfrak{G}$ подстановок q номеров $1, 2, \dots, q$. Мы исследуем эти группы и их нормальные делители и, в частности, найдём, каково должно быть строение группы для того, чтобы она была метациклической.

В § 49 было уже отмечено, что подгруппа $\mathfrak{G}_1$, оставляющая на месте цифру 1, имеет индекс q ; отсюда следует, что порядок группы $\mathfrak{G}$ должен делиться на степень q . (Причём здесь не нужно ещё предполагать, что q — простое число.)

Если $\mathfrak{F}$ — нормальный делитель группы $\mathfrak{G}$, то имеются две возможности: Либо $\mathfrak{F}$ транзитивен. Тогда порядок его снова делится на q .

Либо $\mathfrak{F}$ интранзитивен. Пусть тогда, скажем, $\{1, 2, \dots, k\}$ — область транзитивности для $\mathfrak{F}$ и σ — подстановка из $\mathfrak{G}$, переводящая 1 в номер i , не принадлежащий этой области. $\sigma\{1, 2, \dots, k\}$ будет в этом случае областью транзитивности для $\sigma\mathfrak{F}\sigma^{-1}$. Но так как $\mathfrak{F}$ — нормальный делитель, то $\sigma\mathfrak{F}\sigma^{-1} = \mathfrak{F}$; следовательно, $\sigma\{1, 2, \dots, k\}$ есть снова область транзитивности для $\mathfrak{F}$, содержащая к тому же ровно k номеров и среди них номер i . Так как i произвольно, то заключаем, что все области транзитивности нормального делителя $\mathfrak{F}$ состоят из одинакового числа, а именно k , номеров; тем самым k есть (собственный) делитель числа q .

Если теперь, как было вначале предположено, q — простое число, то k может быть равно только 1. Но в этом случае $\mathfrak{F}$ оставляет на месте все номера $1, 2, \dots, q$. Таким образом:

Нормальный делитель $\mathfrak{F}$ транзитивной группы подстановок простой степени q либо транзитивен, либо совпадает с единичной группой $\mathfrak{E}$.

Докажем теперь следующую теорему:

Транзитивная метациклическая группа $\mathfrak{G}$ простой степени q всегда может быть при надлежащей нумерации переставляемых символов $1, 2, \dots, q$ записана в виде группы линейных подстановок по модулю q :

$$\tau(z) \equiv az + b \pmod{q} \quad (a \not\equiv 0 \pmod{q}; z = 1, 2, \dots, q),$$

причём в группе будут содержаться, в частности, все подстановки с $a = 1$:

$$\sigma(z) \equiv z + b \pmod{q} \quad (b = 1, \dots, q).$$

Доказательство. Порядок группы $\mathfrak{G}$ делится на q . Если он равен q , то группа циклическа (ибо порядок любого отличного от единицы группы

элемента σ , будучи делителем числа q , может быть равен лишь q , а в таком случае σ уже порождает всю группу). Образующая подстановка σ должна состоять из одного единственного цикла, содержащего все символы $1, 2, \dots, q$ ибо в противном случае группа не была бы транзитивной. Поэтому, при надлежащей нумерации символов,

$$\sigma = (12 \dots q),$$

и тем самым

$$\sigma(z) \equiv z + 1 \pmod{q},$$

$$\sigma^b(z) \equiv z + b \pmod{q} \quad (b = 1, \dots, q).$$

Итак, в этом случае теорема доказана. Мы можем, таким образом, проводить индукцию по порядку группы $\mathfrak{G}$, предполагая, что этот порядок равен составному числу $q \cdot j$, и теорема (при фиксированном q) уже верна для всех групп меньшего порядка.

Вследствие своей разрешимости, группа $\mathfrak{G}$ обладает отличным от $\mathfrak{G}$ разрешимым нормальным делителем $\mathfrak{H}$ с простым индексом. В силу предыдущей теоремы, этот нормальный делитель $\mathfrak{H}$ транзитивен и потому, по предположению индукции, является группой линейных подстановок по модулю q , содержащей группу подстановок $z \rightarrow z + b$.

Как легко видеть, подстановки $z \rightarrow z + b$ при $b \neq 0$ суть q -членные циклы, и притом единственные такие циклы в $\mathfrak{H}$, так как всякая другая подстановка $z \rightarrow az + b$ оставляет на месте элемент z , определяемый из сравнения

$$az + b \equiv z,$$

или

$$(a - 1)z \equiv -b.$$

Если теперь σ — подстановка

$$\sigma(z) \equiv z + 1$$

и τ — произвольная подстановка из $\mathfrak{G}$, то $\tau\sigma\tau^{-1}$ снова есть q -членный цикл и снова принадлежит к $\mathfrak{H}$, т. е. снова есть подстановка вида

$$\tau\sigma\tau^{-1}(z) \equiv z + a.$$

Пусть $\tau^{-1}(z) = \zeta$, так что $z = \tau(\zeta)$,

$$\tau\sigma(\zeta) \equiv \tau(\zeta) + a,$$

$$\tau(\zeta + 1) \equiv \tau(\zeta) + a.$$

Индукцией по ν получаем отсюда:

$$\tau(\zeta + \nu) \equiv \tau(\zeta) + \nu a,$$

и в частности при $\zeta = 0$, полагая $\tau(0) = b$, имеем:

$$\tau(\nu) \equiv \nu a + b.$$

Таким образом, τ есть линейная подстановка по модулю q . И так как все подстановки $\sigma(z) \equiv z + b$ содержатся в $\mathfrak{H}$, то они содержатся также в $\mathfrak{G}$. Тем самым теорема доказана.

Верна и обратная теорема:

Каждая группа $\mathfrak{G}$ линейных подстановок по модулю q , содержащая все подстановки

$$\sigma(z) \equiv z + b,$$

разрешима.

Доказательство. Указанные подстановки σ образуют в $\mathfrak{G}$ нормальный делитель $\mathfrak{H}$, так как вместе с каждым σ также каждая сопряженная подстановка $\tau\sigma\tau^{-1}$ является q -членным циклом или, соответственно,

тождественной подстановкой. В каждый смежный класс $\mathfrak{M}\tau$, где τ — подстановка

$$\tau(z) \equiv az + b,$$

входит также подстановка $\sigma^{-1}\tau$:

$$\sigma^{-1}\tau(z) \equiv az.$$

Поэтому композирование двух смежных классов проще всего производить путём композирования подстановок $\tau(z) \equiv az$. Но последнее сводится просто к перемножению коэффициентов a (образующих тем самым мультипликативную группу по модулю q). Следовательно, смежные классы по $\mathfrak{M}$ образуют абелеву группу: $\mathfrak{G}/\mathfrak{M}$ абелева. А так как и нормальный делитель $\mathfrak{M}$ абелев, то $\mathfrak{G}$ разрешима.

Следствия. Линейная нетождественная подстановка

$$\sigma(z) \equiv az + b$$

оставляет на месте не более одного элемента z . Действительно, сравнение

$$(a-1)z \equiv -b \pmod{q}$$

имеет не более одного решения, за исключением того случая, когда $a \equiv 1$ и $b \equiv 0$. Это означает, что *единственной подгруппой, оставляющей на месте два номера i, k , является единичная группа.*

Соображения, использованные в наших доказательствах, дают одновременно средство нахождения всех нормальных делителей линейной группы $\mathfrak{G}$. Действительно, мы обнаружили, что каждый нормальный делитель (отличный от $\mathfrak{G}$) должен содержать в себе нормальный делитель $\mathfrak{M}$ и что в каждом смежном классе по $\mathfrak{M}$ содержится подстановка вида $\tau(z) \equiv az$. Следовательно, достаточно определить все подгруппы мультипликативной группы этих $a \pmod{q}$. Но группа всех ненулевых классов вычетов по модулю q циклическа, значит, циклическа и каждая её подгруппа. Таким образом, если j — порядок заданной группы классов вычетов, то каждому делителю числа j соответствует одна подгруппа.

Если в качестве переставляемых объектов взять корни уравнения, а в качестве группы $\mathfrak{G}$ — его группу Галуа, то наши теоретико-групповые теоремы тотчас же можно перевести на язык теории полей. Мы получим:

Группу Галуа неприводимого метациклического уравнения простой степени q относительно поля K всегда можно, при надлежащей нумерации корней, рассмотреть как группу линейных подстановок номеров по модулю q . Степень поля разложения $K(\alpha_1, \dots, \alpha_q)$ равна $q \cdot j$, где $j | q-1$. Существует нормальное промежуточное поле степени j , содержащее все другие нормальные промежуточные поля. Каждому делителю числа j соответствует нормальное промежуточное поле. Промежуточное поле $K(\alpha_i, \alpha_k)$, порождённое двумя корнями α_i, α_k , необходимо совпадает со всем полем $K(\alpha_1, \dots, \alpha_q)$.

Задача 1. У метациклического неприводимого уравнения простой степени $q \neq 2$ над некоторым вещественным числовым полем K либо только один корень вещественный, либо все корни вещественны.

Задача 2. Неприводимое уравнение пятой степени, имеющее точно три вещественных корня, неразрешимо в радикалах.

Задача 3. Опираясь на результат, сформулированный в предыдущей задаче, доказать, что уравнение

$$x^5 - 4x + 2 = 0$$

неразрешимо в радикалах. [Для определения числа вещественных корней можно привлечь теоремы из главы 9, например, теорему Вейерштрасса о корнях непрерывной функции и теорему Ролля.]

§ 61. Вычисление группы Галуа. Уравнения с симметрической группой.

Следующий метод позволяет (по крайней мере теоретически) найти группу Галуа уравнения $f(x) = 0$ относительно поля Δ .

Пусть $\alpha_1, \dots, \alpha_n$ — корни уравнения. Образует с помощью неопределённых $u_1, \dots, u_n$ выражение

$$\vartheta = u_1\alpha_1 + \dots + u_n\alpha_n,$$

подвергнем коэффициенты u всем подстановкам s_u и составим произведение

$$F(z, u) = \prod_s (z - s_u \vartheta).$$

Это произведение, очевидно, является симметрической функцией корней и, следовательно, по § 26, может быть выражено через коэффициенты полинома $f(x)$. Разложим теперь $F(z, u)$ на неприводимые множители в $\Delta[u, z]$:

$$F(z, u) = F_1(z, u) F_2(z, u) \dots F_r(z, u).$$

Подстановки s_u , переводящие в себя какой-либо из этих множителей, скажем F_1 , образуют группу g . Мы утверждаем теперь, что g и есть группа Галуа заданного уравнения.

Доказательство. По присоединении всех корней полином F , а потому и F_1 , распадется на линейные множители $z - \sum u_i \alpha_i$, каждому из которых соответствует своё расположение корней α_i . Занумеруем теперь корни так, чтобы F_1 содержал множитель $z - (u_1\alpha_1 + \dots + u_n\alpha_n)$. В дальнейшем s_u всюду будет обозначать какую-либо подстановку величин u , а s_α — ту же подстановку корней α . Очевидно, тогда произведение $s_u s_\alpha$ оставляет $\vartheta = u_1\alpha_1 + \dots + u_n\alpha_n$ неизменным, т. е.

$$s_u s_\alpha \vartheta = \vartheta,$$

$$s_\alpha \vartheta = s_u^{-1} \vartheta.$$

Если s_u принадлежит к группе g , т. е. не изменяет F_1 , то s_u переводит каждый линейный множитель полинома F_1 , и в частности множитель $z - \vartheta$, в множитель этого же полинома. И обратно, если подстановка s_u переводит $z - \vartheta$ в некоторый другой линейный множитель полинома F_1 , то она преобразует F_1 в полином, неприводимый в $\Delta[u, z]$ и делящий $F(z, u)$, т. е. в один из F_j ; при этом F_j , обладая общим линейным множителем с F_1 , необходимо совпадает с F_1 ; тем самым s_u принадлежит в этом случае группе g . Таким образом, g состоит из подстановок величин u , переводящих $z - \vartheta$ снова в линейный множитель полинома F_1 .

Подстановки s_α группы Галуа уравнения $f(x) = 0$ суть те подстановки корней α , которые переводят величину

$$\vartheta = u_1\alpha_1 + \dots + u_n\alpha_n$$

в сопряжённые с ней величины, т. е. для которых $s_\alpha\vartheta$ удовлетворяет тому же неприводимому уравнению, что и ϑ ; иными словами, это — подстановки s_α , переводящие $z \rightarrow \vartheta$ в другие линейные множители полинома F_1 . Так как $s_\alpha\vartheta = s_\alpha^{-1}\vartheta$, то тогда и s_α^{-1} переводит $z \rightarrow \vartheta$ снова в линейный множитель полинома F_1 , т. е. s_α^{-1} , а тем самым и s_α , принадлежит группе g . Обратное также верно. Таким образом, искомая группа Галуа состоит из тех же самых подстановок, что и группа g , лишь применённых не к величинам u , а к корням α .

Этот метод нахождения группы Галуа интересен не столько практически, сколько по одному своему теоретическому следствию:

Пусть $\mathfrak{R}$ — область целостности с единицей и в $\mathfrak{R}$ имеет место теорема об однозначном разложении на простые множители. Пусть $\mathfrak{p}$ — простой идеал в $\mathfrak{R}$, $\bar{\mathfrak{R}} = \mathfrak{R}/\mathfrak{p}$ — факторкольцо по $\mathfrak{p}$, Δ и $\bar{\Delta}$ — поля отношений для $\mathfrak{R}$ и $\bar{\mathfrak{R}}$. Если тогда $f(x) = x^n + \dots$ — полином из $\mathfrak{R}[x]$ и $\bar{f}(x)$ — его образ при гомоморфном отображении $\mathfrak{R} \rightarrow \bar{\mathfrak{R}}$, оба — без кратных корней, то группа Галуа $\bar{g}$ уравнения $\bar{f} = 0$ относительно поля $\bar{\Delta}$ (как группа подстановок должным образом занумерованных корней) является подгруппой группы Галуа g уравнения $f = 0$.

Доказательство. Разложение полинома

$$F(z, u) = \prod_i (z - s_{u_i}\vartheta)$$

в произведение неприводимых в $\Delta[z, u]$ множителей $F_1 F_2 \dots F_k$ может быть, согласно § 23, выполнено уже в пределах области $\mathfrak{R}[z, u]$ и переносится тогда, в силу гомоморфизма, в $\bar{\mathfrak{R}}[z, u]$:

$$\bar{F}(z, u) = \bar{F}_1 \bar{F}_2 \dots \bar{F}_k.$$

Множители $\bar{F}_1, \dots$, быть может, ещё разложимы далее. Подстановки из группы g переводят F_1 , а потому также $\bar{F}_1$, в себя, остальные же подстановки величин u переводят $\bar{F}_1$ в $\bar{F}_2, \dots, \bar{F}_k$. Подстановки из группы $\bar{g}$ переводят некоторый неприводимый множитель полинома $\bar{F}_1$ в себя и, значит, не могут переводить $\bar{F}_1$ в $\bar{F}_2, \dots, \bar{F}_k$, а должны переводить $\bar{F}_1$ снова в $\bar{F}_1$. Тем самым $\bar{g}$ есть подгруппа группы g .

Эта теорема часто применяется для нахождения группы g . При этом идеал $\mathfrak{p}$ выбирают часто так, чтобы полином $f(x)$ распадался по модулю $\mathfrak{p}$, поскольку тогда группа Галуа $\bar{g}$ для $\bar{f}$ легче определяется.

Пусть, например, $\mathfrak{R}$ — кольцо целых чисел и $p = (p)$, где p — простое число. Пусть

$$f(x) \equiv \varphi_1(x) \varphi_2(x) \dots \varphi_h(x) \pmod{p}$$

— разложение $f(x)$ на простые множители по модулю p . Тогда

$$\bar{f} = \bar{\varphi}_1 \bar{\varphi}_2 \dots \bar{\varphi}_h.$$

Группа Галуа $\bar{g}$ полинома $\bar{f}(x)$ циклична, поскольку группа автоморфизмов поля Галуа всегда циклична (§ 37). Пусть

$$(1\ 2\dots j)(j+1\dots)\dots$$

— разложение на циклы образующей подстановки s группы $\bar{g}$. Так как области транзитивности группы $\bar{g}$ точно соответствуют неприводимым множителям полинома $\bar{f}$, то номера, входящие в циклы $(1\ 2\dots j), (\dots), \dots$, должны указывать корни полинома $\bar{\varphi}_1$, полинома $\bar{\varphi}_2, \dots$. Таким образом, коль скоро известны степени $j, k, \dots$ полиномов $\varphi_1, \varphi_2, \dots$, становится известным и тип подстановки s : s состоит тогда из j -членного цикла, k -членного цикла и т. д. А, так как, по доказанной выше теореме, при должной нумерации корней $\bar{g}$ есть подгруппа группы g , то и g должна содержать подстановку такого же типа.

Так, если, например, уравнение пятой степени с целыми коэффициентами разлагается по какому-либо простому модулю в произведение неприводимого множителя второй степени и неприводимого множителя третьей степени, то в его группе Галуа содержится подстановка типа (12)(345).

Пример. Пусть задано уравнение

$$x^5 - x - 1 = 0.$$

По модулю 2 левая часть разлагается в произведение

$$(x^2 + x + 1)(x^3 + x^2 + 1),$$

а по модулю 3 она неприводима, так как если бы она имела линейный или квадратичный множитель, то должна была бы иметь общий множитель с $x^9 - x$ (§ 37; задача 6), а значит, и с $x^5 - x$ или с $x^5 + x$, что, очевидно, не имеет места. Следовательно, группа Галуа этого уравнения содержит пятичленный цикл и произведение вида $(ik)(lmn)$. Третья степень последней подстановки равна (ik) . А эта транспозиция (ik) , трансформированная с помощью цикла (12345) и его степеней, даёт цепь транспозиций $(ik), (kp), (pq), (qr), (ri)$, в совокупности порождающих всю симметрическую группу $\mathfrak{S}_5$. Таким образом группа g — симметрическая.

Использованные нами приёмы можно применить к построению уравнений любой степени, имеющих своей группой Галуа соответ-

ствующую симметрическую группу, основываясь на следующей теореме:

Транзитивная группа подстановок n -ной степени, содержащая двучленный и $(n-1)$ -членный циклы, есть симметрическая группа.

Доказательство. Пусть $(1\ 2\ \dots\ n-1)$ — заданный по условию $(n-1)$ -членный цикл. В силу транзитивности, заданный по условию двучленный цикл (ij) может быть трансформирован в (kn) , где k — один из номеров от 1 до $n-1$. Трансформирование цикла (kn) с помощью цикла $(1\ 2\ \dots\ n-1)$ и его степеней даёт все циклы $(1n), (2n), \dots, (n-1\ n)$, а они в совокупности порождают всю симметрическую группу $\mathfrak{S}_n$.

Для того чтобы на основании этой теоремы построить уравнение n -ной степени ($n > 3$), группа Галуа которого симметрическая, выберем сначала полином n -ной степени f_1 , неприводимый по модулю 2, затем полином f_2 , распадающийся по модулю 3 на неприводимый множитель $(n-1)$ -й степени и линейный множитель, и, наконец, полином n -ной степени f_3 , разлагающийся по модулю 5 на квадратный множитель и один или два множителя нечётной степени (все — неприводимые по модулю 5). Всем этим требованиям можно удовлетворить, так как по каждому простому модулю существуют неприводимые полиномы любой степени (§ 37, задача 6). Наконец, выберем f так, чтобы

$$f \equiv f_1 \pmod{2},$$

$$f \equiv f_2 \pmod{3},$$

$$f \equiv f_3 \pmod{5},$$

что тоже всегда возможно; например, достаточно взять

$$f = -15f_1 + 10f_2 + 6f_3.$$

Группа Галуа тогда транзитивна (так как полином неприводим по модулю 2), содержит цикл типа $(1\ 2\ \dots\ n-1)$ и двучленный цикл, умноженный на циклы нечётного порядка. Возведя последнее произведение в надлежащую нечётную степень, мы получим чистый двучленный цикл, а тогда из доказанной выше теоремы и будет следовать, что рассматриваемая группа Галуа симметрическая.

Изложенный метод построения, разумеется, — далеко не единственный. Например, для достижения неприводимости уравнения и тем самым транзитивности группы, можно также воспользоваться теоремой Эйзенштейна (§ 24). Для уравнений нечётной степени $n > 3$ можно поступить ещё проще, озаботившись лишь, чтобы левая часть уравнения разлагалась по модулю 2 на множители степеней $n-1$ и 1, а по модулю 3 — на множители степеней $n-2$ и 2. Неприводимость тогда обеспечивается автоматически. Для всех чётных степеней > 6 мы достигнем того же результата, взяв левую часть, разлагающуюся по модулю 2 на множители тех

же степеней, как выше, а по модулю 3 — на множители степеней 2, 3 и $n-5$. Другие признаки и методы образования уравнений требуемого типа можно найти в статье Ph. Furtwängler'a в *Math. Ann.*, 85 (1922), 34—40. Существуют ли уравнения с рациональными коэффициентами, имеющие своей группой Галуа произвольно заданную группу подстановок, — является проблемой, не решённой в общем виде; см. по этому поводу E. Noether, *Gleichungen mit vorgeschriebener Gruppe. Math. Ann.*, 78 (1917), 221—229.

Задача 1. Какова группа Галуа (относительно поля рациональных чисел) уравнения

$$x^4 + 2x^2 + x + 3 = 0?$$

Задача 2. Построить уравнение шестой степени, имеющее своей группой Галуа симметрическую группу.

ГЛАВА ВОСЬМАЯ.

БЕСКОНЕЧНЫЕ РАСШИРЕНИЯ ПОЛЕЙ.

Каждое поле получается из своего простого поля путём конечного или бесконечного расширения. В главах 5 и 7 мы занимались изучением конечных расширений; в этой главе будут рассмотрены бесконечные расширения, причём сперва алгебраические, а затем трансцендентные. Первый параграф этой главы существенно опирается на понятия и результаты, излагаемые в «Добавлении», посвящённом частично упорядоченным множествам.

§ 62. Алгебраически замкнутые поля.

Среди алгебраических расширений заданного поля важную роль, естественно, играют *максимальные* алгебраические расширения, т. е. такие, которые уже не допускают дальнейшего алгебраического расширения. Существование таких расширений будет доказано в настоящем параграфе.

Для того чтобы Ω было максимальным алгебраическим расширением поля, необходимо, чтобы каждый полином в $\Omega[x]$ полностью распадался на линейные множители (так как в противном случае, согласно § 32, поле Ω можно было бы расширить дальше путём присоединения корня нелинейного простого полинома). Но это условие также достаточно. Действительно, если каждый полином в Ω распадается на линейные множители, то каждый элемент из алгебраического расширения Ω' поля Ω должен удовлетворять некоторому уравнению с коэффициентами из Ω , а значит (в силу разложимости левой части на линейные множители) — и некоторому линейному уравнению над Ω , т. е. должен содержаться уже в Ω ; тем самым $\Omega' = \Omega$, и Ω — максимальное алгебраическое расширение.

В соответствии с этим мы примем следующее определение:

Поле Ω называется алгебраически замкнутым, если в $\Omega[x]$ каждый полином распадается на линейные множители.

Этому равносильно также следующее определение: *поле Ω алгебраически замкнуто, если каждый полином из $\Omega[x]$, не являющийся константой, обладает по крайней мере одним корнем в Ω и, следовательно, по крайней мере одним линейным множителем в $\Omega[x]$.*

Действительно, если это условие выполнено, то в разложении произвольного полинома $f(x)$ на простые множители эти последние, необходимо, будут линейными.

«Основная теорема алгебры», к которой мы ещё вернёмся в § 69, утверждает, что поле комплексных чисел алгебраически замкнуто. Другим примером алгебраически замкнутого поля служит поле всех комплексных алгебраических чисел (т. е. всех тех комплексных чисел, которые удовлетворяют алгебраическим уравнениям с рациональными коэффициентами), поскольку комплексные корни уравнения с алгебраическими коэффициентами являются алгебраическими не только относительно поля алгебраических чисел, но даже и относительно поля рациональных чисел, т. е. сами суть алгебраические числа.

В настоящем параграфе мы покажем, что для всякого поля P можно чисто алгебраическим путём построить алгебраически замкнутое расширение. А именно, справедлива следующая, доказанная Штейницем, основная теорема:

Теорема существования. Для всякого поля P существует алгебраически замкнутое алгебраическое расширение Ω .

Доказательству этой теоремы мы предположим следующую лемму:

Лемма. Пусть Ω — алгебраическое расширение поля P . Для того чтобы Ω было алгебраически замкнутым, достаточно, чтобы все полиномы из $P[x]$ распадались в $\Omega[x]$ на линейные множители.

Доказательство. Пусть $f(x)$ — полином из $\Omega[x]$. Если бы он не распадался на линейные множители, то можно было бы, присоединив некоторый его корень α , прийти к собственному над полю Ω' . Так как α алгебраичен над Ω , а Ω алгебраично над P , то α алгебраичен и над P , т. е. является корнем некоторого полинома $g(x)$ из $P[x]$. Но последний полином распадается в $\Omega[x]$ на линейные множители. Таким образом, α есть корень некоторого линейного полинома из $\Omega[x]$ и, следовательно, лежит в Ω , в противоречие со сделанным предположением.

Приступим теперь к доказательству теоремы существования. Строим над полем P поля разложения для каждого полинома из области $P[x]$, причём считаем, что все эти поля не имеют попарно никаких общих элементов, кроме элементов из P . Мы получим некое множество конечных нормальных расширений поля P , среди которых, однако, безусловно будут встречаться эквивалентные над P . Оставив в нашем множестве лишь по одному полю из каждой совокупности эквивалентных между собою полей, мы придём к множеству конечных нормальных расширений поля P , обозначаемых через $\Sigma_\alpha, \Sigma_\beta, \Sigma_\gamma, \dots$, обладающих следующими двумя свойствами:

1) никакие два различных поля $\Sigma_\alpha, \Sigma_\beta$ не будут эквивалентными над P ,

и, на основании результатов § 35,

2) всякое конечное нормальное расширение поля P эквивалентно одному из полей Σ_α .

Среди полей Σ_α содержится, в частности, само поле P ; для него мы введём обозначение $P = \Sigma_0$.

Пусть поля Σ_α и Σ_β таковы, что в Σ_β содержится собственное подполе Σ_β^α ; эквивалентное полю Σ_α , причём подполе Σ_β^α будет в этом случае нормальным над P и будет внутри поля Σ_β однозначно определено. Если это предположение имеет место, назовём поле Σ_α *предшествующим* полю Σ_β и введём обозначение $\Sigma_\alpha < \Sigma_\beta$. Все требования, входящие в определение частично упорядоченного множества (см. Добавление), будут, очевидно, выполняться, т. е. *множество полей Σ_α оказывается при помощи отношения $<$ частично упорядоченным*. Так как из $\Sigma_\alpha < \Sigma_\beta$ следует, что степень поля Σ_α над P , равная степени поля Σ_β^α , должна быть строго меньше степени поля Σ_β , то *в частично упорядоченном множестве полей Σ_α выполняется условие минимальности*. В частности, в нашем множестве существует единственное поле, предшествующее всем остальным, а именно само P . С другой стороны, для любой пары полей $\Sigma_\alpha, \Sigma_\beta$ можно указать поле Σ_γ , следующее за ними обоими. Действительно, если поля Σ_α и Σ_β служат, соответственно, полями разложения для полиномов $f(x)$ и $g(x)$ из $P[x]$, то в качестве Σ_γ можно взять то из полей нашего множества, которое эквивалентно полю разложения для произведения $f(x)g(x)$.

Если $\Sigma_\beta < \Sigma_\gamma$, то, вообще говоря, существует несколько (притом лишь конечное число) изоморфных отображений поля Σ_β на подполе Σ_β^γ поля Σ_γ , устанавливающих эквивалентность этих полей над P . Будем считать все эти отображения как-то перенумерованными, причём положим, что эти нумерации отображений независимо выполнены для всех пар индексов β, γ , для которых $\Sigma_\beta < \Sigma_\gamma$ ¹⁾. Мы хотим теперь для каждой такой пары индексов β, γ выбрать одно из этих отображений, а именно $\varphi_{\beta\gamma}$, причём так, чтобы выполнялось следующее условие:

Если α, β, γ — любые индексы, для которых $\Sigma_\alpha < \Sigma_\beta < \Sigma_\gamma$, то

$$(1) \quad \varphi_{\alpha\gamma} = \varphi_{\alpha\beta} \varphi_{\beta\gamma}.$$

Отсюда будет следовать, если через $\varphi_{\alpha\beta}^{-1}$ обозначить отображение Σ_β^α на Σ_α , обратное отображению $\varphi_{\alpha\beta}$ (т. е. $\varphi_{\alpha\beta} \varphi_{\alpha\beta}^{-1}$ есть тождественное отображение поля Σ_α на себя), что на подполе Σ_β^α имеет место равенство

$$\varphi_{\beta\gamma} = \varphi_{\alpha\beta}^{-1} \varphi_{\alpha\gamma}.$$

¹⁾ Здесь используется, очевидно, аксиома вы 0 !

Покажем, что такой выбор отображений $\varphi_{\beta\gamma}$ возможен, причём, ввиду условия минимальности, этот выбор будем вести индукцией по индексу β .

Так как поле P содержится в каждом из полей Σ_γ , то для любого γ в качестве $\varphi_{0\gamma}$ возьмём тождественное отображение поля P на себя.

Пусть дан индекс β и пусть отображения $\varphi_{\alpha\gamma}$ с нужными свойствами уже выбраны для всех α , для которых $\Sigma_\alpha < \Sigma_\beta$, и для любых γ , для которых $\Sigma_\alpha < \Sigma_\gamma$. Для того чтобы определить отображение $\varphi_{\beta\gamma}$ для произвольного γ , для которого $\Sigma_\beta < \Sigma_\gamma$, поступим следующим образом. Всякое собственное нормальное подполе поля Σ_β имеет вид Σ_β^α , причём $\Sigma_\alpha < \Sigma_\beta$. Для каждого из таких α поле Σ_γ также обладает подполем Σ_γ^α . Отобразим Σ_β^α на Σ_γ^α при помощи отображения $\varphi_{\alpha\beta}^{-1}\varphi_{\alpha\gamma}$. Будут ли эти отображения для различных α и α' , для которых $\Sigma_\alpha < \Sigma_\beta$, $\Sigma_{\alpha'} < \Sigma_\beta$, согласованы между собой? Так как пересечение двух нормальных подполей поля Σ_β само будет нормальным, то достаточно рассмотреть такие два индекса α' , α , что $\Sigma_{\alpha'} < \Sigma_\alpha < \Sigma_\beta$. При отображении $\varphi_{\alpha\beta}^{-1}\varphi_{\alpha\gamma}$ подполя Σ_β^α на подполе Σ_γ^α содержащееся, очевидно, в $\Sigma_\beta^{\alpha'}$ подполе $\Sigma_\beta^{\alpha'}$ будет отображаться на $\Sigma_\gamma^{\alpha'}$. Покажем, что это отображение совпадает на $\Sigma_\beta^{\alpha'}$ с отображением $\varphi_{\alpha'\beta}^{-1}\varphi_{\alpha'\gamma}$. Действительно, так как для индекса α предположение индукции считается выполненным, то при отображении $\varphi_{\alpha\beta}$ подполе $\Sigma_\alpha^{\alpha'}$ отображается на подполе $\Sigma_\beta^{\alpha'}$ так же, как при отображении $\varphi_{\alpha'\alpha}^{-1}\varphi_{\alpha'\beta}$, и поэтому $\varphi_{\alpha\beta}^{-1}$ отображает Σ_β^α на $\Sigma_\alpha^{\alpha'}$ так же, как $(\varphi_{\alpha'\alpha}^{-1}\varphi_{\alpha'\beta})^{-1} = \varphi_{\alpha'\beta}^{-1}\varphi_{\alpha'\alpha}$. С другой стороны, снова по предположению индукции, при $\varphi_{\alpha\gamma}$ подполе $\Sigma_\alpha^{\alpha'}$ отображается на подполе $\Sigma_\gamma^{\alpha'}$ так же, как при $\varphi_{\alpha'\alpha}^{-1}\varphi_{\alpha'\gamma}$. Отсюда следует, что $\varphi_{\alpha\beta}^{-1}\varphi_{\alpha\gamma}$ отображает Σ_β^α на $\Sigma_\gamma^{\alpha'}$ так же, как

$$\varphi_{\alpha'\beta}^{-1}\varphi_{\alpha'\alpha} \cdot \varphi_{\alpha'\alpha}^{-1}\varphi_{\alpha'\gamma} = \varphi_{\alpha'\beta}^{-1}\varphi_{\alpha'\gamma}.$$

Этим доказано, что выбранные нами отображения собственных нормальных подполей Σ_β^α поля Σ_β на соответствующие подполя Σ_γ^α поля Σ_γ согласованы между собою. Эти отображения можно распространить, следовательно, на подполе Δ , порождённое в поле Σ_β всеми его собственными нормальными подполями. Если Δ совпадает с Σ_β , то этим мы уже определили отображение $\varphi_{\beta\gamma}$ поля Σ_β на подполе Σ_γ^β , удовлетворяющее условиям индукции. Если же Δ отлично от Σ_β и если Δ' — соответствующее ему подполе из Σ_γ , то $\Delta' \subset \Sigma_\gamma^\beta$ и построенное уже отображение Δ на Δ' , являющееся эквивалентностью над P , можно, на основании теоремы о продолжении изоморфизмов из § 35, продолжить до отображения поля Σ_β на подполе Σ_γ^β , устанавливающего эквивалентность над P этих полей. Если таких отображений несколько, то в качестве $\varphi_{\beta\gamma}$ возьмём то

из них, которое имеет наименьший номер в установленной заранее нумерации отображений поля Σ_β на подполе Σ_γ . Все условия индукции будут при этом, очевидно, выполнены.

Таким образом, на основании принципа индукции можно считать, что отображения $\varphi_{\beta\gamma}$, обладающие нужными свойствами, выбраны для всех пар индексов β, γ , для которых $\Sigma_\beta < \Sigma_\gamma$. Дополнительно обозначим через $\varphi_{\beta\beta}$ тождественное отображение поля Σ_β на себя; ясно, что на всяком подполе Σ_β^α отображение $\varphi_{\beta\beta}$ будет совпадать с отображением $\varphi_{\alpha\beta}^{-1} \varphi_{\alpha\beta}$.

Элементы x и y , взятые в некоторых полях Σ_α , различных или одном и том же, будут называться *эквивалентными*, если от x можно перейти к y , последовательно выполняя некоторую конечную цепь отображений вида $\varphi_{\beta\gamma}^{\pm 1}$. Это понятие эквивалентности будет, очевидно, рефлексивным, симметричным и транзитивным и поэтому множество всех элементов всех полей Σ_α распадается на непересекающиеся классы эквивалентных элементов. Будем называть эти классы *нитьями* и обозначать их буквами $\xi, \eta, \zeta, \dots$; условимся также говорить, что *нить ξ проходит через элемент x* , если x содержится в ξ , а также, что *нить ξ проходит через поле Σ_α* , если ξ проходит через некоторый элемент этого поля.

Если элементы x и y эквивалентны, то можно считать, что в цепи отображений, переводящих x в y , не стоят рядом два отображения с одинаковым показателем ($+1$ или -1). Действительно, отображение $\varphi_{\alpha\beta} \varphi_{\beta\gamma}$ (а средние индексы не могут в этом случае не совпадать!) можно заменить через $\varphi_{\alpha\gamma}$ ввиду равенства (1). С другой стороны, если стоят рядом два отображения с показателем -1 , то это может быть лишь случай $\varphi_{\beta\gamma}^{-1} \varphi_{\alpha\beta}^{-1}$, что, снова ввиду (1), можно заменить через $\varphi_{\alpha\gamma}^{-1}$.

Далее, отображение $\varphi_{\gamma\alpha}^{-1} \varphi_{\gamma\beta}$ всегда можно заменить отображением вида $\varphi_{\alpha\delta} \varphi_{\beta\delta}^{-1}$. Для этого достаточно выбрать δ так, чтобы поле Σ_δ следовало за полями Σ_α и Σ_β , и проверить, опираясь на условие (1), что на подполе Σ_α^γ имеет место равенство

$$\varphi_{\gamma\alpha}^{-1} = \varphi_{\alpha\delta} \varphi_{\gamma\delta}^{-1},$$

а на поле Σ_γ — равенство

$$\varphi_{\gamma\beta} = \varphi_{\gamma\delta} \varphi_{\beta\delta}^{-1}.$$

Применяя несколько раз результаты двух предшествующих абзацев, мы получим, что *если элементы x и y эквивалентны, то x переводится в y некоторым отображением вида $\varphi_{\alpha\gamma} \varphi_{\beta\gamma}^{-1}$* , где, впрочем, может быть $\alpha = \gamma$ или $\beta = \gamma$ (случай, когда x переводится в y одним отображением $\varphi_{\alpha\beta}^{\pm 1}$). Индекс γ может быть при этом любым, удовлетворяющим условию $\Sigma_\alpha < \Sigma_\gamma$, $\Sigma_\beta < \Sigma_\gamma$. Действительно,

если индекс γ' удовлетворяет такому же условию, т. е. $\Sigma_\alpha < \Sigma_{\gamma'}$, $\Sigma_\beta < \Sigma_{\gamma'}$, и если индекс δ таков, что $\Sigma_\gamma < \Sigma_\delta$, $\Sigma_{\gamma'} < \Sigma_\delta$, то, применяя несколько раз условие (1), мы получим, что на поле Σ_α справедливы равенства

$$\begin{aligned}\varphi_{\alpha\gamma}\varphi_{\beta\gamma}^{-1} &= (\varphi_{\alpha\delta}\varphi_{\gamma\delta}^{-1})(\varphi_{\beta\delta}\varphi_{\gamma\delta}^{-1})^{-1} = \varphi_{\alpha\delta}\varphi_{\beta\delta}^{-1} = (\varphi_{\alpha\gamma'}\varphi_{\gamma'\delta})^{-1}(\varphi_{\beta\gamma'}\varphi_{\gamma'\delta})^{-1} = \\ &= \varphi_{\alpha\gamma'}\varphi_{\beta\gamma'}^{-1}.\end{aligned}$$

Теперь легко устанавливается следующий важный результат: *никакая нить не может проходить через два различных элемента одного и того же поля Σ_α* . Действительно, если элементы x и y эквивалентны и лежат в одном поле Σ_α , то, по доказанному, x переводится в y некоторым отображением $\varphi_{\alpha\gamma}\varphi_{\alpha\gamma}^{-1}$, равным тождественному отображению $\varphi_{\alpha\alpha}$, а поэтому $x = y$.

Обозначим теперь множество всех нитей через Ω и определим в нём операции сложения и умножения. Для этого заметим, что если даны нити ξ и η , то можно указать поле Σ_α , через которое они обе проходят: если ξ проходит через поле Σ_β , η — через поле $\Sigma_{\gamma'}$, то в качестве Σ_α можно взять любое поле, следующее за Σ_β и $\Sigma_{\gamma'}$. Пусть нить ξ проходит в поле Σ_α через элемент x , нить η — через элемент y . Тогда суммой $\xi + \eta$ этих нитей назовём нить, проходящую через элемент $x + y$, произведением $\xi\eta$ — нить, проходящую через элемент xy . Эти определения не зависят от выбора поля Σ_α : если нити ξ и η проходят, соответственно, через элементы x' и y' некоторого другого поля Σ_β и если поле $\Sigma_{\gamma'}$ следует за обоими полями Σ_α и Σ_β , то, как мы знаем, x переводится в x' и y — в y' при помощи одного и того же отображения $\varphi_{\alpha\gamma}\varphi_{\beta\gamma}^{-1}$, а так как это отображение изоморфное, то оно переводит $x + y$ в $x' + y'$ и xy в $x'y'$; элементы $x + y$ и $x' + y'$ (а также xy и $x'y'$) определяют, следовательно, одну и ту же нить.

Множество Ω является полем относительно этих операций сложения и умножения. Действительно, всякое требование, входящее в определение поля, относится к конечному числу элементов (двум или трём). Однако для всякой конечной системы нитей можно указать такое поле Σ_α , через которое все эти нити проходят, после чего остаётся сослаться на справедливость соответствующего требования в этом поле Σ_α .

Поле P является подполем поля Ω . Действительно, нить, проходящая через элемент x из поля P , состоит лишь из самого элемента x .

Для всякого поля Σ_α можно указать в поле Ω подполе Σ'_α , эквивалентное полю Σ_α над P . Действительно, это будет подполе, составленное всеми нитями, проходящими через поле Σ_α , так как соответствие, сопоставляющее всякому элементу из Σ_α нить, проходящую через этот элемент, будет, как доказано выше, взаимно однозначным и, по определению операций над нитями, изоморфным.

Всякая нить содержится в некотором подполе Σ'_α , т. е. всякий элемент из Ω содержится в некотором конечном расширении поля P и поэтому алгебраичен над P . Поле Ω является, следовательно, алгебраическим расширением поля P . С другой стороны, так как для всякого конечного нормального расширения поля P можно указать эквивалентное ему подполе поля Ω , то над Ω всякий полином из $P[x]$ распадается на линейные множители, а поэтому, ввиду доказанной выше леммы, поле Ω алгебраически замкнуто.

Доказательство теоремы существования закончено. Важным дополнением к ней служит следующая

Теорема единственности. *Каждые два алгебраически замкнутые алгебраические расширения Ω , Ω' поля P эквивалентны над P .*

Доказательство. Будем обозначать конечные нормальные расширения поля P , содержащиеся в поле Ω , символами Σ_α , $\Sigma_\beta, \dots$; ввиду алгебраичности Ω над P всякий элемент из Ω лежит хотя бы в одном из подполей Σ_α , т. е. эти подполя покрывают всё поле Ω . Подполя Σ_α составляют, очевидно, по отношению к теоретико-множественному включению частично упорядоченное множество, удовлетворяющее условию минимальности.

Для всякого подполя Σ_α можно указать в поле Ω' , ввиду алгебраической замкнутости последнего, эквивалентное с Σ_α подполе Σ'_α , и притом только одно. Эквивалентность между Σ_α и Σ'_α можно установить несколькими способами (впрочем, лишь конечным числом их); будем считать отображения, устанавливающие эту эквивалентность, как-то перенумерованными. Мы хотим теперь для каждого α выбрать одно из этих отображений, φ_α , причём так, чтобы выполнялось следующее условие:

Если $\Sigma_\alpha \subset \Sigma_\beta$, то отображение φ_β должно быть продолжением отображения φ_α , т. е. на подполе Σ_α должно иметь место равенство $\varphi_\beta = \varphi_\alpha$.

Будем, ввиду условия минимальности, выбирать эти отображения φ_α , ведя индукцию по индексу α . Для самого поля $P = \Sigma_0$ в качестве φ_0 возьмём тождественное отображение P на себя (напоминаем, что P содержится и в Ω , и в Ω'). Пусть теперь дано подполе Σ_β , причём для всех подполей Σ_α , содержащихся в Σ_β , выбор отображений φ_α , удовлетворяющих поставленным условиям, уже выполнен. Так как, по условию, эти отображения φ_α согласованы между собой, то их можно распространить на подполе Δ , порождённое в Σ_β всеми Σ_α , содержащимися в Σ_β . Если Δ совпадает с Σ_β , то этим мы уже определили отображение φ_β подполя Σ_β на подполе Σ'_β , удовлетворяющее поставленным условиям. Если же Δ отлично от Σ_β и если Δ' — соответствующее ему подполе в Ω' , то $\Delta' \subset \Sigma'_\beta$ и построенное уже отображение Δ на Δ' , являющееся эквивалентностью над P , можно, ввиду § 35, продолжить до отображения Σ_β на Σ'_β ; в качестве

φ_β можно взять то из этих продолжений, которое имеет наименьший номер.

Отображения φ_β можно считать, следовательно, выбранными для всех Σ_β . Так как эти отображения согласованы между собою, а подполя Σ_β покрывают всё поле Ω , то можно определить отображение φ всего поля Ω в поле Ω' , являющееся изоморфным и оставляющее элементы поля P неподвижными: для этого образом элемента x из Ω при отображении φ нужно считать его образ при любом отображении φ_β , если индекс β таков, что x содержится в Σ_β .

Отображение φ , являющееся эквивалентностью над P , отображает поле Ω на всё поле Ω' . Действительно, ввиду алгебраической замкнутости Ω его образ при отображении φ также будет алгебраически замкнутым, а поэтому не может быть собственным подполем поля Ω' ввиду алгебраичности Ω' над P . Этим заканчивается доказательство теоремы единственности.

Приведём ещё одно доказательство теоремы существования весьма простое и прозрачное, но опирающееся на одно утверждение, которое может быть доказано (притом очень легко) лишь при помощи теоремы Цермело (см. Добавление¹⁾). Докажем сперва следующее утверждение:

Для всякого поля P существует алгебраическое расширение P' , в котором для каждого неприводимого полинома из $P[x]$ содержится хотя бы один корень.

Доказательство. Сопоставим каждому неприводимому нелинейному полиному $f(x)$ из кольца $P[x]$ новое неизвестное u_f и построим кольцо полиномов $P[\dots, u_f, \dots]$ над полем P относительно всех неизвестных u_f . Среди элементов этого кольца содержатся, в частности, элементы $f(u_f)$ для всех неприводимых нелинейных полиномов f . Пусть $\mathfrak{m}$ — идеал, порождённый в кольце $P[\dots, u_f, \dots]$ всеми $f(u_f)$. Этот идеал не содержит единицы: если бы имело место соотношение

$$1 = \varphi_1 \cdot f_1(u_{f_1}) + \varphi_2 \cdot f_2(u_{f_2}) + \dots + \varphi_k \cdot f_k(u_{f_k}),$$

где $\varphi_1, \varphi_2, \dots, \varphi_k$ — полиномы из $P[\dots, u_f, \dots]$, то оно оставалось бы справедливым и над расширением поля P , полученным присоединением корней полиномов $f_1, f_2, \dots, f_k$, а поэтому должно было бы сохраняться и при замене неизвестных $u_{f_1}, u_{f_2}, \dots, u_{f_k}$ корнями соответствующих полиномов $f_1, f_2, \dots, f_k$, что, однако, привело бы к равенству $1 = 0$.

Опираясь на теорему Цермело, можно показать, что идеал $\mathfrak{m}$ содержится в некотором максимальном идеале $\mathfrak{m}'$ кольца $P[\dots, u_f, \dots]$, отличным от самого кольца. Факторкольцо $P[\dots, u_f, \dots]/\mathfrak{m}'$ будет уже полем; обозначим его через P' . Можно считать, что в P' содержится основное поле P : действительно, пересечение P и $\mathfrak{m}'$ равно, очевидно, нулю. Всякий неприводимый нелинейный полином $f(x)$ из кольца $P[x]$ обладает в поле P' корнем — этим корнем служит, очевидно, смежный класс $u_f + \mathfrak{m}'$. Наконец присоединение всех этих корней к полю P порождает, очевидно, всё поле P' , а поэтому P' алгебраично над P .

Доказательство теоремы существования проходит теперь очень легко. Строим возрастающую последовательность полей

$$P = P^{(0)} \subset P' \subset P'' \subset \dots \subset P^{(n)} \subset \dots,$$

¹⁾ Это доказательство сообщил редактору И. Р. Шафаревич.

где всякое поле $P^{(n)}$ есть алгебраическое расширение поля $P^{(n-1)}$, $n=1, 2, \dots$, причём всякий полином, неприводимый над $P^{(n-1)}$, обладает в $P^{(n)}$ хотя бы одним корнем. Все поля $P^{(n)}$ будут алгебраическими и над P , как легко доказать индукцией по n . Алгебраическим над P будет, следовательно, и их объединение, которое мы обозначим через Ω ; оно будет, очевидно, полем. Поле Ω уже алгебраически замкнуто. Действительно, если бы над Ω существовал неприводимый нелинейный полином $f(x)$, то он был бы полиномом (притом также неприводимым) уже над некоторым полем $P^{(n)}$; но тогда в $P^{(n+1)}$ для него существовал бы корень, в противоречие с его неприводимостью.

Важность алгебраически замкнутых расширений заключается в том, что они содержат, с точностью до эквивалентности, все вообще возможные алгебраические расширения. Точнее:

Если Ω — алгебраически замкнутое алгебраическое расширение поля P и Σ — какое-либо алгебраическое расширение поля P , то в Ω содержится расширение Σ_0 поля P , эквивалентное Σ .

Доказательство. Пусть Ω' — алгебраически замкнутое алгебраическое расширение поля Σ ; Ω' алгебраично также относительно P и потому эквивалентно полю Ω . Но при изоморфизме, переводящем Ω' в Ω и оставляющем все элементы из P на месте, поле Σ , в частности, переходит в некоторое эквивалентное ему подполе Σ_0 поля Ω .

Если мы примем за исходное поле P поле рациональных чисел Γ , то конструкция, изложенная при доказательстве основной теоремы, даст поле Ω , называемое *полем всех алгебраических чисел* (см. также § 69). Его подполя, т. е. алгебраические расширения поля Γ , называют *алгебраическими числовыми полями*. Таким же образом, исходя из поля $GF(p)$ классов вычетов по модулю p , строят поле $\Omega(p)$, охватывающее все поля Галуа характеристики p .

Задача. Доказать существование и единственность расширения поля P , получающегося путём присоединения всех корней заданного множества полиномов из $P[x]$.

§ 63. Простые трансцендентные расширения.

Каждое простое трансцендентное расширение поля Δ , как мы знаем, эквивалентно полю отношений $\Delta(x)$ области полиномов $\Delta[x]$. Поэтому мы изучим это поле отношений

$$\Omega = \Delta(x).$$

Элементами поля Ω являются рациональные функции

$$\eta = \frac{f(x)}{g(x)},$$

которые можно предполагать записанными в несократимом виде (с взаимно простыми f и g). Наибольшая из степеней $f(x)$ и $g(x)$ называется *степенью функции* η .

Теорема. Каждая функция η степени n , не являющаяся константой, трансцендентна относительно поля Δ , и $\Delta(x)$ алгебраично степени n над $\Delta(\eta)$.

Доказательство. Пусть $\eta = \frac{f(x)}{g(x)}$ — представление функции η в несократимом виде. Тогда x удовлетворяет уравнению

$$g(x) \cdot \eta - f(x) = 0$$

с коэффициентами из $\Delta(\eta)$. Все эти коэффициенты одновременно не могут быть равны нулю. Действительно, если бы это имело место, то, в частности, для отличного от нуля коэффициента a_k полинома $g(x)$ и коэффициента b_k при той же степени x в полиноме $f(x)$ мы имели бы

$$a_k \eta - b_k = 0,$$

откуда $\eta = \frac{b_k}{a_k} = \text{const}$, что, однако, противоречит предположению. Таким образом, x является алгебраическим относительно $\Delta(\eta)$.

Если бы теперь η было алгебраическим относительно Δ , то и x было бы алгебраическим относительно Δ , что, однако, неверно. Тем самым η трансцендентно. x является корнем полинома в $\Delta(\eta)[z]$

$$g(z)\eta - f(z),$$

имеющего степень n . Этот полином неприводим в $\Delta(\eta)[z]$. Действительно, в противном случае он, согласно § 23, был бы приводим также в $\Delta[\eta, z]$; но так как он линеен относительно η , то один из множителей должен был бы зависеть лишь от z , но не от η ; однако такого множителя быть не может, поскольку $g(z)$ и $f(z)$ взаимно простые.

Тем самым x является алгебраическим степени n относительно $\Delta(\eta)$. Отсюда и следует, что $(\Delta(x) : \Delta(\eta)) = n$.

Отметим ещё для дальнейшего, что полином

$$g(z)\eta - f(z)$$

не имеет множителей, которые зависели бы только от z (т. е. лежали бы в $\Delta[z]$). Это останется в силе и при замене η его значением $\frac{f(x)}{g(x)}$ и умножении указанного полинома на $g(x)$; тем самым полином

$$g(z)f(x) - f(z)g(x)$$

из $\Delta[x, z]$ не имеет множителей, зависящих только от z .

Из доказанной теоремы вытекают три следствия:

1. Степень функции $\eta = \frac{f(x)}{g(x)}$ зависит только от полей $\Delta(\eta)$ и $\Delta(x)$, но не от специального выбора образующей x последнего поля.

2. Совпадение полей $\Delta(\eta)$ и $\Delta(x)$, т. е. равенство $\Delta(\eta) = \Delta(x)$, имеет место тогда и только тогда, когда η имеет степень 1, т. е. дробно-линейно. Иными словами: образующими поля $\Delta(x)$ являются все дробно-линейные функции от x и только они.

3. Автоморфизм поля $\Delta(x)$, оставляющий элементы из Δ на месте, должен переводить x снова в образующую поля. И обратно, переводя x в другую образующую поля $\bar{x} = \frac{ax+b}{cx+d}$ и каждый полином $\varphi(x)$ в $\varphi(\bar{x})$, мы получим автоморфизм, оставляющий все элементы из Δ на месте. Таким образом:

Все относительные автоморфизмы поля $\Delta(x)$ над Δ суть дробно-линейные подстановки

$$\bar{x} = \frac{ax+b}{cx+d}, \quad ad-bc \neq 0.$$

Важное значение для некоторых геометрических исследований имеет следующая

Теорема Люрота. Каждое промежуточное поле Σ , такое, что $\Delta \subset \Sigma \subseteq \Delta(x)$, является простым трансцендентным расширением поля Δ .

Доказательство. Элемент x должен быть алгебраическим относительно Σ ; действительно, если η — произвольный элемент поля Σ , не содержащийся в Δ , то x , как было показано, является алгебраическим относительно $\Delta(\eta)$, а значит, тем более относительно Σ . Пусть

$$(1) \quad f_0(z) = z^n + a_1 z^{n-1} + \dots + a_n$$

— неприводимый в $\Sigma[z]$ полином со старшим коэффициентом 1, имеющий корнем x . Определим строение этого полинома $f_0(z)$.

Коэффициенты a_i суть рациональные функции от x . Умножением на общий знаменатель можно сделать их целыми рациональными, добившись при этом, чтобы полученный полином

$$f(x, z) = b_0(x) z^n + b_1(x) z^{n-1} + \dots + b_n(x)$$

был примитивным относительно x (см. § 23). Пусть m — степень этого неприводимого полинома относительно x и n — степень относительно z .

Все коэффициенты $a_i = \frac{b_i}{b_0}$ полинома (1) не могут быть независимыми от x , так как в противном случае x было бы алгебраическим относительно Δ ; таким образом, один из них, скажем,

$$\vartheta = a_i = \frac{b_i(x)}{b_0(x)},$$

или, в несократимой форме,

$$\vartheta = \frac{g(x)}{h(x)}$$

должен действительно зависеть от x . $g(x)$ и $h(x)$ имеют степени $\leq m$. Полином

$$g(z) - \vartheta h(z) = g(z) - \frac{g(x)}{h(x)} h(z)$$

(отличный от нуля) имеет корень $z = x$ и потому делится в $\Sigma[z]$ на $f_0(z)$. При переходе, по § 23, от этих полиномов, рациональных относительно x , к целым рациональным и примитивным относительно x полиномам указанная делимость сохраняется, и мы получим:

$$h(x)g(z) - g(x)h(z) = q(x, z)f(x, z).$$

Левая часть имеет относительно x степень $\leq m$. Но в правой части уже f имеет степень m . Отсюда следует, что степень левой части равна m и что $q(x, z)$ не зависит от x . Однако, левая часть не обладает множителем, зависящим только от z (см. выше); следовательно, $q(x, z)$ есть константа:

$$h(x)g(z) - g(x)h(z) = q \cdot f(x, z).$$

Тем самым, поскольку константа q роли не играет, строение полинома $f(x, z)$ определено. Степень $f(x, z)$ относительно x равна m ; следовательно (в силу симметрии) и степень относительно z равна m , так что $m = n$. По крайней мере один из полиномов $g(x)$ и $h(x)$ обладает наивысшей степенью m ; следовательно, и ϑ как функция от x должно иметь степень m .

Таким образом, с одной стороны,

$$(\Delta(x) : \Delta(\vartheta)) = m,$$

с другой

$$(\Delta(x) : \Sigma) = m,$$

и так как $\Delta(\vartheta)$ содержится в Σ , то

$$\begin{aligned} (\Sigma : \Delta(\vartheta)) &= 1, \\ \Sigma &= \Delta(\vartheta), \end{aligned}$$

что и требовалось доказать.

Теорема Люрота имеет следующее значение для алгебраической геометрии.

Плоская (неприводимая) алгебраическая кривая $F(\xi, \eta) = 0$ называется *рациональной*, если её точки, за конечным числом исключений, могут быть представлены рациональными параметрическими уравнениями

$$\begin{aligned} \xi &= f(t), \\ \eta &= g(t). \end{aligned}$$

Но может случиться, что каждая точка кривой (за конечным числом возможных исключений) соответствует нескольким значениям t . (Пример:

$$\begin{aligned} \xi &= t^2, \\ \eta &= t^2 + 1; \end{aligned}$$

значениям t и $-t$ соответствует одна и та же точка.) Однако, в силу теоремы Люрота, этого всегда можно избежать искусным

выбором параметра. Пусть, в самом деле, Δ — поле, содержащее коэффициенты функций f , g , и t сперва — неизвестная. $\Sigma = \Delta(f, g)$ есть подполе поля $\Delta(t)$. Если t' — примитивный элемент в Σ (теорема Люрота), то, скажем,

$$f(t) = f_1(t') \quad (\text{рационально}),$$

$$g(t) = g_1(t') \quad (\text{рационально}),$$

$$t' = \varphi(f, g) = \varphi(\xi, \eta),$$

и легко проверить, что новое параметрическое представление

$$\xi = f_1(t'),$$

$$\eta = g_1(t')$$

определяет ту же кривую, причём, так как знаменатель функции $\varphi(x, y)$ обращается в нуль лишь для конечного числа точек кривой, то каждой точке кривой (за исключением, самое большее, конечного их числа) соответствует только одно значение t' .

Задача. Если $\Delta(x)$ является нормальным полем над $\Delta(\eta)$, то полином (1) распадается над $\Delta(x)$ на линейные множители. Все эти линейные множители получаются из одного из них, скажем, из $z - x$ с помощью дробно-линейных преобразований неизвестного x . Эти линейные преобразования образуют конечную группу, оставляют функцию $\vartheta = \frac{g(x)}{h(x)}$ инвариантной и вполне характеризуются этим свойством.

§ 64. Степень трансцендентности.

Пусть Ω — расширение некоторого фиксированного поля P . Элемент v из Ω называется *алгебраически зависимым* от $u_1, \dots, u_n$, если v является алгебраическим относительно поля $P(u_1, \dots, u_n)$, т. е. если v удовлетворяет алгебраическому уравнению

$$a_0(u) v^g + a_1(u) v^{g-1} + \dots + a_g(u) = 0,$$

коэффициенты которого $a_0(u), \dots, a_g(u)$ суть полиномы от $u_1, \dots, u_n$ с коэффициентами из P и не все равны нулю.

Алгебраическая зависимость обладает следующими основными свойствами, совершенно аналогичными основным свойствам линейной зависимости (ср. § 33):

Основная теорема 1. Каждое u_i ($i = 1, \dots, n$) алгебраически зависит от $u_1, \dots, u_n$.

Основная теорема 2. Если v алгебраически зависит от $u_1, \dots, u_n$, но не от $u_1, \dots, u_{n-1}$, то u_n алгебраически зависит от $u_1, \dots, u_{n-1}$ и v .

Доказательство. Будем считать $u_1, \dots, u_{n-1}$ присоединёнными к основному полю. Тогда v алгебраически зависит от u_n , т. е. имеет место алгебраическое соотношение

$$(1) \quad a_0(u_n) v^g + a_1(u_n) v^{g-1} + \dots + a_g(u_n) = 0.$$

Располагая левую часть этого уравнения по степеням u_n , получим:

$$(2) \quad b_0(v) u_n^h + b_1(v) u_n^{h-1} + \dots + b_h(v) = 0.$$

По предположению, v трансцендентно относительно основного поля $P(u_1, \dots, u_{n-1})$. Следовательно, каждый из полиномов $b_0(v), \dots, b_h(v)$ либо тождественно по v равен нулю, либо $\neq 0$. Но все эти полиномы не могут быть тождественно равны нулю, так как иначе и левая часть уравнения (1) была бы тождественно равна нулю, т. е. мы имели бы $a_0(u_n) = a_1(u_n) = \dots = a_g(u_n) = 0$, вопреки предположению. Следовательно, в (2) не все коэффициенты $b_k(v)$ равны нулю. А тогда u_n в силу уравнения (2) алгебраически зависит от v относительно основного поля $P(u_1, \dots, u_{n-1})$.

Основная теорема 3. Если w алгебраически зависит от $v_1, \dots, v_s$, а каждое v_j ($j=1, \dots, s$) алгебраически зависит от $u_1, \dots, u_n$, то w алгебраически зависит от $u_1, \dots, u_n$.

Доказательство. Если w алгебраично относительно поля $P(v_1, \dots, v_s)$, а значит, и относительно поля $P(u_1, \dots, u_n, v_1, \dots, v_s)$, последнее же поле, в свою очередь, алгебраично над $P(u_1, \dots, u_n)$, то по § 35 и w алгебраично относительно $P(u_1, \dots, u_n)$, что и требовалось доказать.

Так как теперь доказано выполнение тех же основных теорем, что и для линейной зависимости, то справедливы также все выведенные из них в § 33 следствия, с заменой линейной зависимости алгебраической. Мы называем элементы $u_1, \dots, u_n$ алгебраически независимыми, если никакой из них не зависит алгебраически от остальных. Две системы $\{u_1, \dots, u_n\}$ и $\{v_1, \dots, v_s\}$ называются (алгебраически) эквивалентными, если каждое v_k алгебраически зависит от $u_1, \dots, u_n$ и каждое u_i — от $v_1, \dots, v_s$. Каждая конечная система $\{u_1, \dots, u_n\}$ эквивалентна некоторой своей алгебраически независимой подсистеме (следствие 3). Каждые две эквивалентные алгебраически независимые системы $\{u_1, \dots, u_r\}$ и $\{v_1, \dots, v_s\}$ состоят из одинакового числа элементов (следствие 5).

Говорят, что множество $\mathfrak{M}$ (в частности, поле Ω) имеет конечную степень трансцендентности относительно поля P , если все элементы этого множества алгебраически зависят от конечного их числа. Тогда существует алгебраический базис множества $\mathfrak{M}$, т. е. такая алгебраически независимая подсистема $\{u_1, \dots, u_r\}$, от которой алгебраически зависят все элементы множества $\mathfrak{M}$. Число r базисных элементов не зависит от специального выбора базиса и называется степенью трансцендентности множества $\mathfrak{M}$. Степень трансцендентности есть максимальное число алгебраически независи-

мых элементов множества. Подмножество множества $\mathfrak{M}$ имеет самое большее ту же степень трансцендентности, что и всё множество $\mathfrak{M}$, и всякий алгебраический базис подмножества может быть дополнен до алгебраического базиса всего множества (ср. § 33, задача 2).

Теорема. Элементы $u_1, \dots, u_r$ алгебраически независимы тогда и только тогда, когда из равенства

$$f(u_1, \dots, u_r) = 0,$$

где f — полином с коэффициентами из P , необходимо следует обращение в нуль всех коэффициентов этого полинома.

Доказательство. Если из равенства $f(u_1, \dots, u_r) = 0$ вытекает тождественное обращение полинома f в нуль, то ясно, что ни один из элементов u_i не может алгебраически зависеть от остальных u_j . Пусть теперь, обратно, $u_1, \dots, u_r$ алгебраически независимы. Если тогда

$$f(u_1, \dots, u_r) = 0,$$

то коэффициенты $f_i(u_1, \dots, u_{r-1})$ в разложении полинома f по степеням u_r равны нулю. Располагая эти коэффициенты по степеням u_{r-1} и рассуждая таким же образом дальше, мы получим в конце концов, что все коэффициенты полинома f должны быть равны нулю.

По этой теореме элементы $u_1, \dots, u_r$ в случае, когда они алгебраически независимы, не связаны друг с другом никакими алгебраическими уравнениями. Поэтому их называют также *независимыми трансцендентными*. Таким образом, степень трансцендентности поля Ω относительно P есть максимальное число независимых трансцендентных, содержащихся в Ω .

Если $u_1, \dots, u_r$ алгебраически независимы и $z_1, \dots, z_r$ — неизвестные над P , то каждому полиному $f(z_1, \dots, z_r)$ с коэффициентами из P можно взаимно однозначно поставить в соответствие полином $f(u_1, \dots, u_r)$. Поэтому $P[z_1, \dots, z_r] \cong P[u_1, \dots, u_r]$. Из изоморфизма этих колец полиномов следует изоморфизм их полей отношений:

$$P(z_1, \dots, z_r) \cong P(u_1, \dots, u_r).$$

Таким образом, независимые трансцендентные $u_1, \dots, u_r$ ведут себя алгебраически совершенно так же, как r неизвестных $z_1, \dots, z_r$.

Расширение поля, получающееся путём присоединения конечного или бесконечного числа алгебраически независимых величин $u_1, \dots, u_r$, называется *чисто трансцендентным расширением*.

Если Ω — расширение поля P , имеющее конечную степень трансцендентности, и $u_1, \dots, u_r$ — алгебраический базис поля Ω , то каждый элемент из Ω является алгебраическим над $P(u_1, \dots, u_r)$. Иными словами:

Каждое расширение Ω поля P , имеющее конечную степень трансцендентности, может быть получено путём чисто трансцендентного расширения $P(u_1, \dots, u_r)$ и последующего алгебраического расширения.

Пользуясь методом полного упорядочения, Штейнц доказал эту теорему не только для расширений с конечной степенью трансцендентности, но вообще для произвольных трансцендентных расширений. Этой теоремой Штейнц глубоко вскрывается строение трансцендентных расширений. Однако для применений гораздо большее значение имеют поля с конечной степенью трансцендентности, исследованием которых мы здесь и ограничились.

Задача. Расширение, образующееся в результате двух последовательных расширений, имеющих конечные степени трансцендентности s и t , имеет степень трансцендентности $s+t$.

§ 65. Дифференцирование алгебраических функций.

Данное в § 20 определение производной полинома $f(x)$ без труда распространяется на рациональные функции одного неизвестного

$$\varphi(x) = \frac{f(x)}{g(x)}$$

с коэффициентами из поля P . Действительно, образуем разность

$$(1) \quad \varphi(x+h) - \varphi(x) = \frac{f(x+h)g(x) - f(x)g(x+h)}{g(x)g(x+h)}.$$

Числитель этой дроби обращается в нуль при $h=0$ и потому содержит множитель h . Разделив обе части на h , получим:

$$\frac{\varphi(x+h) - \varphi(x)}{h} = \frac{q(x, h)}{g(x)g(x+h)}.$$

Правая часть является рациональной функцией от h , имеющей при $h=0$ определённое значение, так как знаменатель не обращается в нуль. Это значение мы и назовём *производной* $\varphi'(x)$ рациональной функции $\varphi(x)$:

$$(2) \quad \varphi'(x) = \frac{d\varphi(x)}{dx} = \frac{q(x, 0)}{[g(x)]^2}.$$

Для фактического вычисления $q(x, 0)$ расположим числитель правой части формулы (1) по возрастающим степеням h , разделим на h и положим $h=0$; в результате получим:

$$q(x, 0) = f'(x)g(x) - f(x)g'(x).$$

Подставляя это в (2), придём к известной формуле для производной частного:

$$\frac{d}{dx} \frac{f(x)}{g(x)} = \frac{f'(x)g(x) - f(x)g'(x)}{[g(x)]^2}.$$

Пусть $R(u_1, \dots, u_n)$ — рациональная функция, $R'_1, \dots, R'_n$ — её частные производные соответственно по $u_1, \dots, u_n$ и $\varphi_1, \dots, \varphi_n$ — рациональные функции от x .

Докажем формулу полной производной

$$(3) \quad \frac{d}{dx} R(\varphi_1, \dots, \varphi_n) = \sum_1^n R'_v(\varphi_1, \dots, \varphi_n) \frac{d\varphi_v}{dx}.$$

Для этой цели, в соответствии с определением производной, положим

$$\varphi_v(x+h) - \varphi_v(x) = h\psi_v(x, h), \quad \psi_v(x, 0) = \varphi'_v(x)$$

и

$$(4) \quad \left\{ \begin{aligned} R(u_1 + h_1, \dots, u_n + h_n) - R(u_1, \dots, u_n) &= \\ &= \sum_{v=1}^n [R(u_1 + h_1, \dots, u_v + h_v, u_{v+1}, \dots, u_n) - \\ &\quad - R(u_1 + h_1, \dots, u_v, u_{v+1}, \dots, u_n)] = \\ &= \sum_{v=1}^n h_v S_v(u_1 + h_1, \dots, u_v, h_v, u_{v+1}, \dots, u_n), \end{aligned} \right.$$

с

$$S_v(u_1, \dots, u_v, 0, u_{v+1}, \dots, u_n) = R'_v(u_1, \dots, u_n).$$

Полагая в тождестве (4)

$$u_v = \varphi_v(x), \quad h_v = \varphi_v(x+h) - \varphi_v(x) = h\psi_v(x, h)$$

и деля на h , получим:

$$\begin{aligned} \frac{R(\varphi_1(x+h), \dots, \varphi_n(x+h)) - R(\varphi_1(x), \dots, \varphi_n(x))}{h} &= \\ &= \sum_{v=1}^n \psi_v(x, h) S_v(\varphi_1 + h\psi_1, \dots, \varphi_v, h\psi_v, \varphi_{v+1}, \dots, \varphi_n). \end{aligned}$$

Положив справа $h=0$, получим

$$\frac{d}{dx} R(\varphi_1, \dots, \varphi_n) = \sum \varphi'_v(x) R'_v(\varphi_1, \dots, \varphi_n),$$

т. е. формулу (3).

Постараемся теперь распространить теорию дифференцирования на алгебраические функции одного переменного x . Под *алгебраической функцией неизвестной x* мы понимаем произвольный элемент η некоторого алгебраического расширения поля $P(x)$. При этом мы предполагаем лишь, что η сепарабелен относительно $P(x)$.

Итак, пусть алгебраическая функция η есть корень неприводимого над $P(x)$ сепарабельного полинома $F(x, y)$:

$$F(x, \eta) = 0.$$

Производные от $F(x, y)$ по x и y обозначим через F'_x и F'_y . Вследствие сепарабельности, $F'_y(x, y)$ не имеет общих корней с $F(x, y)$; следовательно,

$$F'_y(x, \eta) \neq 0.$$

От разумного определения производной $\frac{d\eta}{dx}$ естественно требовать, чтобы для полинома $F(x, y)$ выполнялась формула полной производной, т. е. чтобы

$$F'_x(x, \eta) + \frac{d\eta}{dx} F'_y(x, \eta) = 0.$$

Поэтому мы положим по определению

$$(5) \quad \frac{d\eta}{dx} = - \frac{F'_x(x, \eta)}{F'_y(x, \eta)}.$$

Непосредственно ясно, что это определение не зависит от выбора определяющего полинома $F(x, y)$, так как при замене $F(x, y)$ на $F(x, y) \cdot \psi(x)$, где $\psi(x)$ — произвольная рациональная функция от x , производные $F'_x(x, \eta)$ и $F'_y(x, \eta)$ в (5) заменятся на

$$F'_x(x, \eta) \cdot \psi(x) + F(x, \eta) \cdot \psi'(x) = F'_x(x, \eta) \cdot \psi(x)$$

и

$$F'_y(x, \eta) \cdot \psi(x),$$

так что частное (5) не изменится.

Если, в частности, η есть константа из P , $\eta = c$, то x вовсе не входит в определяющее уравнение для η , и следовательно $\frac{dc}{dx} = 0$.

Пусть теперь ζ — элемент поля $P(x, \eta)$, т. е. рациональная функция от x и η , притом целая рациональная относительно η :

$$\zeta = \varphi(x, \eta).$$

Докажем для этой функции φ формулу полной производной:

$$(6) \quad \frac{d\zeta}{dx} = \varphi'_x(x, \eta) + \varphi'_y(x, \eta) \frac{d\eta}{dx},$$

где φ'_x и φ'_y означают производные от $\varphi(x, y)$ по x и y . Для этой цели возьмём определяющее уравнение для ζ , которое можно считать целым рациональным относительно x и ζ :

$$G(x, \zeta) = 0,$$

подставим в него вместо ζ выражение $\varphi(x, \eta)$ и заменим затем η неизвестным y . Полученный в результате полином по y будет иметь корень η и поэтому будет делиться на $F(x, y)$:

$$G(x, \varphi(x, y)) = Q(x, y) F(x, y).$$

Дифференцируя это тождество по x и по y согласно формуле полной производной (3), получим:

$$\begin{cases} G'_x(x, \varphi(x, y)) + G'_\zeta(x, \varphi(x, y)) \varphi'_x(x, y) = QF'_x + Q'_x F(x, y), \\ G'_y(x, \varphi(x, y)) \varphi'_y(x, y) = QF'_y + Q_y F(x, y). \end{cases}$$

Заменяем теперь y снова на η , вследствие чего члены с $F(x, y)$ обратятся в нуль, и положим далее, в соответствии с определением (5),

$$F'_x(x, \eta) = -F'_y(x, \eta) \cdot \frac{d\eta}{dx},$$

$$G'_x(x, \zeta) = -G'_z(x, \zeta) \cdot \frac{d\zeta}{dx}.$$

Мы получим:

$$\begin{cases} -G'_z(x, \zeta) \cdot \frac{d\zeta}{dx} + G'_z(x, \zeta) \varphi'_x(x, \eta) = -Q(x, \eta) F'_y(x, \eta) \cdot \frac{d\eta}{dx}, \\ G'_z(x, \zeta) \varphi'_y(x, \eta) = Q(x, \eta) F'_y(x, \eta). \end{cases}$$

Умножая второе равенство на $\frac{d\eta}{dx}$, складывая с первым и деля результат на G'_z , придём к равенству

$$-\frac{d\zeta}{dx} + \varphi'_x(x, \eta) + \varphi'_y(x, \eta) \cdot \frac{d\eta}{dx} = 0,$$

т. е. к формуле (6).

Теперь, когда формула полной производной установлена проведённой выкладкой для частного случая (6), доказательство общей формулы полной производной не представит уже никакого труда. Формула такова: Если $\eta_1, \dots, \eta_n$ — сепарабельные алгебраические функции от x над некоторым полем и $R(u_1, \dots, u_n)$ — полином с производными R'_i , то

$$(7) \quad \frac{d}{dx} R(\eta_1, \dots, \eta_n) = \sum_1^n R'_i(\eta_1, \dots, \eta_n) \frac{d\eta_i}{dx}.$$

Доказательство. Пусть ϑ — примитивный элемент сепарабельного расширения $P(x, \eta_1, \dots, \eta_n)$ поля $P(x)$. Тогда все η_i рационально выражаются через x и ϑ :

$$\eta_i = \varphi_i(x, \vartheta).$$

Но в силу формулы (6), обозначая через φ'_{ix} и φ'_{it} производные от $\varphi_i(x, t)$ по x и t , имеем:

$$\frac{d\eta_i}{dx} = \varphi'_{ix}(x, \vartheta) + \varphi'_{it}(x, \vartheta) \cdot \frac{d\vartheta}{dx},$$

и точно так же, обозначая через R'_x и R'_t производные функции $R(\varphi_1(x, t), \dots, \varphi_n(x, t))$, имеем:

$$\begin{aligned} \frac{d}{dx} R(\eta_1, \dots, \eta_n) &= \frac{d}{dx} R(\varphi_1(x, \vartheta), \dots, \varphi_n(x, \vartheta)) = \\ &= R'_x(x, \vartheta) + R'_t(x, \vartheta) \cdot \frac{d\vartheta}{dx}. \end{aligned}$$

Но в силу формулы (3)

$$R'_x(x, t) = \sum_1^n R'_i(\varphi_1(x, t), \dots, \varphi_n(x, t)) \varphi'_{ix}(x, t),$$

$$R'_t(x, t) = \sum_1^n R'_i(\varphi_1(x, t), \dots, \varphi_n(x, t)) \varphi'_{it}(x, t).$$

Следовательно,

$$\begin{aligned} \frac{d}{dx} R(\eta_1, \dots, \eta_n) &= \sum_1^n R'_i(\varphi_1(x, \vartheta), \dots, \varphi_n(x, \vartheta)) \left\{ \varphi'_{ix}(x, \vartheta) + \right. \\ &\quad \left. + \varphi'_{it}(x, \vartheta) \cdot \frac{d\vartheta}{dt} \right\} = \sum_1^n R'_i(\eta_1, \dots, \eta_n) \frac{d\eta_i}{dx}. \end{aligned}$$

Важными частными случаями общей формулы (7) являются:

$$(8) \quad \frac{d}{dx} (\eta + \zeta) = \frac{d\eta}{dx} + \frac{d\zeta}{dx},$$

$$(9) \quad \frac{d}{dx} (\eta \zeta) = \eta \frac{d\zeta}{dx} + \frac{d\eta}{dx} \zeta,$$

$$(10) \quad \frac{d}{dx} \frac{\eta}{\zeta} = \frac{1}{\zeta^2} \left(\zeta \frac{d\eta}{dx} - \eta \frac{d\zeta}{dx} \right),$$

$$(11) \quad \frac{d}{dx} \eta^r = r \eta^{r-1} \frac{d\eta}{dx}.$$

Определение (5) производной применимо, разумеется, не только, когда x есть неизвестная, но и во всех тех случаях, когда x является элементом, трансцендентным относительно основного поля P , и η — сепарабельным алгебраическим над $P(x)$. В этих случаях мы предпочтём писать ξ вместо x . Таким образом, в поле степени трансцендентности 1 над P можно все элементы η , сепарабельные над $P(\xi)$, дифференцировать по трансцендентному элементу ξ .

Если η и ζ алгебраически зависят от ξ , то поле $P(\xi, \eta, \zeta)$ имеет степень трансцендентности 1 над P . Если теперь η трансцендентно относительно P , то ζ алгебраически зависит от η ; следовательно, можно образовать $\frac{d\zeta}{d\eta}$. Пусть

$$(12) \quad G(\eta, \zeta) = 0$$

— определяющее уравнение для ζ над $P(\eta)$ и G'_η , G'_ζ — частные производные от $G(y, z)$. Тогда

$$(13) \quad G'_\eta(\eta, \zeta) + G'_\zeta(\eta, \zeta) \frac{d\zeta}{d\eta} = 0.$$

С другой стороны, дифференцируя (12) по ξ , получим по формуле полной производной

$$(14) \quad G'_\eta(\eta, \zeta) \frac{d\eta}{d\xi} + G'_\zeta(\eta, \zeta) \frac{d\zeta}{d\xi} = 0,$$

Из (13) и (14) следует, если умножить (13) на $\frac{d\eta}{d\xi}$ и вычесть из результата (14), *формула производной сложной функции*:

$$(15) \quad \frac{d\zeta}{d\xi} = \frac{d\zeta}{d\eta} \cdot \frac{d\eta}{d\xi}.$$

• В частности, при $\zeta = \xi$ формула (15) даёт:

$$(16) \quad \frac{d\xi}{d\eta} \cdot \frac{d\eta}{d\xi} = 1.$$

Тем самым мы вывели все формулы обычного дифференциального исчисления для алгебраических функций от одной переменной чисто алгебраическим способом, не пользуясь при этом никакими предельными переходами.

ГЛАВА ДЕВЯТАЯ.

ВЕЩЕСТВЕННЫЕ ПОЛЯ.

При изучении алгебраических числовых полей, кроме алгебраических свойств входящих в них чисел, играют роль также некоторые неалгебраические свойства: *абсолютная величина* $|a|$, *вещественность*, *положительность*. Что эти свойства не могут быть однозначно определены с помощью алгебраических операций $+$ и $\cdot$, показывает следующий пример.

Пусть ω — вещественный и, значит, $i\omega$ — чисто мнимый корень уравнения $x^4 = 2$. При изоморфизме

$$\Gamma(\omega) \cong \Gamma(i\omega)$$

все алгебраические свойства сохраняются; однако при этом вещественное число ω переходит в чисто мнимое $i\omega$, положительное число $\omega^2 = \sqrt{2}$ — в отрицательное $(i\omega)^2 = -\sqrt{2}$, число же $1 + \sqrt{2}$, абсолютная величина которого > 1 , — в число $1 - \sqrt{2}$, абсолютная величина которого < 1 .

Однако в ходе дальнейшего исследования мы увидим, что этим неалгебраическим свойствам, тем не менее, присущи некие алгебраические черты, а именно, что в поле алгебраических чисел (т. е. в алгебраически замкнутом алгебраическом расширении поля Γ) можно выделить с помощью алгебраических свойств, правда, не одно подполе, алгебраически эквивалентное полю вещественных алгебраических чисел, но всё же, по крайней мере, семейство таких подполей. При каком-либо определённом выборе одного из этих подполей, элементы которого можно тогда назвать «вещественными», будут доступны алгебраическому определению также такие понятия, как абсолютная величина и положительность. Для каждого конечного алгебраического числового поля определения абсолютной величины, вещественности и т. п. будут тогда конечно-многозначными.

Однако, прежде, чем перейти к этой алгебраической теории, напомним сперва обычное в анализе (трансцендентное) введение вещественных и комплексных чисел — не из-за того, чтобы в этом была логическая необходимость, но потому, что постановка задачи чисто алгебраической теории станет яснее, если уже известно, что вообще

представляют собой вещественные и комплексные числа, а также потому, что это даст нам возможность одновременно познакомиться с принципиально важными понятиями расположения и фундаментальной последовательности.

§ 66. Расположенные поля.

В настоящем параграфе мы аксиоматически исследуем первое неалгебраическое свойство: «положительность» и основывающееся на нём понятие «расположения».

Поле K называется «расположенным», если для его элементов определено свойство быть положительными (>0), удовлетворяющее следующим требованиям:

1) *Для каждого элемента a из K имеет место одно и только одно из соотношений*

$$a=0, \quad a>0, \quad -a>0.$$

2) *Если $a>0$ и $b>0$, то $a+b>0$ и $ab>0$.*

Если $-a>0$, то мы будем говорить, что a отрицательно.

Если мы определим сравнение любых элементов расположенного поля по величине, условившись считать, что

$$\begin{aligned} &a>b, \text{ словами: } a \text{ больше чем } b \\ &(\text{или } b<a, \text{ словами: } b \text{ меньше чем } a), \\ &\text{если } a-b>0, \end{aligned}$$

то без труда обнаружим, что будут выполнены обычные аксиомы порядка. А именно, для каждого двух элементов a, b либо $a<b$, либо $a=b$, либо $a>b$. Из $a>b$ и $b>c$ вытекает $a-b>0$ и $b-c>0$, следовательно, также $a-c=(a-b)+(b-c)>0$, и тем самым $a>c$. Далее, как и в § 3 имеем правило, что из $a>b$ следует $a+c>b+c$ и в случае $c>0$ — также $ac>bc$. Наконец, если a и b положительны, то из $a>b$ всегда следует $a^{-1}<b^{-1}$ (и обратно), так как

$$ab(b^{-1}-a^{-1})=a-b.$$

Будем под *абсолютной величиной* $|a|$ элемента a расположенного поля понимать неотрицательный из элементов a и $-a$. Тогда будут выполняться следующие правила:

$$\begin{aligned} |ab| &= |a| \cdot |b|, \\ |a+b| &\leq |a| + |b|. \end{aligned}$$

Первое правило без труда проверяется для каждого из четырёх возможных случаев

$$\begin{aligned} a \geq 0, \quad b \geq 0; \\ a \geq 0, \quad b < 0; \\ a < 0, \quad b \geq 0; \\ a < 0, \quad b < 0. \end{aligned}$$

Второе правило, очевидно, выполняется со знаком равенства в случае $a \geq 0, b \geq 0$, так как тогда обе части равны неотрицательному элементу $a + b$, и точно так же в случае $a < 0, b < 0$, где обе части равны неотрицательному элементу $-(a + b)$. Из перечисленных четырёх случаев остаются ещё два средних; достаточно рассмотреть один из них, например, случай $a \geq 0, b < 0$. В этом случае

$$\begin{aligned} a + b &< a < a - b = |a| + |b|, \\ -a - b &\leq -b \leq a - b = |a| + |b| \end{aligned}$$

и, следовательно,

$$|a + b| \leq |a| + |b|.$$

Имеем также

$$a^2 = (-a)^2 = |a|^2 \geq 0,$$

со знаком равенства лишь для $a = 0$. Отсюда, далее, следует, что сумма квадратов всегда ≥ 0 , причём $= 0$ лишь тогда, когда каждое слагаемое в отдельности равно нулю.

В частности, единица $1 = 1^2$ всегда положительна, равно как и каждая сумма $n \cdot 1 = 1 + 1 + \dots + 1$. Поэтому ни для какого простого числа p не может выполняться равенство $p \cdot 1 = 0$. Таким образом: *характеристика расположенного поля равна нулю.*

Лемма. Если K — поле отношений расположенного кольца $\mathfrak{R}$, то K может быть расположено, и притом единственным образом, так, чтобы сохранилось расположение кольца $\mathfrak{R}$.

Действительно, пусть K уже расположено требуемым образом.

Произвольный элемент поля K имеет вид $a = \frac{b}{c}$, где b и c принадлежат $\mathfrak{R}$ и $c \neq 0$. Из

$$\frac{b}{c} > 0, \text{ соотв. } = 0, \text{ соотв. } < 0$$

умножением на c^2 непосредственно получаем:

$$bc > 0, \text{ соотв. } = 0, \text{ соотв. } < 0.$$

Следовательно, предполагаемое расположение поля K однозначно определяется расположением кольца $\mathfrak{R}$. И обратно, легко убедиться в том, что, полагая

$$\frac{b}{c} > 0, \text{ если } bc > 0,$$

мы действительно определим расположение поля K , не нарушающее расположения кольца $\mathfrak{R}$.

Таким образом, в частности, поле Γ рациональных чисел может быть расположено единственным образом, поскольку кольцо S целых чисел, очевидно, допускает лишь естественное расположение.

Следовательно, $\frac{m}{n} > 0$, коль скоро $m \cdot n$ есть натуральное число.

Два расположенных поля называются *подобно-изоморфными*, если существует изоморфизм обоих полей, при котором положительным элементам соответствуют всегда положительные же элементы.

Поле называется *архимедовски расположенным*¹⁾, если при заданном его расположении для каждого элемента поля a существует «натуральное число» $n > a$. Тогда для каждого a существует также число $-n < a$ и для каждого положительного a — дробь $\frac{1}{n} < a$. Так, например, поле рациональных чисел Γ архимедовски расположено. В неархимедовски расположенном поле существуют «бесконечно большие» элементы, большие всякого рационального числа, и «бесконечно малые» элементы, меньшие всякого положительного рационального числа и, однако, большие чем нуль.

Литература о неархимедовски расположенных полях.

Artin E. u. Schreier O., *Algebraische Konstruktion reeller Körper* *Abh. Math. Sem. Hamburg*, 5 (1926), 85—99.

Baer R., *Über nichtarchimedisch geordnete Körper*, *Sitzungsber. Heidelb. Ak.* 8. Abhandlung, 1927.

Задача 1. Назовём полином $f(t)$ с рациональными коэффициентами положительным, если положителен коэффициент при наивысшей входящей в него степени переменной t . Показать, что этим определяется расположение кольца полиномов $\Gamma[t]$ и потому также его поля отношений $\Gamma(t)$, и что последнее расположение — неархимедовское (t «бесконечно велико»).

Задача 2. Пусть

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n,$$

где a_i принадлежат некоторому расположенному полю K . Пусть M — больший из элементов 1 и $|a_1| + \dots + |a_n|$. Показать, что

$$\begin{aligned} f(s) &> 0 \text{ при } s > M, \\ (-1)^n f(s) &> 0 \text{ при } s < -M. \end{aligned}$$

Если, таким образом, $f(x)$ имеет корни в K , то они заключены в области $-M \leq s \leq M$.

Задача 3. Пусть, при обозначениях задачи 2, $R > 0$ и $-S$ — сумма отрицательных среди величин $a_1, \frac{a_2}{R}, \frac{a_3}{R^2}, \dots, \frac{a_n}{R^{n-1}}$; пусть M_R — большее из чисел R и S . Тогда для $s > M_R$ всегда $f(s) > 0$.

¹⁾ По аналогии с «аксиомой Архимеда» в геометрии, гласящей, что каждый заданный отрезок PQ («единичный отрезок») всегда можно отложить от заданной точки P («нулевой точки») в направлении PR столько раз, чтобы перешагнуть через любую заданную точку R .

(Полагая здесь $R=1$, получаем уточнение верхней границы M задачи 2.)

Задача 4. Пусть снова $f(x) = x^n + a_1x^{n-1} + \dots + a_n$ и все $a_i \geq -c$, $c \geq 0$. Показать, что $f(s) > 0$ для $s \geq 1 + c$. [Использовать неравенство $s^m \geq c(s^{m-1} + s^{m-2} + \dots + 1)$.] Заменой x на $-x$ определим таким же образом границу $-1 - c'$, такую, что $(-1)^n f(s) > 0$ для $s < -1 - c'$. Если, кроме старшего коэффициента 1, положительны ещё первые r коэффициентов $a_1, \dots, a_r$, то границу $1 + c$ можно заменить на $1 + \frac{c}{1 + a_1 + \dots + a_r}$.

Задача 5. При $a > b > 0$ имеем $a^n > b^n > 0$ (n — натуральное число). Полином $x^n - c$ в каждом расположенном поле K обладает самым большим одним положительным корнем $\sqrt[n]{c}$. Для нечётного n вообще имеется самое большое один корень; для чётного n — самое большое два, которые тогда отличаются друг от друга лишь знаком. Если $\sqrt[n]{c}$ и $\sqrt[n]{d}$ существуют и $0 < c < d$, то $\sqrt[n]{c} < \sqrt[n]{d}$.

§ 67. Определение вещественных чисел.

Пусть K — расположенное поле и $\mathfrak{M}$ — непустое множество элементов из K . Если все элементы множества $\mathfrak{M}$ не больше фиксированной величины s из K , то s называется *верхней границей* множества $\mathfrak{M}$, а $\mathfrak{M}$ — *ограниченным сверху*. Если существует наименьшая верхняя граница, то она называется *верхней гранью* множества $\mathfrak{M}$.

Если все элементы множества $\mathfrak{M}$ не меньше фиксированной величины s' из K , то s' называется *нижней границей* множества $\mathfrak{M}$, а $\mathfrak{M}$ — *ограниченным снизу*.

В поле рациональных чисел Γ не всякое ограниченное сверху множество $\mathfrak{M}$ обладает верхней гранью. Пример: множество $\mathfrak{M}$ положительных чисел, квадрат которых меньше чем 3. Действительно, верхней границей для $\mathfrak{M}$ является каждое положительное число, квадрат которого больше чем 3. Числа же, квадрат которого был бы равен 3, в Γ не существует, так как полином $x^2 - 3$ неприводим в Γ . Если r — положительное рациональное число, такое, что $r^2 > 3$, то

$$r' = \frac{r + 3r^{-1}}{2}$$

есть меньшее положительное число, квадрат которого всё ещё > 3 ; в самом деле,

$$r' = \frac{r + 3r^{-1}}{2} > \frac{r}{2} > 0,$$

$$r' = \frac{r + 3r^{-1}}{2} < \frac{r + r^2r^{-1}}{2} = r,$$

$$r'^2 = \left(\frac{r + 3r^{-1}}{2}\right)^2 = \left(\frac{r - 3r^{-1}}{2}\right)^2 + 3 \geq 3, \text{ следовательно, } > 3.$$

Таким образом, в Γ для каждой верхней границы r существует меньшая верхняя граница r' , и тем самым верхней грани не существует.

Нашей целью будет теперь найти для каждого расположенного поля K такое расположенное расширение Ω , в котором любое непустое ограниченное сверху множество обладало бы верхней гранью. В частности, если K — поле рациональных чисел, то Ω будет хорошо известным полем «вещественных чисел». Из различных построений поля Ω , известных из основ анализа, мы приведём здесь канторово построение с помощью «фундаментальных последовательностей».

Бесконечная последовательность элементов $a_1, a_2, \dots$ расположенного поля K называется *фундаментальной последовательностью* $\{a_n\}$, если для каждой положительной величины ε из K существует натуральное число $n = n(\varepsilon)$ такое, что

$$(1) \quad |a_p - a_q| < \varepsilon \text{ для } p > n, q > n.$$

Из (1), беря $q = n + 1$, получаем:

$$|a_p| \leq |a_n| + |a_p - a_n| < |a_{n+1}| + \varepsilon = M \text{ для } p > n.$$

Таким образом, каждая фундаментальная последовательность ограничена сверху и снизу.

Суммы и произведения фундаментальных последовательностей определяются равенствами

$$c_n = a_n + b_n, \quad d_n = a_n b_n.$$

В том, что они снова являются фундаментальными последовательностями, убеждаемся следующим образом. Для каждого ε существует n_1 такое, что

$$|a_p - a_q| < \frac{1}{2} \varepsilon \text{ для } p > n_1, q > n_1,$$

и n_2 такое, что

$$|b_p - b_q| < \frac{1}{2} \varepsilon \text{ для } p > n_2, q > n_2.$$

Обозначая через n большее из чисел n_1 и n_2 , получаем

$$|(a_p + b_p) - (a_q + b_q)| < \varepsilon \text{ для } p > n, q > n.$$

Равным образом существуют M_1 и M_2 такие, что

$$\begin{aligned} |a_p| &< M_1 \text{ для } p > n_1, \\ |b_p| &< M_2 \text{ для } p > n_2, \end{aligned}$$

и далее для каждого ε существуют $n' > n_2$ и $n'' > n_1$ такие, что

$$|a_p - a_q| < \frac{\varepsilon}{2M_2} \text{ для } p > n', q > n',$$

$$|b_p - b_q| < \frac{\varepsilon}{2M_1} \text{ для } p > n'', q > n''.$$

Отсюда, умножая на $|b_p|$, соответственно на $|a_q|$, получаем:

$$|a_p b_p - a_q b_p| < \frac{\varepsilon}{2} \text{ для } p > n', \quad q > n',$$

$$|a_q b_p - a_q b_q| < \frac{\varepsilon}{2} \text{ для } p > n'', \quad q > n'',$$

и, следовательно, обозначая через n большее из чисел n' и n'' :

$$|a_p b_p - a_q b_q| < \varepsilon \text{ для } p > n, \quad q > n.$$

Сложение и умножение фундаментальных последовательностей, очевидно, удовлетворяют всем постулатам кольца; таким образом, *фундаментальные последовательности образуют кольцо $\mathfrak{o}$* .

Фундаментальная последовательность $\{a_p\}$, «сходящаяся к 0», т. е. обладающая тем свойством, что для каждого ε существует n такое, что

$$|a_p| < \varepsilon \text{ для } p > n,$$

называется *нулевой последовательностью*. Покажем теперь, что:

Нулевые последовательности образуют идеал $\mathfrak{n}$ в кольце $\mathfrak{o}$.

Доказательство. Если $\{a_p\}$ и $\{b_p\}$ — нулевые последовательности, то для каждого ε существуют n_1 и n_2 такие, что

$$|a_p| < \frac{1}{2} \varepsilon \text{ для } p > n_1,$$

$$|b_p| < \frac{1}{2} \varepsilon \text{ для } p > n_2,$$

так что, обозначая снова через n большее из чисел n_1, n_2 , имеем

$$|a_p - b_p| < \varepsilon \text{ для } p > n;$$

тем самым также $\{a_p - b_p\}$ является нулевой последовательностью. Далее, если $\{a_p\}$ — нулевая последовательность и $\{c_p\}$ — произвольная фундаментальная последовательность, то определим n' и M так, чтобы

$$|c_p| < M \text{ для } p > n',$$

и для каждого ε определим $n = n(\varepsilon) \geq n'$ так, чтобы

$$|a_p| < \frac{\varepsilon}{M} \text{ для } p > n.$$

Тогда будем иметь

$$|a_p c_p| < \varepsilon \text{ для } p > n,$$

и тем самым $\{a_p c_p\}$ также является нулевой последовательностью.

Обозначим факторкольцо $\mathfrak{o}/\mathfrak{n}$ через $\mathfrak{Q}$. Покажем, что $\mathfrak{Q}$ есть поле, т. е. что сравнение

$$(2) \quad ax \equiv 1 (n)$$

обладает решением в $\mathfrak{o}$ для каждого $a \not\equiv 0 (n)$; при этом 1 означает единицу кольца $\mathfrak{o}$, т. е. фундаментальную последовательность $\{1, 1, \dots\}$.

Так как $a = \{a_p\} (n)$, то $0 \neq$ должны существовать такие n и $\eta > 0$, что

$$|a_q| \geq \eta \text{ для } q > n.$$

Действительно, если бы для всякого n и всякого $\eta > 0$ существовало $q_0 > n$ такое, что

$$|a_{q_0}| < \eta,$$

то, выбирая, при заданном η , n столь большим, чтобы для всех $p > n$, $q > n$ было

$$|a_p - a_q| < \eta,$$

мы получили бы, что

$$|a_p| \leq |a_p - a_{q_0}| + |a_{q_0}| < 2\eta$$

для всех $p > n$, т. е. $\{a_q\}$ была бы нулевой последовательностью, вопреки предположению.

Фундаментальная последовательность $\{a_p\}$ при замене $a_1, \dots, a_n$ на η останется в том же классе вычетов по модулю n . Обозначая эти n новых элементов η снова через $a_1, \dots, a_n$, будем иметь для всех p :

$$|a_p| \geq \eta, \text{ в частности } a_p \neq 0.$$

Покажем теперь, что $\{a_p^{-1}\}$ есть фундаментальная последовательность. Действительно, для каждого ε существует n такое, что

$$|a_q - a_p| < \varepsilon \eta^2 \text{ для } p > n, q > n.$$

Если бы теперь для некоторого $p > n$ и некоторого $q > n$ имело место неравенство $|a_p^{-1} - a_q^{-1}| \geq \varepsilon$, то умножением на $|a_p| \geq \eta$ и $|a_q| \geq \eta$ мы получили бы:

$$|a_q - a_p| = |a_p a_q (a_p^{-1} - a_q^{-1})| \geq \varepsilon \eta^2,$$

что невозможно. Следовательно,

$$|a_p^{-1} - a_q^{-1}| < \varepsilon \text{ для } p > n, q > n.$$

Фундаментальная последовательность $\{a_p^{-1}\}$, очевидно, и является решением сравнения (2).

Поле Ω содержит, в частности, те классы вычетов по модулю n , которые представляются фундаментальными последовательностями вида

$$\{a, a, a, \dots\}.$$

Эти классы образуют подполе K' поля Ω , изоморфное полю K . Действительно, каждому a из K соответствует такой класс вычетов, различным a соответствуют различные классы вычетов, сумме соответствует сумма и произведению — произведение. Если мы отождествим теперь элементы из K' с соответственными элементами из K , то Ω будет расширением поля K .

Фундаментальная последовательность $\{a_p\}$ называется *положительной*, если существуют такие $\varepsilon > 0$ в K и n , что

$$a_p > \varepsilon \text{ для } p > n.$$

Сумма и произведение двух положительных фундаментальных последовательностей, очевидно, снова положительны. Точно так же сумма положительной последовательности $\{a_p\}$ и нулевой последовательности $\{b_p\}$ всегда положительна; в этом убеждаемся, выбирая n столь большим, чтобы

$$a_p > \varepsilon \text{ для } p > n, \\ |b_p| < \frac{1}{2} \varepsilon \text{ для } p > n,$$

откуда следует, что

$$a_p + b_p > \frac{1}{2} \varepsilon \text{ для } p > n.$$

Тем самым все последовательности из класса вычетов по модулю n положительны, коль скоро положительна хотя бы одна из них. В этом случае класс вычетов называется *положительным*. Класс вычетов k называется *отрицательным*, если $-k$ положителен.

Если ни $\{a_p\}$, ни $\{-a_p\}$ не положительны, то для каждого $\varepsilon > 0$ и каждого n существуют $r > n$ и $s > n$ такие, что

$$a_r \leq \varepsilon \text{ и } -a_s \leq \varepsilon.$$

Выбирая теперь n столь большим, чтобы для $p > n$, $q > n$ было

$$|a_p - a_q| < \varepsilon,$$

заключаем, беря $q = r$ и p произвольное $> n$, что

$$a_p = (a_p - a_q) + a_r < \varepsilon + \varepsilon = 2\varepsilon,$$

а беря $q = s$ и p произвольное $> n$, — что

$$-a_p = (a_q - a_p) - a_s < \varepsilon + \varepsilon = 2\varepsilon;$$

тем самым

$$|a_p| < 2\varepsilon \text{ для } p > n.$$

Поэтому $\{a_p\}$ является нулевой последовательностью.

Таким образом, всегда либо $\{a_p\}$ положительна, либо $\{-a_p\}$ положительна, либо $\{a_p\}$ — нулевая последовательность. Поэтому каждый класс вычетов по модулю n либо положителен, либо отрицателен, либо нулевой. Так как сумма и произведение положительных классов снова положительны, то заключаем:

Ω есть расположенное поле.

Непосредственно ясно, что расположение поля K сохраняется в Ω .

Если последовательность $\{a_p\}$ определяет элемент α , а последовательность $\{b_p\}$ — элемент β поля Ω , то из

$$a_p \geq b_p \text{ для } p > n$$

всегда следует $\alpha \geq \beta$. Действительно, если бы было $\alpha < \beta$ или $\beta - \alpha > 0$, то для фундаментальной последовательности $\{b_p - a_p\}$ существовали бы ε и m такие, что

$$b_p - a_p > \varepsilon > 0 \text{ для } p > m.$$

Взяв здесь $p = m + n$, мы пришли бы к противоречию с предположением $a_p \geq b_p$. Полезно заметить, что из $a_p > b_p$ следует не $\alpha > \beta$, а лишь $\alpha \geq \beta$.

Из ограниченности сверху каждой фундаментальной последовательности следует, что для каждого элемента ω поля Ω существует больший элемент s из K . Если K архимедовски расположено, то для s , в свою очередь, найдётся большее натуральное число n ; тем самым для каждого ω существует $n > \omega$, т. е. и Ω архимедовски расположено.

Внутри поля Ω вновь естественно определяются понятия абсолютной величины, фундаментальной последовательности и нулевой последовательности. Нулевые последовательности снова образуют идеал. Если последовательность $\{a_p\}$ сравнима по этому идеалу с последовательностью $\{\alpha\}$, составленной из одинаковых элементов α , т. е. если $\{a_p - \alpha\}$ есть нулевая последовательность, то говорят, что последовательность $\{a_p\}$ сходится к пределу α , и пишут:

$$\lim_{p \rightarrow \infty} a_p = \alpha \text{ или, короче, } \lim a_p = \alpha.$$

Фундаментальные последовательности $\{a_p\}$ из K , служившие для определения элементов поля Ω , очевидно, можно рассматривать также как фундаментальные последовательности в Ω , поскольку K содержится в Ω . Покажем теперь, что если последовательность $\{a_p\}$ определяет элемент α из Ω , то $\lim a_p = \alpha$. Для доказательства заметим, что для каждого положительного ε из Ω существует меньшее положительное ε' из K , а для последнего — такое n , что для $p > n$, $q > n$ всегда

$$|a_p - a_q| < \varepsilon',$$

т. е. обе разности $a_p - a_q$ и $a_q - a_p$ меньше чем ε' . Отсюда, согласно сделанному выше замечанию, следует, что $a_p - \alpha$ и $\alpha - a_p$ обе $\leq \varepsilon'$; т. е.

$$|a_p - \alpha| \leq \varepsilon' < \varepsilon.$$

Тем самым $\{a_p - \alpha\}$ есть нулевая последовательность.

Покажем теперь, что поле Ω нельзя уже далее расширить, используя фундаментальные последовательности, — напротив, каждая фундаментальная последовательность $\{a_p\}$ из Ω имеет предел уже в Ω (теорема сходимости Коши).

При доказательстве мы можем предполагать, что в последовательности $\{\alpha_p\}$ каждые два соседних элемента α_p, α_{p+1} отличны друг от друга. Действительно, если это не так, то либо можно выбрать подпоследовательность, состоящую из тех α_p , которые отличны от предшествующих им α_{p-1} , причём, разумеется, из сходимости этой подпоследовательности будет сразу следовать и сходимость заданной последовательности; либо последовательность α_p , начиная с некоторого места, остаётся постоянной: $\alpha_p = \alpha$ для $p > n$; но в этом случае, очевидно, $\lim \alpha_p = \alpha$.

Положим теперь

$$|\alpha_p - \alpha_{p+1}| = \varepsilon_p.$$

Так как $\{\alpha_p\}$ было фундаментальной последовательностью, то $\{\varepsilon_p\}$ — нулевая последовательность¹⁾. По предположению $\varepsilon_p > 0$.

Выберем теперь для каждого α_p аппроксимирующее α_p , удовлетворяющее условию

$$|\alpha_p - \alpha_p| < \varepsilon_p.$$

Это возможно, так как α_p само было определено фундаментальной последовательностью $\{\alpha_{p1}, \alpha_{p2}, \dots\}$, имеющей пределом α_p . Далее, для каждого ε существует такое n' , что

$$|\alpha_p - \alpha_q| < \frac{1}{3} \varepsilon \text{ для } p > n', q > n'$$

и n'' такое, что

$$\varepsilon_p < \frac{1}{3} \varepsilon \text{ для } p > n''.$$

Если теперь n — большее из двух чисел n' и n'' , то для $p > n, q > n$ все три абсолютные величины $|\alpha_p - \alpha_p|$, $|\alpha_p - \alpha_q|$ и $|\alpha_q - \alpha_q|$ будут меньше чем $\frac{1}{3} \varepsilon$, и потому

$$\begin{aligned} |\alpha_p - \alpha_q| &\leq |\alpha_p - \alpha_p| + |\alpha_p - \alpha_q| + |\alpha_q - \alpha_q| < \\ < \frac{1}{3} \varepsilon + \frac{1}{3} \varepsilon + \frac{1}{3} \varepsilon = \varepsilon. \end{aligned}$$

Тем самым элементы α_p образуют фундаментальную последовательность в K . Пусть ω — определяемый ею элемент поля Ω . Последовательность $\{\alpha_p\}$ отличается от этой фундаментальной последовательности лишь нулевой последовательностью $\{\alpha_p - \alpha_p\}$ и потому имеет тот же предел ω .

¹⁾ Предшествующая часть доказательства имела единственной целью установить существование нулевой последовательности, используемой в дальнейшем ходе доказательства. В архимедовском случае проще было бы взять $\varepsilon_p = 2^{-p}$, но мы доказываем теорему во всей общности. В неархимедовском случае $\{2^{-p}\}$ не является нулевой последовательностью.

Докажем теперь для того случая, когда K , а следовательно, и Ω архимедовски расположены, теорему о верхней грани:

Каждое непустое ограниченное сверху множество $M \subset \Omega$ обладает в Ω верхней гранью.

Доказательство. Пусть s — какая-нибудь верхняя граница для M , M — целое число $> s$ (значит — также верхняя граница), μ — произвольный элемент из M и m — целое число $> -\mu$. Тогда

$$-m < \mu < M.$$

Образуем теперь дроби $k \cdot 2^{-p}$ (k — целое, p — натуральное число), лежащие «между» $-m$ и M :

$$-m \leq k \cdot 2^{-p} \leq M;$$

для каждого p таких дробей будет конечное число. Возьмём среди этих дробей наименьшую, являющуюся ещё верхней границей для M . По крайней мере одна такая дробь существует, поскольку во всяком случае само M является верхней границей для M .

Эту наименьшую верхнюю границу обозначим через a_p . Тогда $a_p - 2^{-p}$ уже не будет верхней границей; тем самым для каждого $q > p$ будем иметь

$$(4) \quad a_p - 2^{-p} < a_q \leq a_p.$$

Отсюда следует, что

$$|a_p - a_q| < 2^{-p}$$

и, значит,

$$(5) \quad |a_p - a_q| < 2^{-n} \quad \text{для } p > n, q > n.$$

Но при заданном ε всегда можно найти натуральное число $n > \varepsilon^{-1}$ и далее $2^n > h > \varepsilon^{-1}$. Тогда $2^{-n} < \varepsilon$. Таким образом, (5) означает, что $\{a_p\}$ является фундаментальной последовательностью, определяя тем самым некоторый элемент ω поля Ω . Из неравенств (4) следует далее, что

$$a_p - 2^{-p} \leq \omega \leq a_p.$$

ω есть верхняя граница для M , т. е. $\mu \leq \omega$ для всякого элемента μ множества M . Действительно, если бы для некоторого μ из M выполнялось неравенство $\mu > \omega$, то можно было бы найти число $2^p > (\mu - \omega)^{-1}$, откуда $2^{-p} < \mu - \omega$. Складывая это с $a_p - 2^{-p} \leq \omega$, мы получили бы, что $a_p < \mu$, чего, однако, быть не может, так как a_p есть верхняя граница для M .

ω — наименьшая верхняя граница для M . Действительно, если бы существовала верхняя граница σ , меньшая чем ω , то снова можно было бы найти число p такое, что $2^{-p} < \omega - \sigma$. С другой стороны, так как $a_p - 2^{-p}$ не является верхней границей для M , то в M существует μ такое, что $a_p - 2^{-p} < \mu$. Отсюда следует, что

$$a_p - 2^{-p} < \sigma!$$

и, складывая это с предшествующим неравенством $2^{-p} < \omega - \alpha$, мы получили бы

$$a_p < \omega,$$

что невозможно.

Таким образом, ω есть верхняя грань множества $\mathfrak{M}$.

Итак, изложенное построение даёт для каждого расположенного поля K однозначно определённое расположенное расширение Ω , в котором, в случае архимедовского K , имеет место теорема о верхней грани. В частности, если K — поле рациональных чисел, то Ω есть поле *вещественных чисел*. Таким образом, в этой теории вещественное число определяется как класс вычетов по модулю π в кольце фундаментальных последовательностей рациональных чисел.

Задача 1. Доказать следующие свойства понятия предела:

а) Если $\{\alpha_n\}$ и $\{\beta_n\}$ — сходящиеся последовательности, то

$$\lim (\alpha_n \pm \beta_n) = \lim \alpha_n \pm \lim \beta_n,$$

$$\lim (\alpha_n \beta_n) = \lim \alpha_n \cdot \lim \beta_n.$$

б) Если $\lim \beta_n \neq 0$ и все $\beta_n \neq 0$, то

$$\lim (\beta_n^{-1}) = (\lim \beta_n)^{-1}.$$

в) Подпоследовательность сходящейся последовательности сходится к тому же пределу.

Задача 2. Единственным (с точностью до эквивалентности) архимедовски расположенным расширением архимедовски расположенного поля K , таким, в котором имеет место теорема Коши о сходимости, является расширение, построенное указанным выше образом с помощью фундаментальных последовательностей.

Задача 3. Каждое архимедовски расположенное поле подобно изоморфно некоторому подполю поля вещественных чисел.

Задача 4. Каждое вещественное число s представимо в виде бесконечной десятичной дроби

$$s = a_0 + \sum_{v=1}^{\infty} a_v \cdot 10^{-v} \quad \left(\text{т. е. } s = \lim_{n \rightarrow \infty} \left(a_0 + \sum_{v=1}^n a_v \cdot 10^{-v} \right) \right) \quad (0 \leq a_v < 10).$$

§ 68. Корни вещественных функций.

Пусть P — поле вещественных чисел. Рассмотрим теперь вещественные функции $f(x)$ вещественного переменного x . Такая функция называется *непрерывной* при $x = a$, если для каждого $\varepsilon > 0$ существует $\delta > 0$ такое, что

$$|f(a+h) - f(a)| < \varepsilon \quad \text{для } |h| < \delta.$$

Легко доказывается, что суммы и произведения непрерывных функций снова суть непрерывные функции (см. аналогичное доказательство для фундаментальных последовательностей в § 67). Так как

константы и функция $f(x) = x$ суть всюду непрерывные функции, то все полиномы от x являются всюду непрерывными функциями от x .

Теорема Вейерштрасса о корнях непрерывной функции гласит:

Функция $f(x)$, непрерывная для $a \leq x \leq b$ и такая, что $f(a) < 0$ и $f(b) > 0$, обладает корнем между a и b .

Доказательство. Пусть c — верхняя грань множества $\mathcal{M}$ всех тех x , заключённых между a и b , для которых $f(x) < 0$. Представляются три возможности:

1. $f(c) > 0$. Тогда прежде всего $c > a$, и существует $\delta > 0$ такое, что для $0 < h < \delta$

$$|f(c-h) - f(c)| < f(c),$$

$$f(c) - f(c-h) < f(c),$$

т. е.

$$f(c-h) > 0$$

$$f(x) > 0 \quad \text{для } c - \delta < x \leq c.$$

Следовательно, $c - \delta$ является верхней границей для множества $\mathcal{M}$. Но c было наименьшей верхней границей. Следовательно, рассмотренный случай невозможен.

2. $f(c) < 0$. Тогда $c < b$ и существует $\delta > 0$ такое, что для $0 < h < \delta$, например, для $h = \frac{1}{2}\delta$,

$$f(c+h) - f(c) < -f(c),$$

$$f(c+h) < 0.$$

Поэтому c не является верхней границей множества $\mathcal{M}$. Таким образом, и этот случай невозможен.

3. $f(c) = 0$ есть единственный оставшийся ещё случай. Следовательно, $f(x)$ имеет корнем c .

Эта теорема в применении к полиномам лежит в основе всех теорем о вещественных корнях алгебраических уравнений. Ниже мы распространим её на другие поля, отличные от поля вещественных чисел, а именно, на так называемые «вещественно замкнутые поля». Все дальнейшие теоремы настоящего параграфа основываются исключительно на теореме Вейерштрасса о корнях для полиномов и в соответствии с этим справедливы также для указанных более общих полей.

Следствие 1. *Полином $x^n - d$ при $d > 0$ и любом натуральном n всегда обладает корнем, притом даже положительным.*

Действительно, для $x = 0$ имеем $x^n - d < 0$, а для больших x (например, для $x > 1 + \frac{d}{n}$) имеем $x^n - d > 0$.

Из тождества $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ следует далее, что при $a > b > 0$ также $a^n > b^n$; тем самым уравнение $x^n = d$ может обладать лишь одним положительным корнем. Он

обозначается через $\sqrt[n]{d}$, а при $n=2$ — кратко через $\sqrt{d}$ («квадратный корень»). Далее, полагают $\sqrt[n]{0}=0$. Из $a > b \geq 0$ следует теперь $\sqrt[n]{a} > \sqrt[n]{b}$, так как из $\sqrt[n]{a} \leq \sqrt[n]{b}$ следовало бы $a \leq b$.

Следствие 2. Каждый полином нечётной степени обладает в $\mathbb{R}$ корнем.

Действительно, по задаче 2 § 66 существует такое M , что $f(M) > 0$ и $f(-M) < 0$.

Обратимся теперь к вопросу о *вычислении вещественных корней полинома $f(x)$* . Под этим, согласно определению вещественных чисел, следует понимать произвольно точное приближение корней рациональными числами.

Мы уже видели в § 66 (задача 2), как указать границы, в которых заключены вещественные корни полинома $f(x)$: если

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n$$

и M — большее из чисел 1 и $|a_1| + \dots + |a_n|$, то все эти корни лежат между $-M$ и $+M$. [$f(x)$ имеет положительные значения для $x > M$ и значения со знаком $(-1)^n$ для $x < -M$.] Мы можем заметить M (возможно и большим) рациональным числом, обозначить последнее снова через M и разбить затем интервал $-M \leq x \leq M$ рациональными промежуточными точками на произвольно малые части. В каких из этих частей лежат корни, мы сможем установить, коль скоро будем обладать средством определять, сколько корней заключено между двумя заданными границами. Тогда дальнейшим разбиением интервалов, заключающих вещественные корни, мы сможем произвольно точно аппроксимировать эти корни.

Средство для определения количества корней, лежащих между двумя заданными границами, равно как и общего количества корней, доставляет

Теорема Штурма. Определим полиномы $X_1, X_2, \dots, X_r$, исходя из заданного полинома $X = f(x)$, следующим образом:

$$(1) \quad \left\{ \begin{array}{l} X_1 = f'(x) \\ X = Q_1 X_1 - X_2, \\ X_1 = Q_2 X_2 - X_3, \\ \dots \dots \dots \\ X_{r-1} = Q_r X_r \end{array} \right. \quad \begin{array}{l} \text{(дифференцирование),} \\ \\ \text{(алгоритм Эвклида).} \end{array}$$

Пусть для каждого вещественного числа a , не являющегося корнем полинома $f(x)$, $w(a)$ обозначает число перемен знака¹⁾ в чис-

¹⁾ Под знаком числа s мы понимаем символ $+$, $-$ или 0 , смотря по тому, является ли s положительным, отрицательным или равным нулю. Переменной в последовательности знаков $+$ и $-$ считается каждый случай, когда за $+$ следует $-$ или за $-$ следует $+$. Если в последовательности знаков содержатся также нули, то при подсчёте числа перемен знака они просто не принимаются во внимание.

ловом ряде

$$X(a), X_1(a), \dots, X_r(a),$$

в котором опущены все нули. Если тогда b и c , $b < c$, произвольные числа, для которых $f(x)$ не обращается в нуль, то число различных корней полинома $f(x)$ в интервале $b \leq x \leq c$ (засчитывая кратные корни только по одному разу) равно разности

$$\omega(b) - \omega(c).$$

Последовательность полиномов $X_1, X_2, \dots, X_r$ называется *рядом Штурма* для полинома $f(x)$. Теорема утверждает таким образом, что число корней, заключённых между b и c , равно числу перемен знака, потерянных при переходе от b к c .

Доказательство. Последний полином X_r ряда Штурма является, очевидно, наибольшим общим делителем полиномов $X = f(x)$ и $X_1 = f'(x)$. Если разделить все полиномы ряда Штурма на $c \cdot X_r$, где c — константа, то $f(x)$ освободится от кратных линейных множителей, число же перемен знаков для значений a , не являющихся корнями $f(x)$, не изменится; действительно, знаки членов ряда Штурма после такого деления либо все сохранятся, либо все изменятся на противоположные. Таким образом, мы можем при доказательстве предполагать это деление уже выполненным; тогда последний член ряда Штурма будет константой, отличной от нуля. При этом второй член ряда, вообще говоря, уже не будет служить производной для первого; так, если, скажем, d — есть l -кратный корень полинома $f(x)$, т. е.

$$X = f(x) = (x - d)^l g(x), \quad g(d) \neq 0,$$

$$X_1 = f'(x) = l(x - d)^{l-1} g(x) + (x - d)^l g'(x),$$

то в результате сокращения на $(x - d)^{l-1}$ получим два полинома вида

$$\bar{X} = (x - d) \cdot g(x),$$

$$\bar{X}_1 = l \cdot g(x) + (x - d) g'(x),$$

а наличие других кратных корней d' , d'' , ... вызовет ещё сокращение на наибольший общий делитель полиномов $g(x)$ и $g'(x)$. Мы обозначим изменённые так полиномы ряда Штурма снова через $X = X_0, X_1, \dots, X_r$.

При этом предположении два соседних члена ряда не смогут обратиться одновременно в нуль ни для какого a . Действительно, если бы, скажем, $X_k(a)$ и $X_{k+1}(a)$ были равны нулю, то из уравнений (1) последовательно вытекало бы, что $X_{k+2}(a), \dots, X_r(a)$ равны нулю, между тем как $X_r = \text{const} \neq 0$.

Корни полиномов ряда Штурма разбивают интервал $b \leq x \leq c$ на подинтервалы. Внутри каждого такого подинтервала ни X , ни X_k не обращаются в нуль; отсюда, по теореме Вейерштрасса о корнях, следует, что внутри такого интервала все полиномы ряда Штурма сохраняют свои знаки, и тем самым число $w(a)$ остаётся постоянным. Таким образом, нужно лишь ещё исследовать, как изменяется число $w(a)$ при переходе через значение d , в котором один из полиномов ряда Штурма обращается в нуль.

Пусть сперва d — корень полинома X_k ($0 < k < r$). В силу равенства

$$X_{k-1} = Q_k X_k - X_{k+1}$$

числа $X_{k-1}(d)$ и $X_{k+1}(d)$, необходимо, имеют противоположные знаки. Тогда и в двух подинтервалах, примыкающих к d , X_{k-1} и X_{k+1} имеют противоположные знаки. Но в таком случае, какой бы знак ни имел X_k ($+$, $-$ или 0), — для числа перемен знака между X_{k-1} и X_{k+1} это совершенно безразлично: налицо всегда точно одна перемена знака. Таким образом, при переходе a через значение d число $w(a)$ вовсе не изменяется.

Пусть теперь d — корень полинома $f(x)$, так что, по сделанному выше замечанию,

$$\begin{aligned} X &= (x-d)g'_1(x), & g'_1(d) &\neq 0, \\ X_1 &= l \cdot g(x) + (x-d)g'(x), \end{aligned}$$

где l — натуральное число. Знак полинома X_1 при $x=d$, а следовательно, и в обоих примыкающих к этому значению подинтервалах, совпадает со знаком $g(d)$, тогда как знак X для каждого значения x совпадает со знаком $(x-d)g(d)$. Таким образом, при $a < d$ мы имеем между $X(a)$ и $X_1(a)$ перемену знака, а при $a > d$, напротив, — совпадение знаков. Все же остальные возможные перемены знака в ряде Штурма, как уже показано, сохраняются при переходе через значение d . Следовательно, число $w(a)$ при переходе a через значение d уменьшается на единицу. Тем самым теорема Штурма доказана.

Для применения теоремы Штурма к определению общего числа различных корней полинома $f(x)$ следует в качестве границы b взять столь малое, а в качестве границы c — столь большое значения, чтобы среди значений $x < b$ и $x > c$ уже не содержалось корней полинома $f(x)$. Достаточно, например, выбрать $b = -M$ и $c = M$. Однако, ещё удобнее выбрать b и c так, чтобы ни один из полиномов ряда Штурма не имел корней среди значений $x < b$ и $x > c$. Тогда знаки этих полиномов будут определяться знаками их старших коэффициентов: знак полинома $a_0 x^m + a_1 x^{m-1} + \dots$ для очень больших значений x совпадает со знаком a_0 , а для очень больших по абсолютной величине отрицательных значений x — со знаком $(-1)^m a_0$. Поэтому при таком способе не приходится думать о том,

как велики должны быть b и c : достаточно определить лишь знаки старших коэффициентов полиномов Штурма и степени этих полиномов.

Задача 1. Определить число вещественных корней полинома

$$x^3 - 5x^2 + 3x - 8.$$

Между какими последовательными целыми числами лежат эти корни?

Задача 2. Если последние два полинома X_{r-1} , X_r ряда Штурма имеют степени 1, 0, то константу X_r (или, что только и нужно, — её знак) можно также вычислить, подставляя корень полинома X_{r-1} в $-X_{r-2}$.

Задача 3. Если при вычислении ряда Штурма встретится полином X_k , нигде не меняющий своего знака (скажем, являющийся суммой квадратов), то ряд можно оборвать на этом X_k . Равным образом, каждое X_k , обладающее всюду положительным множителем, можно всегда сократить на этот множитель и продолжать вычисление с этим изменённым X_k .

Задача 4. Полином X_1 [делитель производной $f'(x)$], использованный при доказательстве теоремы Штурма, обязательно меняет свой знак между двумя соседними корнями полинома $f(x)$. Доказать! Поэтому $f'(x)$ обращается по крайней мере один раз в нуль между каждыми двумя корнями полинома $f(x)$ (теорема Ролля).

Задача 5. Вывести из теоремы Ролля теорему о среднем значении (из дифференциального исчисления), утверждающую, что

$$\frac{f(b) - f(a)}{b - a} = f'(c)$$

для некоторого c , заключённого между a и b . [Положить

$$f(x) - f(a) - \frac{f(b) - f(a)}{b - a} (x - a) = \varphi(x).]$$

Задача 6. В интервале $a \leq x \leq b$, где $f'(x) > 0$, $f(x)$ есть возрастающая функция от x , а в интервале, где $f'(x) < 0$, — убывающая.

Задача 7. Полином $f(x)$ обладает в каждом интервале $a \leq x \leq b$ наибольшим и наименьшим значениями, причём каждое из них достигается либо в корне производной $f'(x)$, либо в одном из концов a , b интервала.

§ 69. Поле комплексных чисел.

Присоединяя к полю вещественных чисел $\mathbb{R}$ корень i неприводимого в $\mathbb{R}$ полинома $x^2 + 1$, получаем *поле комплексных чисел* $\mathbb{Q} = \mathbb{R}(i)$.

Говоря о «числах», мы будем в дальнейшем всюду подразумевать комплексные (в частности — вещественные) числа. *Алгебраи-*

ческие числа суть числа, алгебраические относительно поля рациональных чисел Γ . Ясно, что понимать теперь под алгебраическими числовыми полями, вещественными числовыми полями и т. д. Вследствие теорем § 35, алгебраические числа образуют поле A ; в нём содержатся все алгебраические числовые поля.

Докажем теперь следующее предложение:

В поле комплексных чисел уравнение $x^2 = a + bi$ (a, b вещественны) всегда разрешимо; иными словами, каждое число обладает в этом поле «квадратным корнем».

Доказательство. Число $x = c + di$ (c, d вещественны) обладает требуемым свойством тогда и только тогда, когда

$$(c + di)^2 = a + bi,$$

т. е. когда выполнены условия

$$c^2 - d^2 = a, \quad 2cd = b.$$

Из этих равенств вытекает далее: $(c^2 + d^2)^2 = a^2 + b^2$ и, следовательно, $c^2 + d^2 = \sqrt{a^2 + b^2}$. Отсюда и из первого условия определяются c^2 и d^2 :

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2},$$

$$d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Стоящие справа величины действительно ≥ 0 . Следовательно, c и d определяются ими с точностью до знака. Перемножение даёт

$$4c^2d^2 = -a^2 + (a^2 + b^2) = b^2;$$

следовательно, знаки у c и d можно определить так, чтобы выполнялось и второе условие

$$2cd = b.$$

Из доказанного следует, что в поле комплексных чисел можно решить каждое квадратное уравнение

$$x^2 + px + q = 0,$$

приводя его к виду

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q.$$

Решением будет

$$x = -\frac{p}{2} \pm w,$$

где w — какое-нибудь решение уравнения $w^2 = \frac{p^2}{4} - q$.

«Основная теорема алгебры», которую лучше было бы назвать основной теоремой учения о комплексных числах, утверждает, что

в поле $\mathfrak{Q}$ не только каждый квадратный полином, но и вообще любой полином $f(z)$, не являющийся константой, обладает корнями. Пожалуй, простейшим доказательством этой фундаментальной теоремы является теоретико-функциональное, состоящее в следующем: если бы полином $f(z)$ не имел ни одного комплексного корня, то

$$\frac{1}{f(z)} = \varphi(z)$$

было бы функцией, регулярной во всей плоскости комплексного переменного z и остающейся ограниченной (даже стремящейся к нулю) при $z \rightarrow \infty$, т. е., по теореме Лиувилля, — константой; но тогда и $f(z)$ был бы константой.

Если пожелать ограничиться применением лишь самых первоначальных сведений из теории функций, то можно рассмотреть вместо функции $\varphi(z)$ также рациональную функцию

$$\psi(z) = \frac{\varphi(z) - \varphi(0)}{z},$$

которая одновременно с $\varphi(z)$ регулярна во всей плоскости z . Интеграл этой функции по окружности K радиуса R с центром в начале координат должен быть, таким образом, равен нулю:

$$\int_K \frac{\varphi(z) - \varphi(0)}{z} dz = \int_0^{2\pi} [\varphi(Re^{i\theta}) - \varphi(0)] i d\theta = 0.$$

Но для достаточно больших R

$$|\varphi(Re^{i\theta})| < \epsilon,$$

$$\left| \int_0^{2\pi} \varphi(Re^{i\theta}) i d\theta \right| < 2\pi \epsilon;$$

далее

$$\int_0^{2\pi} \varphi(0) i d\theta = 2\pi i \varphi(0);$$

следовательно

$$|2\pi i \varphi(0)| < 2\pi \epsilon,$$

$$\varphi(0) = 0,$$

и мы приходим к противоречивому равенству

$$1 = f(0) \varphi(0) = 0.$$

Гаусс дал пять доказательств фундаментальной теоремы. Со вторым гауссовским доказательством, опирающимся лишь на простейшие свойства вещественных и комплексных чисел, не зато использующим довольно сложные алгебраические средства, мы познакомимся в § 70¹⁾.

¹⁾ Другое простое доказательство см. в книге С. Jordan, Cours d'Analyse I, 3-е изд., стр. 202. Интуитивистское доказательство дал Н. Вейль: Math. Zeitschr., 20 (1924), 142—150.

Под *абсолютной величиной* $|\alpha|$ комплексного числа $\alpha = a + bi$ понимают вещественное число

$$|\alpha| = \sqrt{a^2 + b^2} = \sqrt{\alpha \bar{\alpha}},$$

где $\bar{\alpha}$ есть комплексно-сопряжённое с α , т. е. сопряжённое относительно поля вещественных чисел, число $a - bi$.

Очевидно, $|\alpha| \geq 0$, причём $|\alpha| = 0$ лишь для $\alpha = 0$. Далее, $\sqrt{\alpha \bar{\alpha} \beta \bar{\beta}} = \sqrt{\alpha \bar{\alpha}} \sqrt{\beta \bar{\beta}}$ и, следовательно,

$$(1) \quad |\alpha \beta| = |\alpha| |\beta|.$$

Для доказательства соотношения

$$(2) \quad |\alpha + \beta| \leq |\alpha| + |\beta|$$

предположим на один момент уже известным более специальное соотношение

$$(3) \quad |1 + \gamma| \leq 1 + |\gamma|.$$

Если $\alpha = 0$, то (2) тривиально; если же $\alpha \neq 0$, то, используя неравенство (3), имеем:

$$\begin{aligned} |\alpha + \beta| &= |\alpha(1 + \alpha^{-1}\beta)| = |\alpha| |1 + \alpha^{-1}\beta| \leq \\ &\leq |\alpha| (1 + |\alpha^{-1}\beta|) = |\alpha| + |\beta|. \end{aligned}$$

Для доказательства соотношения (3) положим $\gamma = a + bi$. Тогда

$$|\gamma| = \sqrt{a^2 + b^2} > \sqrt{a^2} = |a|,$$

$$\begin{aligned} |1 + \gamma|^2 &= (1 + \gamma)(1 + \bar{\gamma}) = 1 + \gamma + \bar{\gamma} + \gamma\bar{\gamma} = \\ &= 1 + 2a + |\gamma|^2 \leq 1 + 2|\gamma| + |\gamma|^2 = (1 + |\gamma|)^2, \end{aligned}$$

следовательно,

$$|1 + \gamma| \leq 1 + |\gamma|,$$

чем (3), а значит и (2), доказано.

§ 70. Алгебраическая теория вещественных полей.

Расположенные поля, в частности вещественные числовые поля, обладают тем свойством, что в них суммы квадратов обращаются в нуль лишь в том случае, когда каждое слагаемое в отдельности равно нулю. Или, что равнозначно этому: —1 не может быть представлена в виде суммы квадратов¹⁾. Поле комплексных чисел не

¹⁾ Если в каком-либо поле элемент —1 может быть представлен в виде суммы $\sum a_i^2$, то $1^2 + \sum a_i^2 = 0$; тем самым 0 есть сумма квадратов, с основаниями, которые не все равны нулю. Обратное, если задана сумма $\sum b_i^2 = 0$,

обладает этим свойством, так как в нём — 1 даже сама является квадратом. Мы увидим, что указанное свойство является отличительным свойством вещественных алгебраических числовых полей и полей с ними сопряжённых (в поле всех алгебраических чисел) и может быть использовано для алгебраического построения поля вещественных алгебраических чисел вместе с сопряжёнными полями. Введём следующее определение ¹⁾:

Поле, в котором — 1 не представима в виде суммы квадратов, называется формально вещественным.

Всякое формально вещественное поле имеет характеристику нуль; действительно, в поле характеристики p можно представить — 1 в виде суммы $p - 1$ слагаемых ²⁾. Подполе формально вещественного поля, очевидно, также формально вещественно.

Поле P называется вещественно замкнутым ²⁾, если само P формально вещественно, однако никакое его собственное алгебраическое расширение уже не формально вещественно.

Теорема 1. *Каждое вещественно замкнутое поле может быть расположено и притом лишь единственным образом.*

Пусть P вещественно замкнуто. Мы докажем следующее:

Если a — элемент из P , отличный от 0, то либо сам a квадрат, либо — a квадрат, и эти случаи исключают друг друга. Суммы квадратов элементов поля P сами суть квадраты.

Теорема 1 будет непосредственно следовать отсюда; действительно, принимая тогда $a > 0$, если a — квадрат, отличный от нуля, мы, очевидно, введём расположение в поле P , и это — единственно возможное расположение, поскольку квадраты при каждом расположении должны быть ≥ 0 .

Если γ не является квадратом никакого элемента из P , то $P(\sqrt{\gamma})$, где $\sqrt{\gamma}$ — корень полинома $x^2 - \gamma$, будет собственным алгебраическим расширением поля P и, следовательно, не будет формально вещественным. Поэтому имеет место равенство

$$-1 = \sum_{v=1}^n (\alpha_v \sqrt{\gamma} + \beta_v)^2$$

или

$$-1 = \gamma \sum_{v=1}^n \alpha_v^2 + \sum_{v=1}^n \beta_v^2 + 2\sqrt{\gamma} \sum_{v=1}^n \alpha_v \beta_v,$$

в которой некоторое $\beta_{\lambda} \neq 0$, то это β_{λ} можно привести к единице, разделив сумму на β_{λ}^2 , перенеся тогда единицу в другую часть равенства, получим $-1 = \sum \alpha_v^2$.

¹⁾ См. E. Artin u. O. Schreier, *Algebraische Konstruktion reeller Körper*. *Abh. Math. Sem. Hamburg*, 5 (1926), 85—99.

²⁾ Краткое наименование «вещественно замкнуто» предпочитают более точному: «вещественно алгебраически замкнуто».

где α, β , принадлежат полю P . Здесь последний член должен обратиться в нуль, так как иначе $\sqrt{\gamma}$, в противоречие с предположением, лежал бы в P . Напротив, первый член не может обратиться в нуль, так как иначе P не было бы формально вещественным. Отсюда прежде всего заключаем, что γ непредставимо в P в виде суммы квадратов, так как иначе мы для -1 получили бы представление в виде суммы квадратов. Таким образом: если γ не является квадратом, то оно не является и суммой квадратов; или то же самое в положительной форме: каждая сумма квадратов в P является также квадратом в P .

Но теперь получаем:

$$- \gamma = \frac{1 + \sum_{v=1}^n \beta_v^2}{\sum_{v=1}^n \alpha_v^2}.$$

Числитель и знаменатель этого выражения являются суммами квадратов и, следовательно, сами суть квадраты; поэтому $- \gamma = c^2$, где c — элемент из P . Таким образом, для каждого элемента γ из P удовлетворяется по крайней мере одно из равенств $\gamma = b^2$, $- \gamma = c^2$; но при $\gamma \neq 0$ оба одновременно выполняться не могут, так как иначе мы имели бы $-1 = \left(\frac{b}{c}\right)^2$, что невозможно.

Основываясь на теореме 1, мы всюду в дальнейшем будем предполагать вещественно замкнутые поля расположенными.

Теорема 2. *В вещественно замкнутом поле каждый полином нечётной степени обладает по крайней мере одним корнем.*

Для полинома степени 1 теорема тривиальна. Примем, что она уже доказана для всех нечётных степеней $< n$, и пусть $f(x)$ — полином нечётной степени n (> 1). Если $f(x)$ приводим в вещественно замкнутом поле P , то по крайней мере один из неприводимых его множителей имеет нечётную степень $< n$ и потому обладает в P корнем. Приведём теперь предположение о неприводимости $f(x)$ к абсурду. Действительно, пусть $f(x)$ неприводим и α — символически присоединённый корень этого полинома. Тогда $P(\alpha)$ не является формально вещественным, и потому имеет место равенство

$$(1) \quad -1 = \sum_{v=1}^r (\varphi_v(\alpha))^2,$$

где $\varphi_v(x)$ — полиномы не выше $(n-1)$ -й степени с коэффициентами из P . Из (1), в силу неприводимости $f(x)$, получаем тождество

$$(2) \quad -1 = \sum_{v=1}^r (\varphi_v(x))^2 + f(x)g(x).$$

Сумма $\sum_{v=1}^r (\varphi_v(x))^2$ есть полином чётной степени, так как старшие коэффициенты слагаемых являются квадратами и потому не могут при сложении сократиться. Далее, степень эта положительна, так как иначе уже равенство (1) было бы противоречиво. Поэтому $g(x)$ имеет нечётную степень $\leq n-2$ и, значит, во всяком случае обладает в P корнем. Но, подставив этот корень a в (2), мы получим

$$-1 = \sum_{v=1}^r (\varphi_v(a))^2,$$

чем и будет достигнуто противоречие, так как $\varphi_v(a)$ лежат в P .

Теорема 3. *Вещественно замкнутое поле не является алгебраически замкнутым. Напротив, поле, получающееся в результате присоединения к нему i^1 , уже алгебраически замкнуто.*

Первое утверждение теоремы тривиально, так как уже уравнение $x^2 + 1 = 0$ неразрешимо в формально вещественном поле.

Второе утверждение непосредственно вытекает из следующей теоремы:

Теорема 3а. *Если в расположенном поле K из каждого положительного элемента извлекается квадратный корень, и каждый полином нечётной степени обладает по крайней мере одним корнем, то поле, получающееся в результате присоединения i , алгебраически замкнуто.*

Прежде всего заметим, что в $K(i)$ каждый элемент обладает квадратным корнем, и потому каждое квадратное уравнение разрешимо. Доказывается это таким же вычислением, как и для случая поля комплексных чисел в § 69.

Для доказательства алгебраической замкнутости поля $K(i)$ достаточно, по § 62, показать, что каждый полином $f(x)$, неприводимый над K , обладает корнем в $K(i)$. Пусть $f(x)$ — полином без кратных корней, имеющий степень n , где $n = 2^m q$, q — нечётное. Мы применим индукцию по m , в соответствии с чем предположим, что каждый полином без кратных корней с коэффициентами из K , степень которого делится на 2^{m-1} , но не на 2^m , обладает корнем в $K(i)$. (Для $m = 1$ это имеет место по предположению.) Пусть $\alpha_1, \alpha_2, \dots, \alpha_n$ — корни полинома $f(x)$ в некотором расширении поля $K(i)$. Выберем c в K так, чтобы $\frac{n(n-1)}{2}$ выражений $\alpha_j \alpha_k + c(\alpha_j + \alpha_k)$, $1 \leq j < k \leq n$, имели попарно различные значения²⁾. Так как эти выражения удовлетворяют уравнению степени $\frac{n(n-1)}{2}$ над K , то согласно предпо-

¹⁾ i здесь и всюду в дальнейшем означает корень полинома $x^2 + 1$.

²⁾ Это возможно вследствие отсутствия у $f(x)$ кратных корней.

ложению, по крайней мере одно из них, скажем $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$, лежит в $K(i)$. Но в силу условия, наложенного на c , имеем (см. § 40)

$$K(\alpha_1\alpha_2, \alpha_1 + \alpha_2) = K(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2));$$

следовательно, α_1 и α_2 находятся путём решения квадратного уравнения в $K(i)$.

Из теоремы 3а одновременно следует (в соединении с § 68), что поле комплексных чисел алгебраически замкнуто. Это и есть «основная теорема алгебры» (см. § 69).

Обращением теоремы 3 является

Теорема 4. Если присоединение i к формально вещественному полю K даёт алгебраически замкнутое поле, то K вещественно замкнуто.

Доказательство. Между K и $K(i)$ не имеется никакого промежуточного поля; следовательно, не существует никаких алгебраических расширений поля K , кроме самого K и $K(i)$. Но $K(i)$ не является формально вещественным, так как в нём — 1 есть квадрат. Следовательно, K вещественно замкнуто.

Из теоремы 4, в частности, следует, что поле вещественных чисел вещественно замкнуто.

Корни уравнения $f(x) = 0$ с коэффициентами из вещественно замкнутого поля K лежат в $K(i)$; поэтому корни, не содержащиеся в K , должны быть попарно сопряжены (относительно K). Если $a + bi$ — корень, то $a - bi$ будет сопряжённым корнем. Объединяя в разложении полинома $f(x)$ каждую пару сопряжённых линейных множителей, мы получим разложение $f(x)$ на линейные и квадратные множители, неприводимые в K .

Мы теперь в состоянии распространить теорему Вейерштрасса из § 68 на произвольные вещественно замкнутые поля.

Теорема 5. Пусть $f(x)$ — полином с коэффициентами из вещественно замкнутого поля P и a, b — элементы из P , для которых $f(a) < 0$, $f(b) > 0$. Тогда в P существует по крайней мере один элемент c между a и b , для которого $f(c) = 0$.

Доказательство. Как мы только что видели, $f(x)$ распадается в P на линейные и неприводимые квадратные множители. Неприводимый квадратный полином $x^2 + px + q$ всюду положителен в P ; действительно, он может быть записан в виде $(x + \frac{p}{2})^2 + (q - \frac{p^2}{4})$, где первый член всегда ≥ 0 , а второй положителен вследствие предположенной неприводимости. Поэтому $f(x)$ может переменить знак лишь при перемене знака одним из линейных множителей, значит, лишь при наличии корня между a и b .

На основании этой теоремы, для вещественно замкнутых полей справедливы также все следствия, выведенные в § 68 из теоремы Вейерштрасса, и в частности верна теорема Штурма о вещественных корнях.

Докажем в заключение следующую теорему.

Теорема 6. Пусть K — расположенное поле и $\bar{K}$ — поле, получающееся из K в результате присоединения квадратных корней из всех его положительных элементов. Тогда $\bar{K}$ формально вещественно.

Очевидно, достаточно показать, что не может иметь места никакое равенство вида

$$(3) \quad -1 = \sum_{v=1}^n c_v \xi_v^2$$

с положительными элементами c_v из K и элементами ξ_v из $\bar{K}$. Предположим, что такое равенство существует. В элементах ξ_v может действительно содержаться лишь конечное число присоединённых к K квадратных корней; пусть это будут, скажем, $\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_r}$. Среди всех равенств вида (3) выберем такое, в котором r имеет наименьшее возможное значение. [r во всяком случае ≥ 1 , так как в K не существует равенства вида (3).] ξ_v может быть представлено в виде $\xi_v = \eta_v + \zeta_v \sqrt{a_r}$, где η_v, ζ_v лежат в $K(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_{r-1}})$. Следовательно, имеем

$$(4) \quad -1 = \sum_{v=1}^n c_v \eta_v^2 + \sum_{v=1}^n c_v a_r \zeta_v^2 + 2 \sqrt{a_r} \sum_{v=1}^n c_v \eta_v \zeta_v.$$

Если последнее слагаемое в (4) равно нулю, то (4) есть равенство вида (3), содержащее, однако, меньше чем r квадратных корней. Если же это слагаемое отлично от нуля, то элемент $\sqrt{a_r}$ лежит в $K(\sqrt{a_1}, \dots, \sqrt{a_{r-1}})$, и само равенство (3) может быть записано с помощью меньшего чем r числа корней. Таким образом, в любом случае наше предположение ведёт к противоречию.

Задача 1. Поле алгебраических чисел алгебраически замкнуто, а поле вещественных алгебраических чисел вещественно замкнуто.

Задача 2. Алгебраически замкнутое алгебраическое расширение поля Γ , допускающее по § 62 чисто алгебраическое построение, изоморфно полю A алгебраических чисел.

Задача 3. Пусть P — некоторое вещественное числовое поле и Σ — поле всех вещественных чисел, алгебраических относительно поля P . Тогда Σ вещественно замкнуто.

Задача 4. Если P' формально вещественно, и t трансцендентно относительно P , то $P(t)$ также формально вещественно. [Подставить в $-1 = \sum [\varphi_v(t)]^2$ вместо t подходяще выбранную константу из P .]

§ 71. Теоремы существования для формально вещественных полей.

Теорема 7. Пусть K — счётное формально вещественное поле и Ω — также счётное алгебраически замкнутое расширение поля K . Тогда между K и Ω существует (по меньшей мере одно) вещественно замкнутое поле P такое, что $\Omega = P(i)$.

Доказательство. Пусть $\omega_1, \omega_2, \dots$ — элементы поля Ω . Определим последовательность расширений $\Sigma_1, \Sigma_2, \dots$ поля K с помощью полной индукции следующим образом:

$$\Sigma_1 = K,$$

$$\Sigma_{n+1} = \Sigma_n(\omega_n), \text{ если } \Sigma_n(\omega_n) \text{ формально вещественно,}$$

$$\Sigma_{n+1} = \Sigma_n \text{ — в противном случае.}$$

Наконец, определим P как объединение всех Σ_n .

С помощью полной индукции непосредственно заключаем, что все поля Σ_n формально вещественны. Но тогда и их объединение P формально вещественно, так как если бы в P существовало представление $1 = \sum a_i^2$, то оно имело бы место уже в некотором Σ_n , а именно в том, которое содержит все a_i .

Пусть теперь $\omega = \omega_n$ — элемент из Ω , не содержащийся в P . Тогда ω_n не содержится также в Σ_{n+1} , следовательно, $\Sigma_n(\omega_n)$ не формально вещественно и, следовательно, тем более $P(\omega)$ не формально вещественно. Но это возможно, прежде всего, лишь если ω является алгебраическим относительно P , поскольку простое трансцендентное расширение формально вещественного поля снова формально вещественно (§ 70, задача 4). Таким образом, каждый элемент поля Ω является алгебраическим относительно P , т. е. поле Ω алгебраическое относительно P . Так как, далее, в качестве ω можно взять произвольный алгебраический элемент из Ω , не лежащий в P , то никакое собственное простое алгебраическое расширение $P(\omega)$ поля P не является формально вещественным, и тем самым P вещественно замкнуто. Тогда, по теореме 3 (§ 70), $P(i)$ алгебраически замкнуто и, значит, совпадает с Ω . Тем самым теорема доказана.

З а м е ч а н и е. Эта теорема и её доказательство сохраняют силу, лишь с совсем несущественными изменениями, и в том случае, когда Ω не счётно, но зато вполне упорядочено. Таким образом, основываясь на теореме Цермело о полном упорядочении, можно высказать теорему 7 также без предположения счётности. Однако для важнейших применений достаточно уже счётного случая, который мы здесь только и рассматриваем.

Сформулируем особо некоторые частные случаи и непосредственные следствия теоремы 7.

Теорема 7а. Для каждого счётного формально вещественного поля K существует (по крайней мере одно) вещественно замкнутое алгебраическое расширение.

Для доказательства нужно лишь в теореме 7 взять в качестве поля Ω алгебраически замкнутое алгебраическое расширение поля K .

Теорема 7б. Каждое счётное формально вещественное поле может быть (по крайней мере одним способом) расположено.

Это непосредственно следует из теоремы 1 (§ 70) и теоремы 7а.

Взяв в теореме 7 в качестве Ω произвольное алгебраически замкнутое поле характеристики нуль, а в качестве K — поле рациональных чисел, получим:

Теорема 7с. Каждое счётное алгебраически замкнутое поле Ω характеристики нуль содержит (по крайней мере одно) вещественно замкнутое подполе P , такое, что $\Omega = P(i)$.

Для расположенных полей теорема 7а может быть существенно усилена:

Теорема 8. Для каждого счётного расположенного поля K существует — и с точностью до эквивалентных расширений только одно — вещественно замкнутое алгебраическое расширение P , расположение которого является продолжением расположения поля K . P не обладает никакими нетождественными автоморфизмами, которые оставляли бы все элементы из K на месте.

Доказательство. Как и в теореме 6 (§ 70), обозначим через $\bar{K}$ поле, получающееся из K в результате присоединения квадратных корней из всех его положительных элементов. Пусть P — алгебраическое вещественно замкнутое расширение поля K . Поскольку мы уже знаем, что $\bar{K}$ формально вещественно, такое расширение по теореме 7а существует. P является алгебраическим также относительно $\bar{K}$, и расположение поля P представляет собой продолжение расположения поля K , так как всякий положительный элемент из K является квадратом в $\bar{K}$, а значит, тем более в P . Тем самым существование требуемого поля P доказано.

Для доказательства единственности поля P предположение счётности поля K не требуется.

Пусть P^* — второе алгебраическое вещественно замкнутое расширение поля K , обладающее тем свойством, что его расположение служит продолжением расположения поля K . Пусть $f(x)$ — полином с коэффициентами из K (не обязательно неприводимый). Теорема Штурма даёт возможность определить, не выходя за пределы поля K , сколькими корнями обладает $f(x)$ в P или в P^* : для этого нужно лишь рассмотреть ряд Штурма для $f(x) = x^n + a_1x^{n-1} + \dots + a_n$. Поэтому $f(x)$ имеет в P столько же корней, сколько и в P^* . В частности, каждое уравнение с коэффициентами из K , обладающее по крайней мере одним корнем в P , обладает по крайней мере одним корнем и в P^* , и обратно. Пусть теперь $\alpha_1, \alpha_2, \dots, \alpha_r$ — корни $f(x)$

в P , $\beta_1^*, \beta_2^*, \dots, \beta_r^*$ — корни $f(x)$ в P^* . Далее, пусть ξ выбрано в P так, что $K(\xi) = K(\alpha_1, \dots, \alpha_r)$, и $F(x) = 0$ — неприводимое над K уравнение для ξ . Таким образом, $F(x)$ обладает в P корнем ξ , и потому также в P^* по крайней мере одним корнем η^* ; $K(\xi)$ и $K(\eta^*)$ являются эквивалентными расширениями поля K . Так как $K(\xi)$ порождается r корнями $\alpha_1, \dots, \alpha_r$ полинома $f(x)$, то также $K(\eta^*)$ должно порождаться r корнями этого полинома. А так как $K(\eta^*)$ есть подполе поля P^* , то $K(\eta^*) = K(\beta_1^*, \dots, \beta_r^*)$. Таким образом, $K(\alpha_1, \dots, \alpha_r)$ и $K(\beta_1^*, \dots, \beta_r^*)$ являются эквивалентными расширениями поля K .

Для того чтобы показать теперь, что P и P^* — эквивалентные расширения поля K , заметим, что изоморфное отображение P на P^* , необходимо, должно сохранять расположение, поскольку последнее (согласно доказательству теоремы 1 § 70) определяется свойством элемента поля быть или не быть квадратом. Мы определим поэтому следующее отображение σ поля P на P^* . Пусть α — элемент из P , $p(x)$ — неприводимый полином над K , имеющий корнем α , и $\alpha_1, \alpha_2, \dots, \alpha_r$ — корни этого полинома в P , занумерованные так, что $\alpha_1 < \alpha_2 < \dots < \alpha_r$; в частности, пусть $\alpha = \alpha_k$. Если тогда $\alpha_1^*, \alpha_2^*, \dots, \alpha_r^*$ — корни полинома $p(x)$ в P^* и $\alpha_1^* < \alpha_2^* < \dots < \alpha_r^*$, то полагаем $\sigma(\alpha) = \alpha_k^*$. Очевидно, отображение σ однозначно и оставляет все элементы из K на месте. Нужно показать, что σ — изоморфное отображение. Для этой цели рассмотрим снова произвольный полином $f(x)$ над K ; пусть $\gamma_1, \gamma_2, \dots, \gamma_s$ — его корни в P и $\gamma_1^*, \gamma_2^*, \dots, \gamma_s^*$ — корни в P^* . Далее, пусть $g(x)$ — полином над K , имеющий своими корнями квадратные корни из положительных разностей корней полинома $f(x)$, $\delta_1, \delta_2, \dots, \delta_t$ — корни $g(x)$ в P и $\delta_1^*, \delta_2^*, \dots, \delta_t^*$ — в P^* . По доказанному выше, $\Delta = K(\gamma_1, \dots, \gamma_s, \delta_1, \dots, \delta_t)$ и $\Delta^* = K(\gamma_1^*, \dots, \gamma_s^*, \delta_1^*, \dots, \delta_t^*)$ являются эквивалентными расширениями поля K . Таким образом, существует изоморфное отображение τ поля Δ на Δ^* , оставляющее на месте все элементы из K . Это отображение относит каждому γ некоторое γ^* и каждому δ — некоторое δ^* . Выберем обозначения так, чтобы $\tau(\gamma_k) = \gamma_k^*$, $\tau(\delta_h) = \delta_h^*$. Если теперь $\gamma_k < \gamma_l$ (в P), то $\gamma_l - \gamma_k = \delta_h^2$ для некоторого индекса h , значит, также $\gamma_l^* - \gamma_k^* = \delta_h^{*2}$, и потому $\gamma_k^* < \gamma_l^*$ (в P^*). Таким образом, τ ставит друг другу в соответствие корни полинома $f(x)$ в P и в P^* по их величине. Так как отсюда следует, что то же имеет место и для корней неприводимых в K множителей полинома $f(x)$, то имеем $\tau(\gamma_k) = \sigma(\gamma_k)$ ($k = 1, 2, \dots, s$). Выбрав теперь полином $f(x)$ так, чтобы среди его корней содержались два произвольных наперёд заданных элемента α, β из P , равно как и их сумма $\alpha + \beta$ и произведение $\alpha \cdot \beta$, убедимся в том, что σ есть изоморфное отображение поля P на P^* , и притом единственное, оставляющее все элементы из K на месте. Взяв, в частности, $P = P^*$,

получим справедливость нашего утверждения относительно автоморфизмов поля P .

Так как, согласно § 66, поле рациональных чисел Γ допускает только одно расположение, то из теоремы 8 непосредственно следует:

Теорема 8а. Существует — и притом с точностью до изоморфизма только одно — вещественно замкнутое алгебраическое расширение поля Γ .

В качестве этого поля можно, разумеется, взять поле вещественных алгебраических чисел в обычном смысле (§ 67), получающееся путём выделения алгебраических чисел из совокупности всех вещественных. Однако этот трансцендентный окольный путь можно заменить чисто алгебраическим построением из теоремы 7 (принимая $K = \Gamma$ и беря в качестве Ω алгебраически замкнутое алгебраическое расширение A поля Γ). Тем самым будет чисто алгебраическим путём построено поле *вещественных алгебраических чисел*; обозначим его через P . Поле всех алгебраических чисел будет иметь вид $A = P(i)$.

Как мы ещё увидим, P является в A не единственным вещественно замкнутым полем, а лишь одним из бесконечного множества эквивалентных ему.

Теорема 9. Каждое формально вещественное счётное алгебраическое расширение K^ поля Γ изоморфно некоторому подполю поля P , т. е. некоторому вещественному алгебраическому числовому полю.*

Доказательство. По теореме 7а для всякого поля K^* указанного типа можно построить алгебраическое вещественно замкнутое расширение P^* , причём в силу теоремы 8а оно, необходимо, будет изоморфно полю P . Отсюда и следует утверждение.

Каждое изоморфное отображение поля K^* на $K \subseteq P$, естественно, определяет также некоторое расположение поля K^* , поскольку все подполя K из P уже заранее расположены. И обратно, каждое расположение поля K^* может быть получено таким образом, так как построение вещественно замкнутого расширения P^* поля K^* , упомянутого при доказательстве теоремы 9, может быть, по теореме 8, выполнено с сохранением расположения в K^* . Такое расположение поля P^* перейдёт тогда при изоморфизме в (единственно возможное) расположение поля P .

Взяв, в частности, в качестве K^* конечное алгебраическое числовое поле, обладающее в A лишь конечным числом изоморфизмов, получим:

Число изоморфизмов, переводящих K^ в вещественное алгебраическое числовое поле, равно числу различных возможных расположений поля K^* (и в частности, равно нулю, если K^* не является формально вещественным).*

То обстоятельство, что каждое формально вещественное поле, содержащееся в A , может быть расширено до вещественно замкнутого поля

$P^* \subset A$, показывает вместе с тем, что в A содержится бесконечное множество таких полей P^* (которые, впрочем, по теореме 8а все изоморфны между собой). Действительно, всякое поле $K_\zeta^* = \Gamma(\zeta^{\sqrt[n]{2}})$, где n — нечётное натуральное число и ζ — корень n -ной степени из единицы, изоморфно полю $\Gamma(\sqrt[n]{2})$ и, следовательно, формально вещественно. Эти поля K_ζ^* обладают, каждое, некоторым вещественно замкнутым расширением P_ζ^* , и эти последние поля при фиксированном n должны быть все различны, так как расположенное поле может содержать лишь один корень n -ной степени из числа 2 (§ 66, задача 5). Число же n таких полей может быть взято произвольно большим.

Задача 1. Пусть ϑ — корень неприводимого в Γ уравнения $x^4 - x - 1 = 0$. Сколькими способами может быть расположено поле $\Gamma(\vartheta)$?

Задача 2. Поле $\Gamma(t)$, где t — неизвестная, допускает бесконечное множество расположений и притом как архимедовских, так и неархимедовских. И t может быть взято как бесконечно большим, так и бесконечно малым (ср. § 66, задача 1).

Задача 3. Сколько корней имеет полином $(z^2 - t)^2 - t^3$ в вещественно замкнутом расширении поля $\Gamma(t)$, если t бесконечно мало? Где лежат эти корни?

§ 72. Суммы квадратов.

Мы исследуем теперь вопрос, какие элементы поля K могут быть представлены в виде сумм квадратов элементов из K .

При этом, прежде всего, можно будет ограничиться формально вещественными полями. Действительно, если K не формально вещественно, то -1 есть сумма квадратов, скажем,

$$-1 = \sum_1^n \alpha_v^2.$$

Если теперь характеристика поля K отлична от 2, то это равенство влечёт за собой разложение произвольного элемента γ из K на сумму $n+1$ квадратов:

$$\gamma = \left(\frac{1+\gamma}{2}\right)^2 + \left(\sum \alpha_v^2\right)\left(\frac{1-\gamma}{2}\right)^2.$$

Если же K имеет характеристику 2, то

$$\sum \alpha_v^2 = \left(\sum \alpha_v\right)^2,$$

так что γ есть сумма квадратов тогда и только тогда, когда γ само есть квадрат.

Что сумма и произведение сумм квадратов сами суть суммы квадратов, — непосредственно ясно. Но и отношение сумм квадратов есть также сумма квадратов:

$$\frac{\alpha}{\beta} = \alpha \cdot \beta \cdot (\beta^{-1})^2.$$

Докажем теперь для формально вещественных счётных полей K следующее предложение:

Если γ не является в K суммой квадратов, то существует такое расположение поля K , при котором γ отрицательно.

Доказательство. Пусть γ не есть сумма квадратов. Покажем прежде всего, что $K(\sqrt{-\gamma})$ формально вещественно. Если $\sqrt{-\gamma}$ лежит уже в K , то утверждение очевидно. В противном же случае рассуждаем так: если бы

$$-1 = \sum_1^n (\alpha_i \sqrt{-\gamma} + \beta_i)^2,$$

то тем же точно путём, что и при доказательстве теоремы 1 (§ 70), мы получили бы, что

$$\gamma = \frac{1 + \sum \beta_i^2}{\sum \alpha_i^2},$$

и тем самым γ было бы всё же суммой квадратов, в противоречие с предположением. Таким образом, $K(\sqrt{-\gamma})$ формально вещественно. Если мы теперь, согласно теореме 7b (§ 71), расположим поле $K(\sqrt{-\gamma})$, то $-\gamma$, как квадрат, окажется положительным. Тем самым наше утверждение доказано.

В применении к формально вещественным алгебраическим числовым полям (если принять во внимание, что все возможные расположения такого поля могут быть по § 71 получены посредством изоморфных отображений на сопряжённые вещественные числовые поля) это даёт следующую теорему:

Элемент γ алгебраического числового поля K является суммой квадратов в том и только в том случае, если ни при каком изоморфизме, переводящем K в сопряжённое с ним вещественное поле, γ не переводится в отрицательное число.

Эта теорема сохраняет силу и в том случае, когда K не формально вещественно, так как тогда все числа из K являются суммами квадратов, изоморфизмов же указанного вида вообще не существует.

Числа алгебраического числового поля K , переходящие в положительные числа при всяком изоморфном отображении этого поля на сопряжённые с ним вещественные числовые поля, называются *вполне положительными* в K . Если K не обладает вещественными

сопряжёнными полями, то тем самым каждое число из K может быть названо вполне положительным. Понятие вполне положительного элемента можно распространить на произвольные поля K , называя вполне положительными те элементы из поля K , которые оказываются положительными при всяком вообще возможном расположении этого поля. (В частности, вполне положительными будут снова все числа из поля K , не допускающего расположения, т. е. не формально вещественного.) Тогда результаты этого параграфа можно резюмировать следующим образом: *в счётном поле характеристики $\neq 2$ каждый вполне положительный элемент может быть представлен в виде суммы квадратов.*

Литература к главе 9.

Дальнейшие теоремы о числе квадратов, достаточном для представления вполне положительных чисел числового поля, можно найти в работе E. Landau, Über die Zerlegung total positiver Zahlen in Quadrate. *Göttinger Nachr.* 1919, 392—396. Для случая функциональных полей см. D. Hilbert, Über die Darstellung definiter Formen als Summen von Formenquadraten, *Math. Ann.*, 32 (1888), 342—350, а также E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Hamburg*, 5 (1923), 100—115.

ГЛАВА ДЕСЯТАЯ. НОРМИРОВАННЫЕ ПОЛЯ.

§ 73. Нормирования.

Изложенная в § 67 конструкция поля Ω для заданного расположенного поля K использует лишь расположенность абсолютных величин $|a|$ элементов поля, а не расположенность самого поля. Поэтому естественно попытаться распространить указанную конструкцию на любые, хотя бы и нерасположенные поля, для которых, однако, существует функция $\varphi(a)$, обладающая свойствами абсолютной величины.

Поле K называется *нормированным*, если для его элементов a определена функция $\varphi(a)$, называемая *нормой* и обладающая следующими свойствами:

1) $\varphi(a)$ есть элемент некоторого расположенного поля P , называемого *полем значений* нормы.

2) $\varphi(a) > 0$ для $a \neq 0$; $\varphi(0) = 0$.

3) $\varphi(ab) = \varphi(a)\varphi(b)$.

4) $\varphi(a+b) \leq \varphi(a) + \varphi(b)$.

Из 2) и 3) непосредственно следует, что

$$\varphi(1) = 1, \quad \varphi(-1) = 1, \quad \varphi(a) = \varphi(-a).$$

Из (4) следует

$$\varphi(c) - \varphi(a) \leq \varphi(c - a)$$

и точно так же

$$\varphi(a) - \varphi(c) \leq \varphi(c - a),$$

что в совокупности даёт

$$|\varphi(c) - \varphi(a)| \leq \varphi(c - a).$$

Условия 1) — 4) будут, в частности, выполнены, когда K само расположено, если принять $\varphi(a) = |a|$. Каждое поле допускает «тривиальное» нормирование: $\varphi(a) = 1$ для $a \neq 0$, $\varphi(0) = 0$. Существуют, однако, и совсем другие типы нормирований. Пусть Γ — поле рациональных чисел и p — фиксированное простое число. Записывая каждое рациональное число $a \neq 0$ в форме

$$a = \frac{s}{t} p^n,$$

где s и t — целые числа, не делящиеся на p , мы можем определить норму в поле Γ , положив

$$\varphi_p(a) = p^{-n}, \quad \varphi_p(0) = 0.$$

Действительно, выполнение условий 1) — 3) очевидно. Вместо же 4) имеет место более сильное неравенство

$$(1) \quad \varphi_p(a+b) \leq \max(\varphi_p(a), \varphi_p(b)).$$

В самом деле, если

$$a = \frac{s}{t} p^n, \quad b = \frac{u}{v} p^m, \quad s, t, u, v \text{ взаимно просты с } p,$$

и, скажем, $\varphi_p(b) \geq \varphi_p(a)$, т. е. $n \geq m$, то

$$a+b = \frac{svp^{n-m} + tu}{tv} p^m$$

и тем самым

$$\varphi_p(a+b) = p^{-m'} \quad \text{с } m' \geq m,$$

т. е.

$$\varphi_p(a+b) \leq \varphi_p(b).$$

Это — так называемое *p*-адическое нормирование поля Γ .

p-адическое нормирование нетрудно обобщить. Пусть $\mathfrak{o}$ — область целостности, K — её поле отношений и $\mathfrak{p}$ — простой идеал в $\mathfrak{o}$, обладающий следующими свойствами: А. Все степени $\mathfrak{p}$, $\mathfrak{p}^2, \dots$ попарно различны, и их пересечение равно нулю. В. Если a в $\mathfrak{o}$ делится точно на $\mathfrak{p}^\alpha$, т. е. делится на $\mathfrak{p}^\alpha$, но уже не делится на $\mathfrak{p}^{\alpha+1}$, и если, аналогично, b делится точно на $\mathfrak{p}^\beta$, то ab делится точно на $\mathfrak{p}^{\alpha+\beta}$. При этом $\mathfrak{p}^\alpha$ означает совокупность всех сумм $\sum p_{v_1} p_{v_2} \dots p_{v_\alpha}$, где p_{v_k} — элементы из $\mathfrak{p}$. В частности, $\mathfrak{p}^1 = \mathfrak{p}$ и, по определению, $\mathfrak{p}^0 = \mathfrak{o}$. Положим теперь

$$\varphi(0) = 0$$

и, если a в $\mathfrak{o}$ делится точно на $\mathfrak{p}^\alpha$,

$$\varphi(a) = e^{-\alpha},$$

где e — произвольное фиксированное вещественное число > 1 . $\varphi(a)$ будет удовлетворять условиям 1) — 4), определяя тем самым нормирование области $\mathfrak{o}$.

Но если уже определена норма в области целостности, то она сразу распространяется на элементы поля отношений этой области, если положить

$$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}.$$

Это определение однозначно, так как из

$$\frac{a}{b} = \frac{c}{d} \quad \text{или} \quad ad = bc$$

следует

$$\varphi(a)\varphi(d) = \varphi(b)\varphi(c) \quad \text{или} \quad \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(c)}{\varphi(d)}.$$

Далее, условия 1) — 3) для $\varphi\left(\frac{a}{b}\right)$, очевидно, выполнены, выполнение же условия 4) проверяется так:

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{\varphi(ad + bc)}{\varphi(bd)} \leq \frac{\varphi(ad) + \varphi(bc)}{\varphi(bd)} = \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right).$$

Таким образом, из нормирования области целостности $\mathfrak{p}$, определяемого простым идеалом $\mathfrak{p}$, сразу получается нормирование её поля отношений K ; это последнее нормирование называется $\mathfrak{p}$ -адическим нормированием поля K .

Условиям A и B удовлетворяют весьма многие простые идеалы. Например, в кольцах с однозначным разложением на множители свойствами A и B обладают все простые главные идеалы. В кольце же полиномов $\Delta[x_1, \dots, x_n]$ этими свойствами обладает также идеал

$$\mathfrak{p} = (x_1, \dots, x_n).$$

Соответствующей нормой $\varphi(f)$ будет здесь $e^{-\alpha}$, где α — наименьшая из степеней членов, входящих в полином f .

Задача 1. Отказавшись в определении нормы от требования, чтобы $\varphi(a)$ было неотрицательным, доказать, что если в K существует элемент c , для которого $\varphi(c) < 0$, то $a \rightarrow \varphi(a)$ есть изоморфное отображение поля K на некоторое подполе поля R . [То, что в 4) имеет место знак равенства, доказывается рассмотрением содержащегося в 4) неравенства для $\varphi(ac + bc)$.]

Задача 2. При $\mathfrak{p}$ -адическом нормировании неравенство 4) можно заменить более сильным неравенством (1).

Важнейшие исследования о нормированных полях относятся к случаю, когда поле R значений нормы архимедовски расположено. В этом случае, согласно задаче 3 § 67, R может быть вложено в поле вещественных чисел. В соответствии с этим мы примем теперь, что значения $\varphi(a)$ суть вещественные числа. При этом мы будем предполагать известными (натуральные) логарифмы вещественных чисел и их простейшие свойства, равно как и степени a^β положительного числа a с произвольными вещественными показателями β .

Кроме этого, мы воспользуемся ещё следующей леммой о вещественных числах:

Если α, β, γ — положительные вещественные числа и

$$\gamma \leq \alpha + \beta$$

для каждого натурального числа n , то $\gamma \leq 1$.

Доказательство. Пусть, в противоречие с утверждением, $\gamma = 1 + \delta$, $\delta > 0$. Тогда для $v \geq 2$

$$\gamma^v = (1 + \delta)^v = 1 + v\delta + \frac{1}{2}v(v-1)\delta^2 + \dots > v\delta + \frac{1}{2}v(v-1)\delta^2.$$

Но при достаточно большом v будем иметь

$$v\delta > \beta \text{ и } \frac{1}{2}v(v-1)\delta^2 > \alpha,$$

откуда

$$\gamma^v > \beta + \alpha v.$$

Однако, это противоречит предположению.

Вещественная норма $\varphi(a)$ поля K называется *неархимедовской*, если для всех натуральных кратных единицы $n = 1 + 1 + \dots + 1$ выполняется условие

$$\varphi(n) \leq 1.$$

Так, p -адическая норма в поле рациональных чисел неархимедовская. При этом то, что само поле значений нормы является архимедовским, никакой роли не играет.

Норма φ поля K является неархимедовской тогда и только тогда, когда вместо 4) выполняется более сильное неравенство

$$4') \quad \varphi(a + b) \leq \max(\varphi(a), \varphi(b)).$$

Доказательство. 1. Если 4') выполняется, то для $n = 1 + 1 + \dots + 1$ имеем

$$\varphi(n) \leq \max(\dots, \varphi(1), \dots) = 1.$$

2. Если φ — неархимедовская норма, то для $v = 1, 2, \dots$ имеем

$$\begin{aligned} (\varphi(a + b))^v &= \varphi((a + b)^v) = \varphi(a^v + \binom{v}{1}a^{v-1}b + \dots + b^v) \leq \\ &\leq (\varphi(a))^v + (\varphi(a))^{v-1}\varphi(b) + \dots + (\varphi(b))^v \leq (v + 1)M^v, \end{aligned}$$

где $M = \max(\varphi(a), \varphi(b))$. Но отсюда в силу леммы следует, что

$$\frac{\varphi(a + b)}{M} \leq 1, \text{ откуда } \varphi(a + b) \leq M,$$

т. е. имеет место 4').

В дальнейшем мы будем рассматривать неравенство 4') как определяющий признак неархимедовской нормы и в тех случаях, когда поле значений нормы P не есть поле вещественных чисел. Как заметил Круль¹⁾, тогда можно в качестве области значений нормы взять любую расположенную абелеву группу, так как эти значения

¹⁾ Krull W., Allgemeine Bewertungstheorie, *J. reine u. angew. Math.* 167 (1932), 160—196.

требуется лишь перемножать и сравнивать по величине, но отнюдь не складывать.

Часто целесообразно (и в литературе принято) пользоваться другим способом задания неархимедовских норм. Вместо вещественных значений $\varphi(a)$ рассматривают их *показатели* $w(a) = -\log \varphi(a)$. Определяющие соотношения нормы принимают для показателей следующие вид:

- 1) $w(a)$ для $a \neq 0$ есть вещественное число.
- 2) $w(0)$ есть символ ∞ .
- 3) $w(ab) = w(a) + w(b)$.
- 4) $w(a+b) \geq \min(w(a), w(b))$.

Функция $w(a)$, обладающая перечисленными свойствами, называется *логарифмической нормой*. Переход к показателям становится возможным благодаря тому, что замена неравенства 4) более сильным неравенством 4') делает ненужным сложение значений $\varphi(a)$. Образование логарифмов с обратным знаком обращает расположение и заменяет умножение сложением.

Пример. Пусть элементами поля K служат однозначные аналитические (мероморфные) функции в некоторой области плоскости z или, ещё более обще, на некоторой римановой поверхности. Выделив какую-нибудь точку P римановой поверхности, определим $w(a)$ следующим образом: значение $w(a)$ для функции a равно α , если a имеет в P нуль α -го порядка, равно нулю, если a имеет в P конечное значение, отличное от нуля, и равно $-\alpha$, если a имеет в P полюс α -го порядка. Условия 1)–4) будут тогда выполнены. Таким образом, каждой точке P соответствует своё нормирование поля K . Этот пример позволяет предвидеть значение теории нормирования полей для теории алгебраических функций комплексного переменного. Он объясняет также, почему нормы поля называют иногда «точками» или «местами».

Различают логарифмические нормы двух типов: *дискретные*, характеризуемые существованием наименьшего положительного значения $w(a)$, по отношению к которому все остальные значения $w(a)$ являются тогда кратными (см. предыдущий пример), и *недискретные*, для которых значения $w(a)$ могут быть произвольно близкими к нулю. Так как числа, кратные по отношению к значению $w(a)$, суть снова значения функции w : $nw(a) = w(a^n)$, то в недискретном случае значения $w(a)$ расположены всюду плотно в множестве всех вещественных чисел.

p -адическое нормирование поля рациональных чисел дискретно; точно так же дискретны и все p -адические нормирования.

В логарифмически нормированном поле K элементы a , для которых $w(a) \geq 0$, образуют кольцо $\mathfrak{I}$. Действительно, из $w(a) \geq 0$ и $w(b) \geq 0$ следует $w(a \pm b) \geq \min(w(a), w(b)) \geq 0$ и $w(ab) = w(a) + w(b) \geq 0$. Совокупность p всех элементов a поля K , для которых $w(a) > 0$, является простым идеалом кольца $\mathfrak{I}$. Дей-

ствительно, во-первых, из $w(a) > 0$, $w(b) > 0$ снова вытекает, что $w(a \pm b) \geq \min(w(a), w(b)) > 0$; следовательно, p есть модуль. Во-вторых, если $a \in p$, т. е. $w(a) > 0$, и $w(c) \geq 0$, то $w(ca) = w(c) + w(a) > 0$; следовательно, p есть идеал. В-третьих, из $a' \equiv 0 \pmod{p}$, т. е. из $w(a') = w(a) + w(b) > 0$ следует, что по крайней мере одно из чисел $w(a)$ и $w(b)$ положительно, т. е. что по крайней мере один из элементов a и b делится на p ; следовательно, p — простой идеал.

Элементы из $\mathfrak{Z}$ называются *целыми* (относительно рассматриваемой нормы w), а само кольцо $\mathfrak{Z}$ — *кольцом целых элементов*. Элемент a называется *делящимся* на b (относительно нормы w), если $\frac{a}{b}$ целое, т. е. если $w(a) \geq w(b)$.

Элементы a , для которых $w(a) = 0$, являются делителями единицы кольца $\mathfrak{Z}$. Так как все элементы кольца $\mathfrak{Z}$, не входящие в p , являются делителями единицы, то идеал p свободен от делителей. Тем самым факторкольцо $\mathfrak{Z}/p$ есть поле — *поле классов вычетов* нормы w . Если поле K имеет характеристику p , то и указанное поле классов вычетов, очевидно, также имеет характеристику p . Если же K имеет характеристику нуль, то поле классов вычетов некоторой нормы может иметь либо характеристику нуль (случай равных характеристик), либо простую характеристику (случай неравных характеристик). Типичные примеры на случай неравных характеристик доставляют p -адические нормирования. Пример на случай равных характеристик получаем, беря поле рациональных функций одного переменного и принимая значение логарифмической нормы рациональной функции равным степени знаменателя минус степень числителя. p -адические нормирования, определяемые идеалами кольца полиномов $K[x_1, \dots, x_n]$ (см. выше), также относятся к случаю равных характеристик.

Дальнейшая разработка этих понятий вплоть до полной классификации всех нормирований дана в работах Н. Hasse, F. K. Schmidt'a, O. Teichmüller'a и E. Witt'a¹⁾.

Задача 3. Показать, что в $\mathfrak{Z}$ каждый идеал есть либо множество всех a , для которых $w(a) > \delta$, либо множество всех a , для которых $w(a) \geq \delta$, где δ — неотрицательное вещественное число. При дискретном нормировании можно ограничиться случаем $\geq$, беря при этом в качестве δ лишь числа, фактически содержащиеся среди множества значений $w(a)$. При недискретном нормировании δ однозначно определяется идеалом.

Задача 4. При дискретном нормировании все идеалы кольца $\mathfrak{Z}$ суть степени идеала p ; напротив, при недискретном нормировании все степени идеала p совпадают с p .

¹⁾ Witt E., *J. reine u. angew. Math.* 176 (1936), 126—140, и указанная там литература.

§ 74. Полные расширения.

Для каждого нормированного поля K можно, точно следуя способу, изложенному в § 67, построить нормированное расширение Ω_K , в котором имеет место *теорема сходимости Коши*. С этой целью предварительно строим для поля P — поля значений нормы — соответствующее расположенное поле Ω_P , которое дальше послужит полем значений нормы для Ω_K . Затем определяем в K фундаментальные последовательности $\{a_v\}$, как удовлетворяющие свойству

$$\varphi(a_p - a_q) < \varepsilon \text{ для } p > n(\varepsilon), q > n(\varepsilon),$$

где ε — произвольный положительный элемент из P . Из кольца фундаментальных последовательностей получаем поле классов вычетов Ω_K точно таким же путём, как в § 67 (все доказательства переносятся дословно). Единственное отличие состоит в том, что Ω_K , как и K , будет не расположенным, а только нормированным. Норма в поле Ω_K задаётся следующим образом: если α определяется фундаментальной последовательностью $\{a_v\}$, то в силу доказанного уже неравенства

$$|\varphi(a_v) - \varphi(a_\mu)| \leq \varphi(a_v - a_\mu),$$

и значения $\varphi(a_v)$ образуют в P фундаментальную последовательность, имеющую, следовательно, некоторый предел ω в Ω_P . Тогда полагаем

$$\varphi(\alpha) = \omega.$$

Всем фундаментальным последовательностям с одинаковым пределом α соответствует и одинаковое значение $\varphi(\alpha)$, причём последнее удовлетворяет условиям 1)–4). Ω_K называется *полным расширением поля K относительно нормы φ* .

Для логарифмических нормирований признак сходимости Коши принимает следующий простой вид:

Если поле K — полное относительно логарифмической нормы w , то последовательность $\{a_v\}$ сходится тогда (и только тогда), когда

$$\lim_{v \rightarrow \infty} w(a_{v+1} - a_v) = \infty.$$

Действительно, общий признак сходимости Коши в нашем случае гласит: $\{a_v\}$ сходится тогда и только тогда, когда для каждого фиксированного k выполняется соотношение $\lim_{v \rightarrow \infty} w(a_{v+k} - a_v) = \infty$.

Но так как

$$w(a_{v+k} - a_v) \geq \min(w(a_{v+k} - a_{v+k-1}), \dots, w(a_{v+1} - a_v)),$$

то для сходимости достаточно уже, чтобы $\lim_{v \rightarrow \infty} w(a_{v+1} - a_v) = \infty$.

Этот признак можно высказать также в следующей форме: для сходимости бесконечного ряда $a_1 + a_2 + a_3 + \dots$ необходимо и достаточно, чтобы $\lim_{v \rightarrow \infty} \varphi(a_v) = \infty$.

В дальнейшем мы ограничимся тем случаем, когда значениями нормы служат вещественные числа. Поле P , из которого берутся эти значения, является тогда вещественным числовым полем, а Ω_P есть поле всех вещественных чисел; мы можем заранее принять, что $P = \Omega$.

Приняв в поле Γ рациональных чисел за норму обыкновенную абсолютную величину $\varphi(a) = |a|$, мы в качестве полного расширения получим, конечно, поле вещественных чисел.

p -адическое же нормирование поля Γ даёт в качестве полного расширения гензелевское поле Ω_p p -адических чисел.

Таким образом, поля $\Omega_2, \Omega_3, \Omega_5, \Omega_7, \Omega_{11}, \dots$ оказываются совершенно равноправными с полем вещественных чисел (а для арифметики и столь же важными) полными полями.

Для изображения элементов поля Ω_p , т. е. p -адических чисел, можно указать способ, более удобный, чем задание их произвольными фундаментальными последовательностями. Рассмотрим для $\lambda = 0, 1, 2, 3, \dots$ модули $\mathfrak{M}_\lambda$, образованные рациональными числами, числители которых делятся на p^λ , знаменатели же не делятся на p , так что для этих чисел $\varphi(a) \leq p^{-\lambda}$. Будем называть два рациональных числа сравнимыми по модулю p^λ , если их разность содержится в $\mathfrak{M}_\lambda$. Если теперь $\{r_\mu\}$ — p -адическая фундаментальная последовательность рациональных чисел, то для каждого λ имеем, начиная с некоторого $n = n(\lambda)$:

$$\varphi(r_\mu - r_\nu) \leq p^{-\lambda} \text{ для } \mu > n(\lambda), \nu > n(\lambda),$$

т. е.

$$r_\mu \equiv r_\nu \pmod{p^\lambda}.$$

Таким образом, все числа r_μ с $\mu > n(\lambda)$ принадлежат одному и тому же классу вычетов $\mathfrak{R}_\lambda$ по модулю $\mathfrak{M}_\lambda$. Поэтому фундаментальная последовательность $\{r_\mu\}$ определяет некоторую последовательность классов вычетов

$$\mathfrak{R}_0 \supset \mathfrak{R}_1 \supset \mathfrak{R}_2 \supset \mathfrak{R}_3 \supset \mathfrak{R}_4 \supset \dots,$$

вложенных друг в друга указанным образом. И обратно, каждая последовательность $\{r_1, r_2, \dots\}$, определяющая указанным образом некоторую последовательность $\{\mathfrak{R}_\lambda\}$ вложенных друг в друга классов вычетов $\mathfrak{R}_\lambda$ по модулям $\mathfrak{M}_\lambda$, такую, что

$$r_\mu \in \mathfrak{R}_\lambda \text{ для всех } \mu > n(\lambda),$$

необходимо является фундаментальной последовательностью.

В частности, если $\{r_\mu\}$ — нулевая последовательность, то $\mathfrak{R}_\lambda$ будут нулевыми классами, $\mathfrak{R}_\lambda = \mathfrak{M}_\lambda$. При сложении двух фундамен-

тальных последовательностей: $\{r_\mu\} + \{s_\mu\} = \{r_\mu + s_\mu\}$, будут складываться также соответствующие последовательности классов вычетов: $\{\mathfrak{R}_\lambda + \mathfrak{S}_\lambda\}$. В частности, при сложении фундаментальной последовательности с нулевой последовательностью соответствующая последовательность классов вычетов останется неизменной. Обратно, если двум последовательностям $\{r_\mu\}$ и $\{s_\mu\}$ соответствует одна и та же последовательность классов вычетов $\{\mathfrak{R}_\lambda\}$, то их разность является нулевой последовательностью. Таким образом, *каждому p -адическому числу $\alpha = \lim r_\mu$, взаимно однозначно соответствует некоторая последовательность классов вычетов $\{\mathfrak{R}_\lambda\}$ указанного вида.*

Это представление p -адических чисел последовательностями классов вычетов и есть то удобное изображение этих чисел, которое мы выше имели в виду. Чтобы от изображения p -адического числа α с помощью последовательности классов вычетов вернуться к заданию его (индивидуальной) фундаментальной последовательностью, достаточно выбрать из каждого класса вычетов $\mathfrak{R}_\lambda$ по одному r'_λ : тогда $\alpha = \lim r'_\lambda$. Можно представить α также в виде бесконечной суммы, положив

$$r'_1 = s_0, \quad r'_{\lambda+1} - r'_\lambda = s_\lambda p^\lambda,$$

так что

$$r'_{\lambda+1} = s_0 + s_1 p + s_2 p^2 + \dots + s_\lambda p^\lambda,$$

и, следовательно,

$$(1) \quad \alpha = \lim_{\lambda \rightarrow \infty} \sum_{v=0}^{\lambda} s_v p^v = \sum_{v=0}^{\infty} s_v p^v.$$

Здесь $s_1, s_2, \dots$ — рациональные числа, знаменатели которых не делятся на p .

p -адические пределы обыкновенных целых чисел называются *целыми p -адическими числами*. Для классов вычетов $\mathfrak{R}_0, \mathfrak{R}_1, \dots$ это означает, что в каждом из них должно содержаться целое число. В частности, в случае целого p -адического числа $\mathfrak{R}_0$ есть нулевой класс вычетов $\mathfrak{M}_0$ — совокупность всех рациональных чисел с знаменателями, не делящимися на p . Но это условие и достаточно для того, чтобы p -адическое число было целым: если $\mathfrak{R}_0$ — нулевой класс вычетов по модулю $\mathfrak{M}_0$, то все классы вычетов $\mathfrak{R}_1, \mathfrak{R}_2, \dots$ содержат целые числа. Действительно, $\mathfrak{R}_\lambda$ содержится в $\mathfrak{R}_0$ и потому состоит лишь из чисел $\frac{r}{s}$ с $s \not\equiv 0 \pmod{p}$. Если теперь x — решение сравнения

$$sx \equiv r \pmod{p^\lambda},$$

то

$$x - \frac{r}{s} = \frac{sx - r}{s} \equiv 0 \pmod{\mathfrak{M}_\lambda},$$

и значит, x принадлежит к классу вычетов $\mathfrak{R}_\lambda$.

В соответствии с этим, если α — целое p -адическое число, то в его представлении в виде ряда (1) можно взять все r'_λ , а значит, и все s_λ , обыкновенными целыми числами. Таким образом, (1) есть степенной ряд относительно p с целочисленными коэффициентами. Каждый такой степенной ряд сходится в смысле p -адической нормы и представляет собою целое p -адическое число.

Каждое p -адическое число $\alpha = \{\mathfrak{N}_0, \mathfrak{N}_1, \dots\}$, будучи умножено на некоторую степень числа p , даёт целое p -адическое число. Действительно, пусть r'_0 — какой-нибудь элемент из класса вычетов $\mathfrak{N}_0$. Умножением r'_0 на надлежащую степень p^m числа p можно добиться того, чтобы знаменатель произведения $p^m r'_0$ уже не содержал более множителем p и, значит, $p^m r'_0$ принадлежало к нулевому классу вычетов по модулю $\mathfrak{M}_0$. Тогда $p^m \alpha$ будет целым p -адическим числом. Развёртывая его в степенной ряд (1) с целочисленными $s_0, s_1, \dots$, мы получим для α представление с конечным числом отрицательных показателей:

$$(2) \quad \alpha = a_{-m} p^{-m} + a_{-m+1} p^{-m+1} + \dots + a_0 + a_1 p + a_2 p^2 + \dots$$

Представление (1) целого p -адического числа α можно нормировать, беря всюду в качестве r'_λ наименьшее неотрицательное целое число из класса вычетов $\mathfrak{N}_\lambda$. Тогда все числа s_λ удовлетворяют условию $0 \leq s_\lambda < p$. Переходя снова от (1) к (2), получим для каждого p -адического числа однозначно определённое разложение (2) с $0 \leq a_\lambda < p$.

Из представления p -адических чисел в виде (2) непосредственно следует, что кольцо целых элементов относительно p -адической нормы в $\mathfrak{O}_p$ совпадает с кольцом всех целых p -адических чисел, так что введённое в § 73 понятие «целого» элемента находится в согласии с названием «целое p -адическое число».

Исходя из p -адического нормирования поля отношений K области целостности $\mathfrak{o}$, определяемого описанным в § 73 способом простым идеалом $\mathfrak{p}$ области $\mathfrak{o}$, мы таким же образом получим полное p -адическое поле $\mathfrak{O}_p$, обобщение гензелевских p -адических полей. Если, например, $\mathfrak{p}$ — идеал $(x - c)$ в области полиномов $\Delta[x]$, то $\mathfrak{O}_p$ будет кольцом всех степенных рядов

$$(3) \quad \alpha = a_{-m} (x - c)^{-m} + \dots + a_0 + a_1 (x - c) + a_2 (x - c)^2 + \dots$$

с постоянными a_λ из Δ (доказательство проводится как выше). Эт степенные ряды сходятся в смысле p -адической нормы всегда, как бы ни были выбраны коэффициенты a_λ . Выражения (3) называют *формальными степенными рядами относительно $(x - c)$* .

Задача 1. Записать -1 и $\frac{1}{2}$ в виде 3-адически нормированных степенных рядов.

Задача 2. Уравнение $f(\xi) = 0$, где f — целочисленный полином, разрешимо в поле $\mathbb{Q}_p$ тогда и только тогда, когда сравнение

$$f(\xi) \equiv 0 \pmod{p^n}$$

обладает рациональным решением ξ для каждого натурального n .

Задача 3. Разрешимы ли уравнения

$$x^2 = -1, \quad x^2 = 3, \quad x^2 = 7$$

в поле $\mathbb{Q}_3$?

Задача 4. Пусть p — идеал $(x_1, x_2, \dots, x_n)$ в области полиномов $\Delta[x_1, x_2, \dots, x_n]$. Показать, что сравнение

$$fg \equiv 1 \pmod{p}$$

обладает решением при каждом заданном $f \not\equiv 0 \pmod{p}$. С помощью этого показать, что p -адическое поле $\mathbb{Q}_p$ состоит из всех отношений формальных степенных рядов

$$h_0 + h_1 + h_2 + \dots,$$

где h_k — однородная форма степени k относительно $x_1, \dots, x_n$.

Две различные нормы φ и ψ , определённые в поле K , могут приводить к одному и тому же полному расширению $\mathbb{Q}$. Очевидно, это имеет место тогда и только тогда, когда каждая последовательность $\{a_n\}$ элементов из K , нулевая относительно φ , является нулевой также относительно ψ , и наоборот. В этом случае, т. е. когда $\lim_{n \rightarrow \infty} \varphi(a_n) = 0$ и $\lim_{n \rightarrow \infty} \psi(a_n) = 0$ означают одно и то же, мы

будем называть нормы φ и ψ *эквивалентными*.

Можно образовать бесконечное множество норм в поле комплексных чисел, эквивалентных обыкновенной абсолютной величине $\varphi(a) = |a|$, полагая, например, $\varphi(a) = |a|^p$, где p — фиксированное положительное вещественное число, не превосходящее 1. Действительно, выполнение условий 1) — 3) очевидно. Неравенство же 4) вытекает из $|a+b| \leq |a|+|b|$ в силу неравенства $\varepsilon^p + \delta^p \geq (\varepsilon + \delta)^p$, справедливого для произвольных вещественных чисел $\varepsilon \geq 0, \delta \geq 0$ и $0 < p \leq 1$).

p -адической норме $\varphi_p(a)$ в поле рациональных чисел эквивалентна каждая норма $\psi(a) = (\varphi_p(a))^\sigma$, где σ — произвольное фиксированное положительное число.

Если φ и ψ — две эквивалентные нормы в поле K , то ψ есть некоторая степень φ , т. е. существует фиксированное положительное число σ такое, что $\psi(a) = (\varphi(a))^\sigma$ для всех a из K .

1) Действительно, предположив, например, что $\varepsilon \leq \delta$, будем иметь $\left(\frac{\varepsilon}{\delta}\right)^p \geq \frac{\varepsilon}{\delta}$ и, следовательно, $\log(\varepsilon + \delta)^p = p \log \delta + p \log\left(\frac{\varepsilon}{\delta} + 1\right) \leq p \log \delta + p \log\left(\frac{\varepsilon^p}{\delta^p} + 1\right) = \log(\varepsilon^p + \delta^p)$, ибо $0 < p \leq 1$. Ред.

Доказательство. Если $\varphi(a) < \varphi(b)$, то также $\psi(a) < \psi(b)$, и обратно. Действительно, из $\varphi(a) < \varphi(b)$ следует $\varphi\left(\frac{a}{b}\right) < 1$, и следовательно, $\left(\frac{a}{b}\right)^n$ при $n \rightarrow \infty$ стремится к нулю в смысле нормы φ . Тогда $\left(\frac{a}{b}\right)^n$ стремится к нулю и в смысле нормы ψ . Но это означает, что $\psi\left(\frac{a}{b}\right) < 1$, т. е. $\psi(a) < \psi(b)$. Пусть теперь p — произвольный фиксированный элемент из K с $\varphi(p) > 1$. Тогда, вследствие доказанного, также $\psi(p) > 1$. Пусть a — произвольный элемент из K и $\varphi(a) = (\varphi(p))^\delta$, $\psi(a) = (\psi(p))^{\delta'}$. Покажем, что $\delta = \delta'$. Беря натуральные числа n и m такие, что $\frac{n}{m} \leq \delta$, имеем

$$(\varphi(p))^{\frac{n}{m}} \leq (\varphi(p))^\delta = \varphi(a), \text{ следовательно, } \varphi(p^n) \leq \varphi(a^m).$$

Но отсюда вытекает, что

$$\psi(p^n) \leq \psi(a^m), \quad (\psi(p))^{\frac{n}{m}} \leq \psi(a) = (\psi(p))^{\delta'}, \quad \frac{n}{m} \leq \delta'.$$

Так как верхней гранью всех дробей $\frac{n}{m} \leq \delta$ является само δ , то заключаем, что $\delta \leq \delta'$, и на том же основании $\delta' \leq \delta$, следовательно, $\delta = \delta'$. Обозначая теперь через ε не зависящее от a положительное число $\frac{\log \psi(p)}{\log \varphi(p)}$, в силу доказанного равенства $\delta = \delta'$ имеем для всех a :

$$\log \psi(a) = \delta' \log \psi(p) = \delta \log \psi(p) = \delta \varepsilon \log \varphi(p) = \varepsilon \log \varphi(a),$$

и, следовательно,

$$\psi(a) = (\varphi(a))^\varepsilon.$$

Если K — поле с нормой φ , K' — изоморфное с K поле с нормой ψ , то изоморфизм этих полей называется *непрерывным в обе стороны* или *топологическим*, если φ -нулевая последовательность из K всегда соответствует ψ -нулевая последовательность из K' , и обратно. Поля K и K' называются в этом случае *непрерывно изоморфными*. При топологическом изоморфизме сходящиеся последовательности соответствуют сходящимся и фундаментальным — фундаментальным. Отсюда непосредственно следует:

Непрерывно изоморфные нормированные поля K и K' имеют и непрерывно изоморфные полные расширения Ω_K и $\Omega_{K'}$.

Задача 5. Показать, что среди известных нам нормирований поля рациональных чисел, а именно, нормирования абсолютными величинами и p -адических нормирований, нет двух эквивалентных.

§ 75. Нормирования поля рациональных чисел. Архимедовские нормирования числовых полей.

Следующая теорема Островского показывает, что известные нам нормирования поля рациональных чисел, а именно, p -адические и по абсолютной величине, являются, с точностью до эквивалентности, единственно возможными. При этом полем значений нормы снова считается поле вещественных чисел.

Нетривиальная норма φ в поле Γ рациональных чисел есть либо $\varphi(a) = |a|^p$ с $0 < p \leq 1$, т. е. эквивалентна обыкновенному нормированию абсолютными величинами, либо $\varphi(a) = (\varphi_p(a))^c$ с фиксированным простым числом p и фиксированным положительным числом c , т. е. эквивалентна некоторой p -адической норме.

Доказательство. Для каждого целого рационального n имеем

$$\varphi(n) \leq |n|.$$

Действительно,

$$\begin{aligned} \varphi(n) &= \varphi(|n|) = \varphi(1 + 1 + \dots + 1) \leq \\ &\leq \varphi(1) + \varphi(1) + \dots + \varphi(1) = |n|. \end{aligned}$$

Пусть $a > 1$ и $b > 1$ — два произвольных целых рациональных числа. Развернём b^n по степеням a :

$$\begin{aligned} b^n &= c_0 + c_1 a + \dots + c_n a^n, \\ 0 &\leq c_v < a, \quad c_n \neq 0. \end{aligned}$$

Наивысшая входящая сюда степень a^n числа a не превосходит b^n

$$a^n \leq b^n,$$

т. е.

$$n \leq \nu \frac{\log b}{\log a}.$$

Так как теперь

$$\begin{aligned} \varphi(b^n) &\leq \varphi(c_0) + \varphi(c_1) \varphi(a) + \dots + \varphi(c_n) (\varphi(a))^n < \\ &< a(1 + \varphi(a) + \dots + (\varphi(a))^n) \leq a(n+1)M^n, \end{aligned}$$

где $M = \max(1, \varphi(a))$, то

$$(\varphi(b))^n < a \left(\frac{\log b}{\log a} \nu + 1 \right) M^{\frac{\log b}{\log a} \nu}$$

или

$$\left(\frac{\varphi(b)}{M^{\frac{\log b}{\log a}}} \right)^n < a \frac{\log b}{\log a} \nu + a.$$

В силу леммы § 73 отсюда следует, что

$$\varphi(b) \leq M^{\frac{\log b}{\log a}},$$

т. е.

$$\varphi(b) \leq \max \left(1, (\varphi(a))^{\frac{\log b}{\log a}} \right).$$

Первый случай. φ — архимедовская. Тогда существует целое число b такое, что $\varphi(b) > 1$. Если бы для какого-либо другого целого числа $a > 1$ мы имели бы $\varphi(a) \leq 1$, то из только что установленного неравенства вытекало бы $\varphi(b) \leq 1$, что неверно. Следовательно, $\varphi(a) > 1$ для всех целых $a > 1$. Тем самым наше неравенство принимает в рассматриваемом случае вид

$$\varphi(b) \leq (\varphi(a))^{\frac{\log b}{\log a}}$$

или

$$(\varphi(b))^{\frac{1}{\log b}} \leq (\varphi(a))^{\frac{1}{\log a}}.$$

Но так как a и b можно поменять ролями, то имеем также

$$(\varphi(a))^{\frac{1}{\log a}} \leq (\varphi(b))^{\frac{1}{\log b}}$$

и, следовательно,

$$(\varphi(a))^{\frac{1}{\log a}} = (\varphi(b))^{\frac{1}{\log b}}.$$

Отсюда вытекает, что если $\varphi(b) = b^p$, то и $\varphi(a) = a^p$, и, таким образом,

$$\varphi(r) = |r|^p$$

для каждого рационального числа r . При этом $p > 0$, так как $\varphi(a) > 1$, и $p \leq 1$, так как

$$2^p = \varphi(2) = \varphi(1+1) \leq \varphi(1) + \varphi(1) = 2.$$

Второй случай. φ — неархимедовская; таким образом $\varphi(a) \leq 1$ для всех целых чисел a . Совокупность всех целых чисел a , для которых $\varphi(a) < 1$, является простым идеалом в кольце целых чисел. Это устанавливается совершенно так же, как в § 73: из $\varphi(a) < 1$ и $\varphi(b) < 1$ следует $\varphi(a+b) \leq \max(\varphi(a), \varphi(b)) < 1$, и потому множество всех целых чисел a , для которых $\varphi(a) < 1$, есть идеал; этот идеал — простой, так как из $\varphi(ab) = \varphi(a)\varphi(b) < 1$ следует, что либо $\varphi(a) < 1$, либо $\varphi(b) < 1$ (либо и то, и другое). Но в кольце целых чисел каждый идеал — главный, в частности, каждый, простой идеал порождается некоторым простым числом. Таким образом, целые числа a с $\varphi(a) < 1$ суть кратные некоторого простого числа p . Но каждое рациональное число r может быть записано в виде $r = \frac{z}{n} p^p$ с целыми

z и n , не делящимися на p . Так как $\varphi(z) = \varphi(n) = 1$, то получаем, что $\varphi(r) = (\varphi(p))^p = p^{-p\sigma} = (\varphi_p(r))^\sigma$, где $\sigma = -\frac{\log \varphi(p)}{\log p}$ — фиксированное число, положительное вследствие неравенства $\varphi(p) < 1$.

Для более глубоких исследований по теории нормированных полей интерес представляют лишь неархимедовские нормы. Действительно, имеет место, также доказанная Островским, теорема: *архимедовски нормированное поле K непрерывно изоморфно некоторому подполю поля комплексных чисел, нормированному обыкновенными абсолютными величинами*. За доказательством отошлём читателя к оригинальному мемуару Островского¹⁾.

Здесь мы рассмотрим лишь важнейшие частные случаи и прежде всего случай самого поля комплексных чисел.

Поле $\Omega = \mathbb{C}$ комплексных чисел допускает только одно нормирование Φ , совпадающее для поля вещественных чисел $\mathbb{R}$ с нормированием абсолютными величинами $\varphi(a) = |a|^p$, а именно $\Phi(a) = |a|^p$.

Доказательство. Допустим, что существует комплексное число ξ , для которого $\Phi(\xi) \neq |\xi|^p$. Смотря по тому, будет ли $\Phi(\xi) > |\xi|^p$ или $\Phi(\xi) < |\xi|^p$, положим $\eta = \frac{\xi}{|\xi|}$ или $\eta = \frac{|\xi|}{\xi}$. Тогда $|\eta| = 1$ и $\Phi(\eta) > 1$. Полагая

$$\eta^v = a_v + i b_v,$$

будем иметь

$$a_v^2 + b_v^2 = |\eta^v|^2 = |\eta|^{2v} = 1,$$

$$|a_v| \leq 1, \quad |b_v| \leq 1,$$

$$\Phi(a_v) = |a_v|^p \leq 1, \quad \Phi(b_v) = |b_v|^p \leq 1,$$

$$(\Phi(\eta))^v = \Phi(\eta^v) \leq \Phi(a_v) + \Phi(b_v) \leq 1 + \Phi(i)$$

для всех v . Но это несовместимо с неравенством $\Phi(\eta) > 1$.

Теперь мы можем найти все архимедовские нормирования алгебраического числового поля.

Все архимедовские нормирования алгебраического числового поля Σ могут быть получены путём вложения поля Σ всевозможными способами в поле вещественных или в поле комплексных чисел, полагая каждый раз $\varphi(a) = |a|^p$, $0 < p \leq 1$.

Доказательство. Пусть поле Σ порождается присоединением к полю рациональных чисел Γ корня ϑ полинома $f(x)$.

Элементы содержащегося в $\Gamma(\vartheta)$ простого поля Γ могут быть нормированы, в силу первой теоремы этого параграфа, лишь функцией $\varphi(a) = |a|^p$. Полное расширение Ω поля $\Gamma(\vartheta)$ содержит полное расширение поля Γ , т. е. поле вещественных чисел $\mathbb{R}$. Согласно

¹⁾ Ostrowski A., Über einige Lösungen der Funktionalgleichung $\varphi(x) \varphi(y) = \varphi(xy)$. *Acta Math.* 41 (1918), 271–284.

основной теореме алгебры, в $P[x]$ полином $\bar{f}(x)$ разлагается на r_1 линейных и r_2 квадратных множителей:

$$f(x) = (x - \vartheta_1) \dots (x - \vartheta_{r_1}) q_1(x) \dots q_{r_2}(x),$$

$$q_v(x) = (x - a_v)^2 + b_v^2.$$

Так как ϑ есть корень полинома $f(x)$, то один из множителей этого полинома должен иметь корень ϑ . Если это — один из линейных множителей, то $\vartheta = \vartheta_\mu$ ($\mu \leq r_1$), и $\Gamma(\vartheta)$ оказывается вложенным в поле вещественных чисел с нормой $\varphi(a) = |a|^p$. Если же ϑ есть корень квадратного множителя $q_v(x)$, то присоединение ϑ равносильно присоединению $i = \sqrt{-1}$, и $\Gamma(\vartheta) = \Sigma$ оказывается вложенным в поле комплексных чисел с нормой $\varphi(a) = |a|^p$, так как, по предыдущему, это — единственная норма в поле $P(i)$, являющаяся продолжением нормы $|a|^p$ в поле P .

Если ϑ — корень квадратного полинома $q_v(x)$, то ϑ может быть вложено в $P(i)$ двояким способом, а именно, либо равенством $\vartheta = a_v + ib_v$, либо равенством $\vartheta = a_v - ib_v$. Однако, оба эти вложения приводят к одной и той же норме, поскольку комплексно сопряжённые элементы равны по абсолютной величине. Таким образом, каждый линейный или квадратный множитель полинома $f(x)$ приводит к одному и, с точностью до эквивалентности, только одному нормированию поля $\Gamma(\vartheta)$. И обратно, каждое нормирование поля $\Gamma(\vartheta)$ однозначно определяет некоторое полное расширение Ω , в котором элемент ϑ может обратиться в нуль лишь один из множителей $x - \vartheta_\mu$ или $q_v(x)$. Поэтому число существенно различных архимедовских нормирований поля $\Gamma(\vartheta)$ равно числу $r_1 + r_2$ множителей полинома $f(x)$, где r_1 — число вещественных корней, а r_2 — число пар комплексно сопряжённых корней этого полинома.

Нормирования поля $\Gamma(\vartheta)$ абсолютными величинами весьма тесно связаны с «делителями единицы» этого поля¹⁾.

§ 76. Нормирование алгебраических расширений.

Исследуем, когда и сколькими способами заданная неархимедовская норма поля K может быть продолжена до нормы алгебраического расширения Δ этого поля K . При этом в соответствии с § 73 мы перейдём к логарифмической норме $w(a) = -\log \varphi(a)$ и обозначим через $\mathfrak{p}$ идеал, образованный элементами a , для которых $w(a) > 0$, в кольце целых элементов, т. е. в кольце элементов a , для которых $w(a) \geq 0$.

¹⁾ См. по этому поводу В. L. van der Waerden, Ein logarithmenfreier Beweis des Dirichletschen Einheitensatzes. *Abh. Math. Sem. Hamburg*, 6 (1928), 259—262.

Это исследование будет опираться на признак приводимости в полных полях, идущий от Гензеля. Если a_v — коэффициент полинома

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

в логарифмически нормированном поле, имеющий наименьшую норму, то

$$\frac{a_n}{a_v} x^n + \frac{a_{n-1}}{a_v} x^{n-1} + \dots + \frac{a_0}{a_v}$$

есть полином с целыми коэффициентами, по крайней мере один из которых не делится на p . Полином, обладающий этим свойством, называется *примитивным*.

Признак приводимости. Пусть поле K — полное относительно логарифмической нормы w и $f(x)$ — примитивный полином с целыми коэффициентами из K . Если $g_0(x)$ и $h_0(x)$ — два полинома с целыми коэффициентами из K , удовлетворяющие сравнению

$$f(x) \equiv g_0(x) h_0(x) \pmod{p}$$

и взаимно простые по модулю p , то существуют два таких полинома $g(x)$, $h(x)$ с целыми коэффициентами из K , что

$$\begin{aligned} f(x) &= g(x) h(x), \\ g(x) &\equiv g_0(x) \pmod{p}, \\ h(x) &\equiv h_0(x) \pmod{p}. \end{aligned}$$

При этом $g(x)$ и $h(x)$ можно определить так, чтобы степень полинома $g(x)$ была равна степени $g_0(x)$ по модулю p .

Доказательство. Так как в $g_0(x)$ и $h_0(x)$ коэффициенты, делящиеся на p , можно просто опустить, не нарушая этим предположения и утверждения теоремы, то можно принять, что старшие коэффициенты в $g_0(x)$ и $h_0(x)$ не делятся на p , причём $g_0(x)$ есть полином степени r . Так как, опять-таки, ничто не нарушится, если мы заменим $g_0(x)$ на $\frac{1}{a} g_0(x)$ и $h_0(x)$ на $ah_0(x)$, то мы можем заранее принять, что $g_0(x) = x^r + \dots$, т. е. $g_0(x)$ есть «нормированный» полином степени r . Если тогда b — старший коэффициент произведения $g_0(x) h_0(x)$ равен b , и степень этого произведения $r + s \leq n$, где n — степень полинома $f(x)$. Мы определим теперь множители $g(x)$ и $h(x)$ так, что $g(x)$ будет «нормированным» полиномом степени r и, следовательно, $h(x)$ — полиномом степени $n - r$.

Все коэффициенты полинома $\hat{f}(x) = g_0(x) h_0(x)$, по предположению, имеют положительные значения нормы; пусть $\delta_1 > 0$ — наименьшее из этих значений. Если $\delta_1 = \infty$, то $f(x) = g_0(x) h_0(x)$, так что нечего доказывать,

Так как $g_0(x)$ и $h_0(x)$ взаимно просты по модулю p , то существуют два полинома $l(x)$ и $m(x)$ с целыми коэффициентами из K , такие, что

$$l(x)g_0(x) + m(x)h_0(x) \equiv 1 \pmod{p}.$$

Пусть $\delta_2 > 0$ — наименьшее из значений нормы для коэффициентов полинома

$$l(x)g_0(x) + m(x)h_0(x) - 1,$$

ε — меньшее из чисел δ_1^p , δ_2 , и, наконец, π — элемент, для которого $w(\pi) = \varepsilon$. Тогда, следовательно,

$$(1) \quad f(x) \equiv g_0(x)h_0(x) \pmod{\pi},$$

$$(2) \quad l(x)g_0(x) + m(x)h_0(x) \equiv 1 \pmod{\pi}.$$

Мы построим теперь $g(x)$ как предел начинающейся с $g_0(x)$ последовательности полиномов $g_v(x)$ степени r и точно так же $h(x)$ — как предел начинающейся с $h_0(x)$ последовательности полиномов $h_v(x)$ степени $\leq n - r$. Пусть $g_v(x)$ и $h_v(x)$ уже определены так, что

$$(3) \quad f(x) \equiv g_v(x)h_v(x) \pmod{\pi^{v+1}},$$

$$(4) \quad g_v(x) \equiv g_0(x) \pmod{\pi},$$

$$(5) \quad h_v(x) \equiv h_0(x) \pmod{\pi}$$

и что, кроме того, $g_v(x)$ имеет старшим коэффициентом 1, $g_v(x) = x^r + \dots$. Для определения полиномов $g_{v+1}(x)$ и $h_{v+1}(x)$ положим

$$(6) \quad g_{v+1}(x) = g_v(x) + \pi^{v+1}u(x),$$

$$(7) \quad h_{v+1}(x) = h_v(x) + \pi^{v+1}v(x),$$

где $u(x)$ и $v(x)$ должны быть ниже определены. Тогда

$$g_{v+1}(x)h_{v+1}(x) - f(x) = g_v(x)h_v(x) - f(x) + \pi^{v+1}[g_v(x)v(x) + h_v(x)u(x)] + \pi^{2v+2}u(x)v(x).$$

Полагая, в соответствии с (3),

$$f(x) - g_v(x)h_v(x) = \pi^{v+1}p(x),$$

получим:

$$\begin{aligned} g_{v+1}(x)h_{v+1}(x) - f(x) &\equiv \\ &\equiv \pi^{v+1}[g_v(x)v(x) + h_v(x)u(x) - p(x)] \pmod{\pi^{v+2}}. \end{aligned}$$

Для того чтобы левая часть делилась на π^{v+2} , достаточно, чтобы выполнялось сравнение

$$(8) \quad g_v(x)v(x) + h_v(x)u(x) \equiv p(x) \pmod{\pi}.$$

Чтобы достичь этого, умножим сравнение (2) на $p(x)$:

$$(9) \quad p(x)l(x)g_0(x) + p(x)m(x)h_0(x) \equiv p(x) \pmod{\pi},$$

разделим $p(x) m(x)$ на $g_0(x)$, так что остаток $u(x)$ будет иметь степень $< r$:

$$(10) \quad p(x) m(x) = q(x) g_0(x) + u(x),$$

подставим (10) в (9):

$$[p(x) l(x) + q(x) h_0(x)] g_0(x) + u(x) h_0(x) \equiv p(x) \pmod{\pi},$$

заменяем все делящиеся на π коэффициенты полинома, стоящего в прямых скобках, нулями, и получим в результате:

$$(11) \quad v(x) g_0(x) + u(x) h_0(x) \equiv p(x) \pmod{\pi}.$$

Из (11), в силу (4) и (5), и будет следовать требуемое сравнение (8). Далее, так как $u(x)$ имеет степень $< r$, то $g_{v+1}(x)$, в силу (6), имеет ту же степень и тот же старший коэффициент, что и $g_v(x)$. Остаётся ещё показать, что $v(x)$ имеет степень $\leq n - r$. Если бы это было не так, то в первом члене формулы (11), и только в нём, старший член имел бы степень $> n$. Коэффициент этого члена должен был бы, в силу (11), делиться на π , и следовательно, старший коэффициент в $v(x)$ делился бы на π . Однако, мы удалили из $v(x)$ все коэффициенты, делящиеся на π . Следовательно, $v(x)$ имеет степень $\leq n - r$.

Из сравнения (8), как мы выше видели, следует, что

$$(12) \quad f(x) \equiv g_{v+1}(x) h_{v+1}(x) \pmod{\pi^{v+2}}.$$

Построенные таким образом последовательности $\{g_v(x)\}$ и $\{h_v(x)\}$ сходятся, в силу (3), (6), (7), к полиномам $g(x) = x^r + \dots$ и $h(x)$ с

$$f(x) = g(x) h(x).$$

Наконец, в силу (4) и (5),

$$g(x) \equiv g_0(x) \pmod{p},$$

$$h(x) \equiv h_0(x) \pmod{p}.$$

Из доказанного признака приводимости, как простое следствие, вытекает:

Если

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

— неприводимый полином над K , то

$$\min(w(a_0), w(a_1), \dots, w(a_n)) = \min(w(a_0), w(a_n)).$$

При доказательстве мы можем предположить, что $f(x)$ примитивен. Тогда $\min(w(a_0), \dots, w(a_n)) = 0$. Если бы $w(a_0)$ и $w(a_n)$ были оба больше нуля, то существовало бы r , $0 < r < n$, такое, что $w(a_r) = 0$ и $w(a_v) > 0$ для $v = r + 1, \dots, n$. Мы имели бы тогда

$$f(x) \equiv (a_0 + a_1 x + \dots + a_r x^r) \cdot 1 \pmod{p} \quad (0 < r < n),$$

и, следовательно, $f(x)$, согласно признаку приводимости, разлагался бы в произведение множителя степени r и множителя степени $n-r$.

Задача 1. Полином $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ с целыми коэффициентами из K , неприводимый по модулю p , неприводим также в полном поле $\mathbb{Q}_K$.

Задача 2. Если у $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ все коэффициенты $a_{n-1}, \dots, a_0$ делятся на p , и a_0 не есть произведение двух элементов из p , то $f(x)$ неприводим (обобщение признака неприводимости Эйзенштейна).

Задача 3. Исследовать разложение неприводимых над полем рациональных чисел полиномов

$$x^2 + 1, x^2 + 2, x^2 - 3, x^2 + x + 1, x^3 + 2$$

в поле 3-адических чисел.

Наиболее важным применением последней теоремы является доказательство продолжаемости полных логарифмических норм на алгебраические расширения.

Пусть поле K — полное относительно логарифмической нормы w , и Δ — алгебраическое расширение поля K . Тогда в Δ существует логарифмическая норма W , совпадающая в K с w .

Доказательство. Пусть ξ — элемент из Δ , и

$$\xi^n + a_{n-1}\xi^{n-1} + \dots + a_0 = 0$$

— неприводимое уравнение для ξ с коэффициентами из K . Мы утверждаем, что

$$W(\xi) = \frac{1}{n} w(a_0)$$

есть норма в поле Δ (очевидно, совпадающая на K с w). Чтобы доказать для двух элементов ξ, η поля Δ соотношения

$$W(\xi\eta) = W(\xi) + W(\eta),$$

$$W(\xi + \eta) \geq \min(W(\xi), W(\eta)),$$

рассмотрим подполе $\Delta_0 = K(\xi, \eta)$; оно имеет относительно K конечную степень t . Согласно § 41, функция $W(\xi)$ может быть записана также в следующем виде:

$$W(\xi) = \frac{1}{t} w(N_{\Delta_0/K}(\xi)).$$

Вследствие равенства $N(\xi\eta) = N(\xi)N(\eta)$ отсюда сразу вытекает, что

$$W(\xi\eta) = W(\xi) + W(\eta).$$

Так как

$$W(\xi + \eta) = W(\eta) + W\left(1 + \frac{\xi}{\eta}\right)$$

и

$$\min (W(\xi), W(\eta)) = W(\eta) + \min \left(W\left(\frac{\xi}{\eta}\right), 0 \right),$$

то при доказательстве неравенства $W(\xi + \eta) \geq \min (W(\xi), W(\eta))$ мы можем ограничиться случаем $\eta = 1$.

Но неприводимым уравнением для $\xi + 1$ служит

$$(\xi + 1)^n + \dots + (a_0 - a_1 + a_2 - \dots + (-1)^{n-1} a_{n-1} + (-1)^n) = 0,$$

и в силу предыдущей теоремы действительно

$$\begin{aligned} W(\xi + 1) &= \frac{1}{n} \cdot w(a_0 - a_1 + \dots) \geq \\ &\geq \frac{1}{n} \min (w(a_0), w(a_1), \dots, w(a_{n-1}), w(1)) = \\ &= \frac{1}{n} \min (w(a_0), w(1)) = \min (W(\xi), 0). \end{aligned}$$

Если мы перейдем от логарифмических норм $w(a)$, $W(\xi)$ снова к обыкновенным нормам

$$\varphi(a) = e^{-w(a)}, \quad \Phi(\xi) = e^{-W(\xi)},$$

то нормирование расширения Λ будет определяться формулой

$$\Phi(\xi) = \sqrt[n]{\varphi(a_0)}$$

или, в случае, когда Λ имеет конечную степень t относительно K , — формулой

$$\Phi(\xi) = \sqrt[t]{\varphi(N_\Lambda(\xi))}.$$

Заметим, что совершенно такая же формула верна и в случае архимедовских нормирований, если K — поле вещественных чисел, Λ — поле комплексных чисел и $\Phi(\xi) = |\xi|^p$. Действительно, в этом случае для $\xi = a + bi$ имеем

$$|\xi| = \sqrt{a^2 + b^2} = \sqrt{N(\xi)} = \sqrt{|N(\xi)|}.$$

Поэтому, начиная отсюда, мы снова будем рассматривать архимедовские и неархимедовские нормирования совместно, понимая, таким образом, под K либо полное неархимедовски нормированное поле, либо поле вещественных или поле комплексных чисел, нормированные посредством абсолютных величин, т. е. функцией $\varphi(a) = |a|^p$.

Пусть Λ имеет конечную степень относительно K , $u_1, \dots, u_n$ — базис поля Λ над K , и K — полное относительно нормы φ . Если Φ — норма в поле Λ , совпадающая на K с φ , то последовательность

$$c_v = a_1^{(v)} u_1 + \dots + a_n^{(v)} u_n, \quad v = 1, 2, 3, \dots,$$

является фундаментальной относительно Φ тогда и только тогда, когда n последовательностей $\{a_i^{(v)}\}$ являются фундаментальными относительно Φ .

Так как последовательности $\{a_i^{(v)}\}$ сходятся к пределам a_i из K , то заключаем, что Δ — полное относительно Φ .

Доказательство. Сходимость последовательностей $\{a_i^{(v)}\}$ мы докажем методом полной индукции. Если c_v имеют вид

$$c_v = a_1^{(v)} u_1,$$

то $\{a_1^{(v)}\}$, разумеется, есть фундаментальная последовательность, коль скоро таковою является $\{c_v\}$. Пусть теперь наше утверждение уже доказано для всех последовательностей $\{c_v\}$ вида

$$c_v = \sum_{i=1}^{m-1} a_i^{(v)} u_i,$$

и рассмотрим последовательность

$$c_v = \sum_{i=1}^m a_i^{(v)} u_i.$$

Если последовательность $\{a_m^{(v)}\}$ сходится, то $\{c_v - a_m^{(v)} u_m\}$ также есть фундаментальная последовательность и, следовательно, $\{a_i^{(v)}\}$, $i < m$, сходятся по предположению индукции. Предположим теперь, что $\{a_m^{(v)}\}$, вопреки утверждению теоремы, не сходится. Тогда можно выбрать последовательность номеров $n_1, n_2, n_3, \dots$ так, чтобы $\varphi(a_m^{(v)} - a_m^{(v+n_v)}) > \varepsilon$ для всех v , где ε — фиксированное положительное число. Поэтому последовательность

$$d_v = \frac{c_v - c_{v+n_v}}{a_m^{(v)} - a_m^{(v+n_v)}} = \sum_{i=1}^{m-1} \frac{a_i^{(v)} - a_i^{(v+n_v)}}{a_m^{(v)} - a_m^{(v+n_v)}} u_i + u_m = \sum_{i=1}^{m-1} b_i^{(v)} u_i + u_m$$

должна стремиться к нулю, ибо последовательность числителей стремится к нулю, поскольку $\{c_v\}$ есть фундаментальная последовательность. Но

$$d_v - u_m = \sum_{i=1}^{m-1} b_i^{(v)} u_i.$$

Таким образом, в силу предположения индукции, последовательности $\{b_i^{(v)}\}$ сходятся к некоторым пределам b_i , и

$$-u_m = \sum_{i=1}^{m-1} b_i u_i,$$

что, однако, противоречит тому обстоятельству, что $u_1, \dots, u_n$ образуют базис поля Δ над K .

Совершенно так же докажем, что последовательность $\{c_i\}$ является нулевой тогда и только тогда, когда последовательности $\{a_i^{(v)}\}$ ($i=1, \dots, n$) нулевые.

На этом замечании основывается доказательство следующей теоремы единственности:

Продолжение Φ нормы φ , заданной в полном относительно η поле K , на алгебраическое расширение Δ этого поля однозначно определено, а именно

$$\Phi(\xi) = \sqrt[n]{\varphi(N(\xi))},$$

где норма $N(\xi)$ предполагается взятой в поле $K(\xi)$, а n — степень этого поля относительно K .

Доказательство. Достаточно рассмотреть какой-нибудь фиксированный элемент ξ с соответствующим полем $K(\xi)$; под нормами $N(\xi)$ тогда будут всюду подразумеваться нормы в этом поле. Если последовательность $\{c_i\}$ в поле $K(\xi)$ стремится к нулю (в смысле Φ) и если c_i выражены линейно через базисные элементы $u_1, \dots, u_n$ этого поля, то, по выше доказанному, также коэффициенты $a_i^{(v)}$ стремятся к нулю, а потому стремится к нулю и норма, являющаяся однородным полиномом этих коэффициентов. Предположим теперь, что, вопреки утверждению теоремы, $(\Phi(\xi))^n < \varphi(N(\xi))$ или $(\Phi(\xi))^n > \varphi(N(\xi))$. Полагая тогда

$$\eta = \frac{\xi^n}{N(\xi)}, \text{ соответственно } \eta = \frac{N(\xi)}{\xi^n},$$

в обоих случаях будем иметь $N(\eta) = 1$ и $\Phi(\eta) < 1$. Но в таком случае $\lim \eta^v = 0$ и, следовательно, $\lim N(\eta^v) = 0$, что, однако, противоречит равенству $N(\eta^v) = (N(\eta))^v = 1$.

Из доказанной теоремы вытекает следующее предложение:

Изоморфизм между двумя нормированными алгебраическими расширениями Δ, Δ' полного нормированного поля K , оставляющий элементы из K на месте, необходимо переводит норму, определённую в поле Δ , в норму, определённую в поле Δ' .

Архимедовские нормирования алгебраического числового поля строились в § 75 путём вложения этого поля в полное поле, которое можно было затем отождествлять с полем вещественных, соответственно комплексных, чисел. Совершенно аналогичным образом мы изучим теперь и продолжения неархимедовского нормирования неполного основного поля на алгебраическое расширение этого поля путём вложения алгебраического расширения в полное поле. При этом мы ради простоты ограничимся случаем конечного расширения Δ основного поля K , получающегося путём присоединения к K некоторых величин $\xi_1, \dots, \xi_r$, хотя все нижеследующие рассуждения непосредственно применимы и к тому случаю, когда к K присоединяется счётная (или вполне упорядоченная) последовательность величин $\xi_1, \xi_2, \dots$.

Пусть $\xi_1, \dots, \xi_t$ — корни полиномов $f_1(x), \dots, f_t(x)$, Ω — полное расширение поля K , и Σ — поле разложения полиномов $f_1(x), \dots, f_t(x)$ над Ω . В Σ , как алгебраическом расширении полного поля Ω , существует единственная норма, продолжающая норму, заданную в поле Ω . То же верно для всех полей, заключённых между Ω и Σ ; норма в таком промежуточном поле задаётся вместе с нормой в поле Σ .

Ясно, что мы получим норму в поле $\Lambda = K(\xi_1, \dots, \xi_t)$, как только мы *вложим* Λ в Σ , т. е. укажем изоморфное отображение σ поля Λ на подполе $\Lambda' = K(\xi'_1, \dots, \xi'_t)$ поля Σ , оставляющее при этом все элементы из K на месте. Действительно, тогда норму, заданную в поле Λ' как подполе поля Σ , можно будет с помощью отображения σ^{-1} непосредственно перенести на Λ .

Мы утверждаем теперь, что посредством этих вложений исчерпываются все нормы в поле Λ , продолжающие норму, заданную в поле K .

Для каждой такой нормы φ , заданной в поле Λ , существует изоморфное отображение этого поля на некоторое подполе Λ' поля Σ , оставляющее все элементы из K на месте и переводящее норму φ , заданную в поле Λ , в норму, определённую в поле Λ' .

Доказательство. Образует полное расширение поля Λ . Оно содержит полное расширение Ω поля K , а также величины $\xi_1, \dots, \xi_t$ и следовательно, содержит поле $\Omega(\xi_1, \dots, \xi_t)$. Но последнее всегда может быть продолжено до поля разложения полиномов $f_1, \dots, f_t$, которое изоморфно полю разложения Σ . Этот изоморфизм переводит $\Omega(\xi_1, \dots, \xi_t)$ в подполе $\Omega(\xi'_1, \dots, \xi'_t)$, оставляя все элементы из Ω на месте, и потому переводит также норму, определённую в поле $\Omega(\xi_1, \dots, \xi_t)$, в единственно возможную норму в поле $\Omega(\xi'_1, \dots, \xi'_t)$.

Из доказанной теоремы следует, что *все возможные продолжения заданной нормы в поле K до нормы в поле $\Lambda = K(\xi_1, \dots, \xi_n)$ определяются вложениями поля Λ всеми возможными способами в полное нормированное поле разложения Σ .*

Если, в частности, Λ — простое расширение, $\Lambda = K(\xi)$, с определяющим уравнением $f(\xi) = 0$, то Σ есть поле разложения полинома $f(x)$. Пусть

$$f(x) = f_1(x)f_2(x) \dots f_s(x)$$

— разложение полинома $f(x)$ на неприводимые множители над Ω . Каждое изоморфное отображение σ поля $K(\xi)$ в Σ переводит элемент ξ в корень полинома $f(x)$, т. е. в корень одного из полиномов $f_i(x)$. Каждому полиному $f_i(x)$ соответствует расширение $\Omega(\xi')$, где ξ' — какой-нибудь корень этого полинома (совершенно безразлично — какой), причём $\Omega(\xi')$ нормировано однозначно определённым способом. Каждый изоморфизм $K(\xi) \cong K(\xi')$, переводящий ξ

в ξ' и оставляющий элементы из K на месте, определяет вложение в указанном выше смысле, а потому и возможное нормирование поля $K(\xi)$. Поэтому (совершенно так, как в § 75) существует столько же различных норм, сколько имеется неприводимых множителей у $f(x)$ в $\Omega[x]$.

Случай непростого алгебраического расширения можно свести к последовательным простым расширениям, присоединяя элементы $\xi_1, \dots, \xi_r$ один за другим. Но можно также разложить непростое расширение на сепарабельное расширение, являющееся по теореме о примитивном элементе простым, и последующее расширение путём присоединения корней p -той степени (где p — характеристика поля K), на которое норма однозначно переносится тривиальным образом, поскольку тогда каждый элемент расширения есть корень p -той степени, и норма задаётся формулой

$$\varphi\left(\sqrt[p]{a}\right) = \sqrt[p]{\varphi(a)}.$$

Задача 4. Указать все нормы, определённые в поле гауссовских чисел (§ 14).

Задача 5. Если каждой норме в поле $\Delta(\xi_1, \dots, \xi_r)$ поставить в соответствие число, равное степени поля $\Omega(\xi'_1, \dots, \xi'_r)$ относительно Ω , то сумма этих чисел будет равна степени $(\Delta : K)$.

Новейшая литература о нормированных полях.

Ostrowski A., Untersuchungen zur arithmetischen Theorie der Körper (Die Theorie der Teilbarkeit in allgemeinen Körpern.). *Math. Zeitschr.*, **39** (1934), 269—404.

Witt E., Zyklische Körper und Algebren der Charakteristik p von Grad p^n . *J. reine u. angew. Math.* **176** (1936), 126—140.

Teichmüller O., Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper. *J. reine u. angew. Math.* **176** (1936), 141—152.

Mahler K., Über Pseudobewertungen. I. *Acta math.* **65** (1936), 79—119; II. *Acta math.* **67** (1936), 51—80.

Krull W., Allgemeine Bewertungstheorie. *J. reine u. angew. Math.* **167** (1932), 163—196.

Mac Lane S., The uniqueness of the power-series representation of certain fields with valuations. *Ann. of Math.* **39** (1938), 370—382.

Kaplansky J., Maximal fields with valuations. *Duke Math. J.* **9** (1942), 303—321.

ДОБАВЛЕНИЕ.

Частично упорядоченные множества.

Добавление посвящено изложению простейших свойств частично упорядоченных множеств, используемых в главах 8, 12, 14 и 16 книги и находящихся приложение во многих современных алгебраических исследованиях.

Множество S называется *частично упорядоченным*, если для некоторых пар его элементов a, b определено отношение $a \leq b$ (словами: « a предшествует b », « a содержится в b », « a меньше или равно b »), удовлетворяющее следующим условиям:

1) $a \leq a$;

2) из $a \leq b$ и $b \leq a$ следует $a = b$, т. е. элементы a и b совпадают;

3) из $a \leq b$, $b \leq c$ следует $a \leq c$ (транзитивность).

Символ $a < b$ будет означать, что $a \leq b$ и $a \neq b$. Символы $a \geq b$ (словами: « a следует за b », « a содержит b », « a больше или равно b ») и $a > b$ равносильны соответственно с $b \leq a$ и $b < a$.

Простейшим примером частично упорядоченного множества является множество всех подмножеств $A, B, \dots$ некоторого множества M , если отношение $A \leq B$ понимать так: «всякий элемент подмножества A содержится в подмножестве B » (т. е. $A \subseteq B$ в смысле § 1). Другим примером будет множество всех натуральных чисел, если в качестве отношения $a \leq b$ взять отношение: «натуральное число a является делителем натурального числа b ». Впрочем, если в случае множества натуральных чисел (или множества всех целых чисел, или множества всех вещественных чисел) отношение $\leq$ понимать в его обычном арифметическом смысле, то условия 1—3 также будут выполняться. Эти множества будут даже линейно упорядоченными в смысле следующего определения:

Частично упорядоченное множество S называется *линейно упорядоченным* (или просто *упорядоченным*), если для всякой пары его элементов a, b будет или $a \leq b$, или $b \leq a$.

Если множество S частично упорядочено (в частности, линейно упорядочено) при помощи отношения $\leq$, то и всякое его подмножество будет при помощи того же отношения частично упорядочено (соответственно линейно упорядочено).

Элемент a частично упорядоченного множества S называется *минимальным элементом* этого множества, если в S нет ни одного элемента x , удовлетворяющего соотношению $x < a$. Множество S может обладать или одним единственным минимальным элементом (в множестве всех подмножеств некоторого множества M единственным минимальным элементом будет пустое множество), или же многими различными минимальными элементами (в множестве всех непустых подмножеств множества M минимальными будут подмножества, состоящие из одного элемента); с другой стороны, множество S может вообще не иметь ни одного минимального элемента (таково множество всех бесконечных подмножеств некоторого бесконечного множества M , а также множество всех вещественных чисел с его естественной упорядоченностью по величине).

Сейчас мы определим очень важный класс частично упорядоченных множеств. Говорят, что частично упорядоченное множество S удовлетворяет *условию минимальности*, если в нём выполняется следующее свойство: *всякое непустое подмножество множества S обладает хотя бы одним минимальным элементом*.

Условие минимальности эквивалентно следующему условию *обрыва убывающих цепей*:

Всякая убывающая цепь элементов множества S :

$$a_1 > a_2 > \dots > a_n > \dots,$$

обрывается на конечном месте. Иными словами, если в S дана последовательность элементов $a_1, a_2, a_3, \dots$, причём

$$a_i \geq a_{i+1}, i = 1, 2, 3, \dots,$$

то, начиная с некоторого индекса n , все элементы последовательности будут равны между собой:

$$a_n = a_{n+1} = \dots$$

Из условия минимальности следует условие обрыва убывающих цепей: если множество S содержит бесконечную убывающую цепь элементов, то подмножество, составленное из всех элементов этой цепи, не может, очевидно, обладать минимальным элементом. Обратно, из условия обрыва убывающих цепей следует условие минимальности. Действительно¹⁾, пусть в подмножестве T множества S нет ни одного минимального элемента. Возьмём произвольный элемент a_1 из T . Так как он не минимальный, то в T можно найти такой элемент a_2 , что $a_1 > a_2$. Так как a_2 — снова не минимальный элемент подмножества T , то в T найдётся такой элемент

¹⁾ Здесь используется аксиома выбора, см. ниже.

a_3 , что $a_2 > a_3$. Продолжая так далее, мы получим бесконечную убывающую цепь элементов.

Всякое конечное множество при любой его частичной упорядоченности будет удовлетворять, понятно, условию минимальности. В указанном выше примере частичной упорядоченности множества натуральных чисел при помощи отношения делимости условие минимальности также выполняется.

Во всяком частично упорядоченном множестве S с условием минимальности справедлив следующий принцип индукции снизу по частично упорядоченному множеству:

Если все минимальные элементы множества S обладают свойством E и если из справедливости свойства E для всех элементов множества S , предшествующих некоторому элементу a и отличным от него, вытекает справедливость этого свойства для самого a , то все элементы множества S обладают свойством E .

В самом деле, пусть не все элементы множества S обладают свойством E . Тогда, по условию минимальности, среди всех элементов, не обладающих свойством E , можно указать хотя бы один минимальный; пусть это будет a . По предположению индукции, элемент a не будет минимальным в самом множестве S , т. е. в S существуют элементы, отличные от a и предшествующие ему. Все эти элементы уже обладают свойством E , а тогда, снова по предположению индукции, сам элемент a должен обладать свойством E , т. е. мы приходим к противоречию.

В действительности принцип индукции снизу для всех свойств E может выполняться лишь на множестве с условием минимальности и поэтому он эквивалентен условию минимальности. Пусть, в самом деле, в частично упорядоченном множестве S справедлив принцип индукции снизу. Применим его к следующему свойству E_0 : элемент a обладает свойством E_0 , если всякая убывающая цепь элементов, начинающаяся от элемента a , обрывается на конечном месте. Все минимальные элементы множества S обладают, очевидно, этим свойством E_0 . С другой стороны, пусть все элементы, предшествующие элементу a и отличным от него, обладают свойством E_0 . Если мы возьмем произвольную убывающую цепь элементов, начинающуюся от элемента a :

$$a > a' > a'' > \dots,$$

то второй член этой цепи, a' , уже обладает свойством E_0 , а поэтому наша цепь обрывается на конечном месте; этим доказано, что свойство E_0 справедливо и для a . Мы можем теперь, используя принцип индукции снизу, утверждать справедливость свойства E_0 для всех элементов множества S . Отсюда следует справедливость в S условия обрыва убывающих цепей, а поэтому и равносильного ему условия минимальности.

Построения методом индукции. На частично упорядоченных множествах с условием минимальности можно методом индукции проводить не только доказательства, но и построения. Пусть мы хотим всякому элементу x частично упорядоченного множества S с условием минимальности сопоставить некоторый новый объект $\varphi(x)$, причём эти объекты должны удовлетворять некоторым «рекуррентным соотношениям», связывающим каждый раз значение $\varphi(a)$ «функции» $\varphi(x)$ со значениями $\varphi(b)$, где $b < a$. Предположим, что этими соотношениями значение $\varphi(a)$ однозначно определяется, коль скоро уже заданы значения $\varphi(b)$ для всех $b, b < a$, удовлетворяющие между собою заданным соотношениям; в частности, значения $\varphi(a)$ для всех минимальных элементов a множества S вообще однозначно определены. При этих условиях существует одна и только одна функция $\varphi(x)$, определённая на множестве S , значения которой удовлетворяют заданным соотношениям.

Докажем сперва единственность функции $\varphi(x)$, причём в следующей более общей форме: если подмножества T множества S содержит вместе со всяким своим элементом и все элементы, ему предшествующие, и если на T может быть определена функция $\varphi(x)$, удовлетворяющая рекуррентным соотношениям, то лишь единственным способом. В самом деле, пусть на T можно определить две такие функции, $\varphi(x)$ и $\bar{\varphi}(x)$. В множестве тех элементов x , для которых $\varphi(x) \neq \bar{\varphi}(x)$, существует, по условию минимальности, хотя бы один минимальный элемент a . Для всех $b < a$ будет, следовательно, $\varphi(b) = \bar{\varphi}(b)$. Однако, задание всех $\varphi(b)$ однозначно определяет, по предположению, значение $\varphi(a)$, а поэтому должно быть $\varphi(a) = \bar{\varphi}(a)$, т. е. мы пришли к противоречию.

Для того чтобы доказать существование функции $\varphi(x)$ на множестве S , мы будем сперва индукцией по множеству S доказывать существование для каждого элемента a из S функции $\varphi_a(x)$, определённой на множестве всех элементов, предшествующих элементу a (включая само a), и удовлетворяющей поставленным условиям. Для минимальных элементов множества S существование таких функций было предположено заранее. Пусть теперь наше утверждение уже доказано для всех таких элементов b , что $b < a$. Если $b_1 < a$ и $b_2 < a$, то на множестве элементов, предшествующих как b_1 , так и b_2 , функции $\varphi_{b_1}(x)$ и $\varphi_{b_2}(x)$ будут совпадать, как вытекает из доказанной выше единственности функции, удовлетворяющей рекуррентным соотношениям. Отсюда следует, что если мы положим для каждого $b < a$

$$\varphi_a(b) = \varphi_b(b),$$

то этим определим функцию $\varphi_a(x)$, удовлетворяющую заданным

соотношениям на множестве всех элементов, предшествующих a и отличных от него. Однако, задание значений $\varphi_a(b)$ для всех $b < a$ однозначно определяет, в силу рекуррентных соотношений, значение $\varphi_a(a)$. Таким образом, функция $\varphi_a(x)$ полностью определена.

Так как на множестве S справедлив, ввиду условия минимальности, принцип индукции снизу, то существование функций $\varphi_a(x)$ нами доказано для всех a . Полагая

$$\varphi(a) = \varphi_a(a),$$

мы определим на множестве S функцию $\varphi(x)$. Она удовлетворяет заданным соотношениям, что устанавливается такими же рассуждениями, как те, которые были проведены в предшествующем абзаце.

Вполне упорядоченные множества. Линейно упорядоченное множество, удовлетворяющее условию минимальности, называется *вполне упорядоченным множеством*. Данные выше три равносильных определения частично упорядоченного множества с условием минимальности читатель без труда перенесёт на случай вполне упорядоченных множеств. Индукция по вполне упорядоченному множеству называется обычно *трансфинитной индукцией*.

Примером вполне упорядоченного множества будет множество натуральных чисел в его собственной упорядоченности: 1, 2, 3, ... Множество всех целых чисел в его естественной упорядоченности:

$$\dots, -2, -1, 0, 1, 2, \dots,$$

не будет вполне упорядоченным, так как не имеет первого элемента. Его можно, однако, вполне упорядочить, например, так:

$$0, 1, -1, 2, -2, \dots,$$

или же так:

$$1, 2, 3, \dots, 0, -1, -2, -3, \dots,$$

т. е. положив, что все положительные числа предшествуют нулю и всем отрицательным, а в остальном упорядочивая числа по их величине.

Значение вполне упорядоченных множеств и роль трансфинитной индукции, как метода, используемого в самых различных исследованиях, основаны на следующей теореме:

Теорема Цермело. *Всякое множество может быть вполне упорядочено.*

Доказательство этой теоремы см. в книге Хаусдорф, Теория множеств, § 12. Мы заметим лишь, что все доказательства теоремы

Цермело используют следующее предположение, которое, как впервые заметил Цермело, лежит в основе многих математических исследований:

Аксиома выбора. На всякой системе непустых множеств существует функция, сопоставляющая каждому из этих множеств один из его элементов.

Конечно, в каждом из заданных множеств, взятом отдельно, можно выбрать, ввиду его непустоты, один из его элементов. Аксиома утверждает, однако, что такой выбор во всех заданных множествах возможен одновременно, единым соответствием. Вопрос о логических основах этой аксиомы и о её совместимости с другими принципами, лежащими в фундаменте математики, ещё далеко не исчерпан.

В настоящей книге теорема Цермело не используется; что же касается аксиомы выбора, то она используется во многих местах, причём далеко не только там, где это отмечено соответствующим примечанием.

Множества с условием максимальности. Назовём элемент a частично упорядоченного множества S *максимальным элементом* этого множества, если в S нет ни одного элемента x , удовлетворяющего соотношению $x > a$. Говорят, что частично упорядоченное множество S удовлетворяет *условию максимальности*, если в нём выполняется следующее свойство: *всякое непустое подмножество множества S обладает хотя бы одним максимальным элементом.*

Если в частично упорядоченном множестве S с условием максимальности мы заменим заданную упорядоченность на противоположную, т. е. будем считать, что $b \leq a$ тогда и только тогда, если $a \leq b$ в заданной частичной упорядоченности множества S , то получим, очевидно, частично упорядоченное множество с условием минимальности. Отсюда вытекает, что *всё, доказанное выше для множеств с условием минимальности, может быть перенесено на множества с условием максимальности.* В частности, каждое из следующих двух условий равносильно условию максимальности:

Условие обрыва возрастающих цепей. *Всякая возрастающая цепь элементов множества S :*

$$a_1 < a_2 < \dots < a_n < \dots,$$

обрывается на конечном месте. Иными словами, если в S дана последовательность элементов $a_1, a_2, a_3, \dots$, причём

$$a_i \leq a_{i+1}, \quad i = 1, 2, 3, \dots,$$

то, начиная с некоторого индекса n , все элементы последовательности будут равны между собой:

$$a_n = a_{n+1} = \dots$$

Принцип индукции сверху. Если все максимальные элементы множества S обладают свойством E и если из справедливости свойства E для всех элементов множества S , следующих за некоторым элементом a и отличных от него, вытекает справедливость этого свойства для самого a , то все элементы множества S обладают свойством E .

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.

Числа указывают номера страниц, где впервые встречаются понятия.

- Абелева (= коммутативная) группа 28
- Абелево расширение 200
 - уравнение 200
- Абсолютная величина 268
 - — комплексного числа 287
- Автоморфизм 45
 - внешний 46
 - внутренний 46
- Аддитивная группа (= модуль) 33
 - — кольца 54
- Аксиома Архимеда 270
 - выбора 330
- Аксиомы Пеано 19
- Алгебра (= гиперкомплексная система) 67
 - с бесконечным базисом 70
 - с делением 68
- Алгебраическая зависимость 258
 - функция 262
- Алгебраически замкнутое поле 246
 - эквивалентные системы элементов 259
- Алгебраический базис 259
 - элемент 129
- Алгебраическое расширение 129, 142
 - число 284
 - числовое поле 254, 285
- Алгоритм деления 72, 81
 - Эвклида 82
- Арифметическая прогрессия n -го порядка 98
- Архимедовская норма 303
- Архимедовски расположенное поле 270
- Ассоциативность 20, 28, 53
- Ассоциированные элементы 85
- Базис алгебраический 259
 - векторного пространства 66
 - идеала 74
 - конечного расширения 136
- Базис линейно независимый 137
 - минимальный 137
 - множества 137
 - модуля 137
- Базисный элемент 66, 137
- Бесконечно-большой (малый) элемент 270
- Бесконечное множество 23
 - расширение 246
- Биномиальная теорема 58
- Вектор 66
- Векторное пространство (= модуль линейных форм) 65
- Верхняя граница (грань) 271
- Вес полинома 109
- Вещественное поле 287
 - число 25, 279
- Вещественно-замкнутое поле 288
- Взаимно однозначное отображение 18
 - простые множества 18
 - — элементы 82
- Внешний автоморфизм 46
- Внутренний автоморфизм 46
- Вполне положительное число 298
 - приводимая группа 192
 - упорядоченное множество 329
- Вторая теорема об изоморфизмах 185
- Вычет степенной 156
- Гауссовское числовое поле 68
- Гензелевские p -адические числа 307
- Гиперкомплексная система (= алгебра) 67
 - Главный идеал 74
- Гомоморфизм 48, 60
 - модулярный 183
 - операторный 182
- Гомоморфный образ 48, 60
- Граница верхняя 271
 - нижняя 271
- Грань верхняя 271

Группа 28

- абелева 28
 - автоморфизмов 45
 - аддитивная 33
 - вполне приводимая 192
 - Галуа поля 199
 - — поля деления круга 209
 - — уравнения 199
 - знакопеременная 38, 193
 - клейновская четверная 47
 - конечная 32
 - коммутативная (= абелева) 28
 - метациклическая (= разрешимая) 224
 - подстановок (преобразований) 29
 - — импримитивная 195
 - — интранзитивная 194
 - — примитивная 195
 - — транзитивная 194
 - простая 185
 - разрешимая 189
 - симметрическая 31
 - с операторами 180
 - циклическая 39
- Групповая таблица 33
Групповое кольцо 69

Двусторонний идеал 73

Двучленное уравнение 216

Действительное (= вещественное) число 25, 279

Деление 32

Делимая задача об удвоении куба 236

Делимость идеалов 78

— элементов 78, 305

Делитель 78

— единицы 85

— наибольший общий 80, 82

— нуля 56

— собственный 78, 85

Дискретная норма 304

Дистрибутивность 20, 36, 54

Дискриминант полинома 114

Дифференцирование 91

Длина нормального ряда 186

Допустимая подгруппа 180

Допустимый нормальный делитель 180

Единица группы 28

— кольца 56

Единичный идеал 74

— оператор 182

Зависимость алгебраическая 258

— линейная 134

Закон ассоциативности 20, 28, 53

— дистрибутивности 20, 36, 54

— коммутативности 20, 28, 53

— композиции 28

Знак числа 281

Знакопеременная группа 38, 193

Идеал 73

— главный 74

— двусторонний 73

— единичный 74

— левый 73

— нулевой 74

— правый 73

— простой 79

— свободный от делителей 79

Изоморфизм 44, 61

— непрерывный (= топологический) 311

— операторный 182

— относительный 159

— топологический (= непрерывный) 311

Изоморфные группы 44

— кольца 61

— множества 44

— нормальные ряды 187

Импримитивная группа 195

Инвариантная подгруппа (= нормальный делитель) 43

Индекс подгруппы 42

Индукция полная 19

— по частично упорядоченному множеству 327

— трансфинитная 329

Интерполяционная формула Лагранжа 95

— — Ньютона 95

Интранзитивная группа 194

Исключение 117

Канторово построение поля вещественных чисел 272

Квадратура круга 236

Кватернионы 69

Класс 26

— вычетов 51, 74

— смежный 41

— — левый 41

— — правый 41

— сопряженных элементов 47

Клейновская четверная группа 47

Кольцевое присоединение 70

Кольцо 53

— автоморфизмов 182

— без делителей нуля 56

— вычетов (= факторкольцо) 77

- Кольцо главных идеалов 81
 — групповое 69
 — коммутативное 54
 — матриц 69
 — нулевое 58
 — отношений 65
 — полиномов 70, 71
 — с единицей 57
 — целых гауссовских чисел 68
 — целых элементов поля 305
 — эвклидово 81
 — эндоморфизмов 182
 Коммутант 51
 Коммутативная (= абелева) группа 28
 Коммутативное кольцо 54
 Коммутативность 20, 28, 53
 Комплекс 41
 Комплексное число 68, 284
 Композиционные факторы 186
 Композиционный ряд 186
 Композиция элементов 28
 Компонента вектора 66
 Конечная группа 32
 Конечное множество 23
 — поле (= поле Галуа) 153
 — расширение 138
 Конечный ранг 137
 Корень вещественной функции 279
 — из единицы 148
 — — первообразный 149
 Корень полинома 92
 — — кратный 93, 145
 — — простой 94
 Корневое поле 165
 Коэффициент полинома 70
 — — старший 70
 Кратность корня 93, 145
 Кратное 57, 78
 — наименьшее общее 80
 — собственное 78
 Кратный корень полинома 93, 145
 Критерий (= признак) неприводимости Дюма 106
 — — Эйзенштейна 104, 319
 — приводимости Гензеля 316
 Круговое поле (= поле деления круга) 206
 Кубическая резольвента 231
 Левый идеал 73
 — обратный 57
 — смежный класс 41
 Лексикографическое расположение полинома 112
 Линейная зависимость 134
 — независимость 135
 — подстановка по модулю q 238
 Линейная форма 139
 Линейно-зависимый элемент 134
 — независимый базис 137
 — упорядоченное множество 325,
 — эквивалентные системы 136
 Линейный ранг множества 137
 — — (= степень) конечного расширения 138
 Логарифмическая норма 304
 Максимальный элемент множества 330
 Матрица 69
 Мёбиусовская функция 151
 Место (= норма поля) 304
 Метациклическая (= разрешимая) группа 224
 Метациклическое поле 224
 — уравнение 224
 Минимальный базис 137
 — элемент множества 326
 Многочлен (= полином) 70
 Множество 16
 — бесконечное 23
 — вполне упорядоченное 329
 — конечное 23
 — линейно упорядоченное 325
 — ограниченное сверху (снизу) 271
 — пустое 16
 — счётно-бесконечное 24
 — счётное 25
 — упорядоченное 325
 — частично упорядоченное 325
 Модуль (= аддитивная группа) 33
 — линейных форм (= векторное пространство) 65
 — относительно кольца 182
 — числовой 29
 Модулярный гомоморфизм 183
 Мощность множества 18
 Мультипликативная группа тела 59
 Надмножество (= объемлющее множество) 17
 Надполе (= расширение) 127
 Надтело (= расширение) 127
 Наибольший общий делитель (= сумма) идеалов 80
 — — элементов 82
 Наименьшее общее кратное идеалов 80
 Натуральное число 19
 Натуральный ряд 19
 Нейархимедовская норма 303
 Нейархимедовски расположенное поле 270
 Недискретная норма 304

- Независимость линейная 135
- Независимые трансцендентные 260
- Неизвестная 70
- Непрерывная функция 279
- Непрерывно изоморфные поля 311
- Непрерывный (= топологический) изоморфизм 311
- Неприводимость уравнения деления круга 208
- Неприводимый полином 85
 - радикал 222
 - случай («casus irreducibilis») 225
- Неразложимый (= простой) элемент 85
- Несепарабельное расширение 159
- Несепарабельный полином 159
 - элемент (= элемент 2-го рода) 159
- Несовершенное поле 163
- Нечётная подстановка 38
- Нижняя граница (грань) 271
- Норма гауссовского числа 83
 - элемента 169
 - — приведённая 174
- Норма 300
 - архимедовская 303
 - дискретная 304
 - логарифмическая 304
 - неархимедовская 303
 - недискретная 304
 - p -адическая 301
 - p -адическая 302
- Нормализатор подгруппы 51
 - элемента 47
- Нормальное расширение (= расширение Галуа) 146
 - —, соответствующее данному 198
 - уравнение (= уравнение Галуа) 147
- Нормальный делитель 43
 - — допустимый 180
 - ряд 186
 - — без повторений 186
 - — по подгруппе 187
- Нормированное поле 300
- Нулевая последовательность 273
- Нулевое кольцо 58
- Нулевой идеал 74
 - элемент 33, 54
- Нуль 22, 33, 54
- Область значений функции 16
 - импримитивности 195
 - мультипликаторов 181
 - операторов 180
 - определения функции 18
 - рациональности (= поле) 59
- Область транзитивности 194
 - целостности 56
- Образ 18
- Обратное отображение 18
 - преобразование (подстановка) 31
- Обратный элемент 28, 57
 - левый 57
 - правый 57
- Общее уравнение 224
- Объединение множеств 17
 - групп (полей) 203
- Объект преобразования 30
- Объемлющее множество (надмножество) 17
 - — собственное 17
- Ограниченное сверху (снизу) множество 271
- Однозначность разложения на простые множители 88
- Однородный полином (= форма) 72
- о-модуль 182
- Операторный гомоморфизм 182
 - изоморфизм 182
- Операторы 180
- Определение методом полной индукции 21
- Определяющее уравнение поля 130
- Основная теорема алгебры 285
 - — о конечных множествах 24
 - — о нормальных рядах (= теорема Шрайера) 187
 - — о симметрических функциях 110
 - — теории Галуа 201
- Относительный изоморфизм 159
- Отображение 18
 - взаимно однозначное 18
 - обратное 18
- Отрезок натурального ряда 22
- Отрицательное число 22
- Отрицательность 268
 - p -адическая норма 301
 - p -адическая норма 302
 - p -адическое поле 309
 - p -адическое число 307
 - — целое 308
- Первая теорема об изоморфизмах 184
- Первообразный корень из единицы 149
 - — по модулю p 156
- Переменная 71
- Пересечение 17
- Периоды поля деления круга 212
- Подгруппа 37

- Подгруппа допустимая 180
 — единичная 38
 — инвариантная (= нормальный делитель) 43
 — характеристическая 181
 Подкольцо 73
 Подмножество 17
 — собственное 17
 Подобно изоморфные поля 270
 — упорядоченные множества 44
 Подполе 124
 — простое 124
 Подстановка (= преобразование множества) 29
 — дробно-линейная 256
 — линейная по модулю q 238
 — нечётная 38
 — обратная 31
 — циклическая 38
 — чётная 38
 Подтело 121
 Показатель полинома 159
 — поля 162
 Поле 59
 — алгебраически замкнутое 246
 — алгебраических чисел 254, 285
 — архимедовски расположенное 270
 — вещественно замкнутое 288
 — вещественных алгебраических чисел 296
 — вещественных чисел 279
 — конечное (= поле Галуа) 153
 — гауссовское числовое 68
 — действительных (= вещественных) чисел 279
 — деления круга (= круговое поле) 206
 — значений нормы 300
 — классов вычетов нормы w 305
 — комплексных чисел 284
 — конечное (= поле Галуа) 153
 — корневое 165
 — корней из единицы 148
 — круговое (= поле деления круга) 206
 — метациклическое 224
 — неархимедовски расположенное 270
 — несовершенное 163
 — нормальное 146
 — нормированное 300
 — отношений 62
 — p -адических чисел 307
 — p -адическое 309
 — простое 124
 — разложения 142
 — расположенное 268
 Поле рациональных чисел 65, 125
 — совершенное 159, 163
 — формально вещественное 288
 — явно заданное 175
 Полином 70
 — деления круга 151
 — неприводимый 65
 — несепарабельный 159
 — однородный (= форма) 72
 — примитивный 100, 316
 — регулярный 103
 — сепарабельный 159
 — целочисленный 71
 Полная индукция 19
 — производная 262
 Полное расширение 306
 Положительность 268
 Порядок группы 33
 — элемента группы 40
 Последовательное исключение 141
 Последовательность фундаментальная 272
 — нулевая 273
 Построение методом индукции 21, 328
 — правильного многоугольника 237
 — — 17-угольника 215
 Построения с помощью циркуля и линейки 233
 Правый идеал 73
 — кратный 73
 — обратный 57
 — смежный класс 41
 Предел 276
 Представитель класса 27
 Преобразование множества 29
 — обратное 31
 Приведённая норма элемента 174
 — степень полинома 159
 — — поля 162
 Приведённый след 174
 Признак неприводимости Дюма 106
 — — Эйзенштейна 104, 319
 — приводимости Гензеля 316
 Примитивная группа 195
 Примитивное уравнение 200
 Примитивный полином 100, 316
 — элемент 165
 Принцип индукции сверху 331
 — — снизу 327
 — полной индукции 19
 Присоединение 127
 — неизвестной 70
 — кольцевое 70
 — символическое 133
 Продолжение изоморфизма 143
 — нормы 315

- Произведение комплексов 41
 — преобразований 30
 — прямое 190, 191
 — разностей 226
 — чисел 20
 — элементов 28
 Производная алгебраической функции 263
 — полинома 91
 — полная 262
 — сложной функции 266
 Прообраз 18
 Простая группа 185
 Простое алгебраическое расширение 129
 — поле 124
 — расширение 128
 — тело 124
 — трансцендентное расширение 129, 254
 — число 85
 Простой идеал 79
 — корень 94
 — (= неприводимый) элемент 85
 Простота знакопеременной группы 193
 Противоположный элемент 54
 Прямое произведение 190, 191
 Пустое множество 16

 Равномощные множества 18
 Радикал 220
 — неприводимый 222
 Разбиение на классы 26
 Разложение на множители 84
 — — — конечным числом проб 108
 — — — полиномов 100
 — на простейшие дроби 121
 Размерность векторного пространства 66, 137
 Разностное отношение 96
 Разрешимая группа 189
 Разрешимость в радикалах 220
 Ранг множества 137
 — конечного расширения 138
 — линейный 137
 — системы линейных уравнений 139
 Расположенное поле 268
 — — , архимедовски 270
 — — , неархимедовски 270
 Расширение (= надтело) 127
 — абелево 200
 — алгебраическое 129, 142
 — бесконечное 246
 — Галуа (= нормальное) 146
 — конечное 136
 — несепарабельное 159

 Расширение нормальное (= расширение Галуа) 146
 — полное 306
 — простое 128
 — — алгебраическое 129
 — — трансцендентное 129, 254
 — сепарабельное 159
 — трансцендентное 129
 — циклическое 200, 216
 — чисто трансцендентное 260
 Рациональная кривая 257
 — функция 254
 Рациональное число 65
 Регулярный полином 103
 Резольвента Галуа 147
 — кубическая 231
 — Лагранжа 217
 Результат 116
 Рекуррентные определяющие соотношения 21, 328
 Рефлексивность 26
 Ряд композиционный 186
 — натуральный 19
 — нормальный 186
 — — без повторений 186
 — — по подгруппе 187
 — степенной 309
 — Штурма 282

 Свойство модуля 73
 Сепарабельное расширение 159
 Сепарабельный полином 159
 — элемент (= элемент 1-го рода) 159
 Символическое присоединение 133
 Симметрическая группа 31
 — функция 109
 — — элементарная 109
 Симметричность 26
 Система кватернионов 68
 Система с двойной композицией 53
 След 169
 — приведённый 174
 Сложное произведение (сумма) 34
 Смежный класс 41
 — — левый 41
 — — правый 41
 Собственное кратное 78
 — объёмлющее множество 17
 — подмножество 17
 Собственный делитель идеала 78
 — — элемента 85
 Совершенное поле 159, 163
 Содержание полинома 100
 Соотношение эквивалентности 26
 Сопряжённые величины (элементы поля) 131

- Сопряжённые подгруппы 46
 - расширения 131
 - резольвенты 218
 - элементы группы 46
- Сравнение (по идеалу) 74
 - (по модулю) 52, 75
- Старший коэффициент полинома 70
 - — —, формальный 115
- Степенной ряд 309
- Степенные вычеты 156
 - суммы 113
- Степень элемента 35, 57
 - алгебраической величины 130
 - группы подстановок 197
 - (= линейный ранг) конечного расширения 138
 - — —, приведённая 162
 - полинома 70
 - — —, приведённая 159
 - — —, формальная 115
 - рациональной функции 254
 - трансцендентности 259
- Структурные константы алгебры 67
- Сумма Гаусса 216
 - (= наибольший общий делитель) идеалов 80
 - квадратов 287, 297
 - степенная 113
 - чисел 20
 - элементов 29
 - — —, сложная 34
- Схема разностей 97
- Счётно бесконечное множество 24
- Счётно множество 25
- Тело 58
 - кваaternionов 69
- Теорема Абеля 226
 - Вейерштрасса о корнях непрерывной функции 280, 291
 - Вильсона 156
 - Гаусса 100
 - Жордана-Гельдера 189
 - Люрота 256
 - об изоморфизме, 1-ая и 2-ая 184, 185
 - о верхней грани 278
 - однозначности для симметрических полиномов 111
 - о гомоморфизмах 51, 183
 - о замене (Штейница) 136
 - о примитивном элементе 165
 - о разрешимости в радикалах 221
- Теорема основная, алгебры 285
 - о конечных множествах 24
 - о нормальных рядах (Шрайера) 187
- Теорема основная, о симметрических функциях 110
 - — теории Галуа 201
 - о среднем значении 284
 - Островского 312, 314
 - о существовании алгебраически замкнутого расширения (Штейница) 247
 - Роля 284
 - сходимости Коши 276
 - Ферма 156
 - Цермело 329
 - Шрайера о нормальных рядах 187
 - Штейница о замене 136
 - — о существовании алгебраически замкнутого расширения 247
 - Штурма 281
 - Эйзенштейна 104
- Теория Галуа 198
- Тожественное преобразование (подстановка) 30
- Тожество Эйлера 92
- Топологический (=непрерывный) изоморфизм 311
- Точка (= норма поля) 304
- Транзитивная группа 194
- Транзитивность 26, 194
- Транспозиция 38
- Трансфинитная индукция 329
- Трансцендентное расширение 129, 254
- Трансцендентный элемент 129
- Трисекция угла 236
- Удвоение куба 236
- Уплотнение нормального ряда 186
- Упорядоченное множество 325
- Уравнение абелево 200
 - Галуа (= нормальное) 147
 - двучленное 216
 - деления круга 153, 206
 - метациклическое 224
 - нормальное (= уравнение Галуа) 147
 - общее 224
 - определяющее 130
 - примитивное 200
 - циклическое 200, 216
- Уравнения 2, 3 и 4 степени 226
- Условие максимальности 330
 - минимальности 326
 - обрыва возрастающих цепей 330
 - — убывающих цепей 326
- Факторгруппа 50
- Факторкольцо (= кольцо вычетов) 77

- Фактормодуль 51
 Факторы композиционные 186
 — нормального ряда 186
 Форма (= однородный полином) 72
 — линейная 139
 Формальная степень полинома 115
 Формально вещественное поле 288
 Формальный старший коэффициент 115
 — степенной ряд 309
 Формула Гаусса 213
 — Кардана 229
 — производной сложной функции 266
 Фундаментальная последовательность 272
 Функция 18
 — алгебраическая 262
 — Мёбиуса 151
 — непрерывная 279
 — рациональная 254
 — симметрическая 109
 — элементарная симметрическая 109
 — целая рациональная (=полином) 70, 71
 — Эйлера 149
 Характеристика тела (поля) 125
 Характеристическая подгруппа 161
 Целая рациональная функция (=полином) 70, 71
 Целое гауссовское число 68
 — p -адическое число 308
 — число 22
 Целочисленный полином 71
 Целые элементы поля 305
 Центр группы 44
 Цикл (= циклическая подстановка) 38
 Циклическая группа 39
 Циклическое расширение 200, 216
 — уравнение 200, 216
 Частично упорядоченное множество 325
 Четверная группа Клейна 47
 Четная подстановка 38
 Число алгебраическое 284
 — вещественное 25, 279
 — алгебраическое 296
 — вполне положительное 298
 — гауссовское 68
 — комплексное 68, 284
 — натуральное 19
 — отрицательное 22, 268
 — p -адическое 307
 — положительное 266
 — простое 85
 — рациональное 65
 — целое 22
 — гауссовское 68
 — p -адическое 308
 — элементов множества 24
 Числовой модуль 29
 Чисто трансцендентное расширение 260
 Эвклидово кольцо 81
 Эйлерово тождество 92
 Эйлеровская функция 149
 Эквивалентность 26
 Эквивалентные нормы 310
 — расширения 130
 — системы элементов 136
 Элемент множества 16
 — алгебраический 129
 — второго рода (= несепарабельный) 159
 — первого рода (= сепарабельный) 159
 — трансцендентный 129
 — (поля) целый 305
 Элементарная симметрическая функция 109
 Эндоморфизм 48
 Явно заданное поле 175

ОГИЗ
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
«ГОСТЕХИЗДАТ»

Москва, Орликов пер., 3

ПРОДОЛЖАЕТСЯ ПОДПИСКА
НА 1947 г. НА ЖУРНАЛ:
«УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК»

Ответственный редактор академик А. Н. КОЛМОГОРОВ
Журнал выходит 6 раз в год.

Подписная цена 90 рублей в год.

Подписка принимается во всех отделениях «Союзпечати»
и в местных почтовых отделениях.

Продажа производится во всех магазинах КОГИЗ'а и
нацкнижторгах.

ЗАМЕЧЕННЫЕ ОПЕЧАТКИ

СТР.	СТРОКА	НАПЕЧАТАНО	СЛЕДУЕТ ЧИТАТЬ	ПО ЧЬЕЙ ВИНЕ
49	8 стр.	$\overline{ab}$	$\overrightarrow{a\overline{b}}$	тип.
50	10 св.	x	$\overline{x}$	"
76	14 св.	образ $\bar{o}$	образ $\bar{o}$	"
121	12 св.	$f(x)$ и $f(x)$	$f(x)$ и $f'(x)$	"
143	4 св.	$\overline{a\overline{a}}$	$a\overline{a}$	"
148	6,7,11,20 св. }	II	II	"
151	5 св.	$x^{p^{n-1}}$	x^{p^n-1}	"
155	18 св.	$a^{p^{m-1}}$	a^{p^m-1}	"
156	14 св.	$a^{p^{n-1}}$	a^{p^n-1}	ред.
05	13 св.	$\sigma' = \tau\beta\tau\beta$	$\sigma\tau\beta = \tau\beta$	тип.
223	15 св.	x^{p^v}	x^{p_v}	"
23	16 св.	x^{q^v}	x^{q_v}	"
29	10 св.	$\rho^2(\rho, x_1)$	$\rho^2(\rho^2, x_1)$	"
237	15 св.	2^v-	2^v-1	ред.
242	20 св.	$\overline{\mathfrak{N}} \rightarrow \mathfrak{N}$	$\mathfrak{N} \rightarrow \overline{\mathfrak{N}}$	тип.
248	списка	аксиома вы о I	аксиома выбора I	"
274	1 св.	$a = \{a_p\} (n), \text{ то } 0 \neq$	$a = \{a_p\} \neq 0 (n), \text{ то}$	"
279	15 св.	$\lim \alpha_n + \lim \beta_n$	$\lim \alpha_n \pm \lim \beta_n$	"
282	8 св.	$X_1, X_2, \dots, X_r$	$X, X_1, \dots, X_r$	"
294	20 св.	$\overline{K}$	$\overline{K}$	ред.

