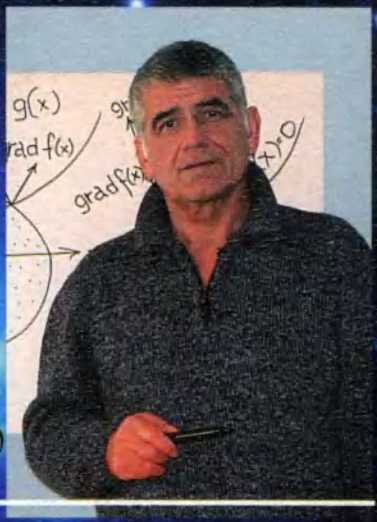
В. Босс



ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 8

Теория групп

Краткое и ясное изложение предмета

URSS

В. Босс

ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 8

Теория групп

МОСКВА

URSS

ББК 22.144я73

Босс В.

Лекции по математике. Т. 8: **Теория групп:** Учебное пособие. — М.: КомКнига, 2007. — 216 с.

В настоящей книге изложение преследует цель перевести теорию групп из разряда узкоспециализированных дисциплин в диапазон общеобразовательных математических предметов за счет иной расстановки акцентов, повышения доступности идеологии и освещения прикладных аспектов. Проблематика охватывается довольно широко, от обычных основ до теории Галуа и групп Ли. Делается особый упор на приложения к динамическим системам. Рассматриваются также сопутствующие вопросы из общей алгебры.

Изложение отличается краткостью и прозрачностью.

Для студентов, преподавателей, инженеров и научных работников.

Издательство «КомКнига». 117312, г. Москва, пр-т 60-летия Октября, 9.
Формат 60×90/16. Бумага офсетная. Печ. л. 13,5. Зак. № 720.

Отпечатано в ООО «ЛЕНАНД». 117312, г. Москва, пр-т 60-летия Октября, д. 11А, стр. 11.

13-значный ISBN, вводимый с 2007 г.:
ISBN 978–5–484–00941–1
Соотв. 10-значный ISBN, применяемый до 2007 г.:
ISBN 5–484–00941–3

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (495) 135–42–16
URSS Тел./факс: 7 (495) 135–42–46

4673 ID 50795

Оглавление

Предисловие к «Лекциям»

Озарение случается, когда пухнущая голова проваливается на уровень «дважды два», в то время как счет идет на миллионы.

Для нормального изучения любого математического предмета необходимы, по крайней мере, 4 ингредиента:

1) *живой учитель*;
2) *обыкновенный подробный учебник*;
3) *рядовой задачник*;
4) *учебник, освобожденный от рутины, но дающий общую картину, мотивы, связи, «что зачем».*

До четвертого пункта у системы образования руки не доходили. Конечно, подобная задача иногда ставилась и решалась, но в большинстве случаев — при параллельном исполнении функций обыкновенного учебника. Акценты из-за перегрузки менялись, и намерения со второй-третьей главы начинали дрейфовать, не достигая результата. В виртуальном пространстве так бывает. Аналог объединения гантели с теннисной ракеткой перестает решать обе задачи, хотя это не сразу бросается в глаза.

«Лекции» ставят 4-й пункт своей главной целью. Сопутствующая идея — экономия слов и средств. Правда, на фоне деклараций о краткости и ясности изложения предполагаемое издание около 20 томов может показаться тяжеловесным, но это связано с обширностью математики, а не с перегрузкой деталями.

Необходимо сказать, на кого рассчитано. Ответ «на всех» выглядит наивно, но он в какой-то мере отражает суть дела. Обозримый вид, обнаженные конструкции доказательств, — такого сорта книги удобно иметь под рукой. Не секрет, что специалисты

самой высокой категории тратят массу сил и времени на освоение математических секторов, лежащих за рамками собственной специализации. Здесь же ко многим проблемам предлагается короткая дорога, позволяющая быстро освоить новые области и освежить старые. Для начинающих «короткие дороги» тем более полезны, поскольку облегчают движение любыми другими путями.

В вопросе «на кого рассчитано» — есть и другой аспект. На сильных или слабых? На средний вуз или физтех? Опять-таки выходит «на всех». Звучит странно, но речь не идет о регламентации кругозора. Простым языком, коротко и прозрачно описывается предмет. Из этого каждый извлечет свое и двинется дальше.

Наконец, последнее. В условиях информационного наводнения инструменты вчерашнего дня перестают работать. Не потому, что изучаемые дисциплины чересчур разрослись, а потому, что новых секторов жизни стало слишком много. И в этих условиях мало кто готов уделять много времени чему-то одному. Поэтому учить всему — надо как-то иначе. «Лекции» дают пример. Плохой ли, хороший — покажет время. Но в любом случае, это продукт нового поколения. Те же «колеса», тот же «руль», та же математическая суть, — но по-другому.

Предисловие к восьмому то́му

Истина нуждается в недосказанности.

Если из арифметики убрать числовую конкретику, остается виртуальная основа, которая была бы не так интересна, если бы при манипуляциях иной природы не возникала та же самая абстракция. Различные физические и геометрические преобразования, теория кодирования, комбинаторные трюки — все это без маскирующих одежд перекликается друг с другом неожиданной идентичностью. И как глаголы без существительных, так и «операции вообще» — без предметного заземления — оказываются ядром соприкосновения различных интерпретаций. Задачи, раздетые догола, вдруг сливаются воедино, и начинает казаться, что еще усилие — и станет ясно, что в мире есть всего одна задача.

Название тома до некоторой степени условно. Речь идет об общей алгебре, но с акцентом на теории групп. Как ни странно, рассматриваемая область — несмотря на красоту и практическую значимость — остается за рамками общего образования. С этим надо что-то делать. Помня о том, что «научить» и «дать представление» — разные задачи. Обе важны для освоения предмета, но вторая — важнее, потому что формальное знание без укрупненного понимания — даже опасно. Более того, выучить математику по книгам вообще невозможно. Получить представление — другое дело. Остальное время целесообразно потратить на решение задач и продолжение рода.

Глава 1

Преобразования и симметрия

Интересные приложения часто начинают обсуждаться на той стадии, до которой мало кто добирается. Поэтому о сути и перспективах целесообразно говорить как можно раньше, сколь бы ни было это неудобно в отсутствие инструментов. Кое-что всегда можно сделать голыми руками.

1.1. Факторы «второго дна»

В устройстве мира топологические свойства располагаются на поверхности, алгебраические — в глубине. Поэтому с «непрерывности» приходится начинать, а если не углубляться, то ей и заканчивать. В итоге рейтинги матанализа превалируют, а *группы*, *кольца и поля* остаются на задворках образования, причем вроде бы заслуженно, поскольку остальное процветает в значительной степени независимо. Если сюда прибавить излишнюю настойчивость алгебраистов, рассказывающих, как важно то, чем они занимаются, спрос на алгебраические фокусы сильно падает, ибо «второе дно» остается вне поля зрения.

Конечно, разговоры о «втором дне» нередко возникают, когда нечего предъявить, как поначалу кажется. Скажем, учебники полны примерами, в которых те или иные замены переменных приводят к быстрому интегрированию дифференциального уравнения, или сводят уравнение в частных производных к обыкновенному. Но это производит впечатление разрозненных эпизодов, ибо причины успехов остаются невыявленными. Величина «замаха» не превосходит масштаба задачи — уравнение решено, и ладно. В результате кое-что не обнаруживается — вплоть до законов мироздания.

Уравнения электродинамики *Максвелла* после элементарных преобразований приводят к волновому уравнению

$$\frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2} = \frac{\partial^2 \mathbf{A}}{\partial x^2} + \frac{\partial^2 \mathbf{A}}{\partial y^2} + \frac{\partial^2 \mathbf{A}}{\partial z^2} \tag{1.1}$$

относительно векторного потенциала **A**, связанного с напряженностью электрического и магнитного поля соотношениями

$$\mathbf{E} = -\frac{1}{c}\frac{\partial \mathbf{A}}{\partial t}, \quad \mathbf{H} = \operatorname{rot} \mathbf{A}.$$

Понимание физики в данном случае не играет роли. Речь о другом. Уравнение (1.1) не выдерживает естественных замен координат (*преобразований Галилея*). Но это «вроде бы бред», поскольку физический процесс и его дифференциальное описание не могут зависеть от точки отсчета.

Подобного сорта казусы имеют обыкновение не привлекать внимания, тогда как необходимо, казалось бы, бить во все колокола. Либо уравнение (1.1) неправильно, либо мир устроен по-другому. (!) И если бы вопрос был так сразу поставлен (обострен), *группа преобразований Лоренца* [1] и *теория относительности* были бы открыты намного раньше. Причем для успеха нужны были бы даже не теоремы, а один лишь стиль теоретико-группового мышления.

Последнее обстоятельство весьма примечательно. Ценить принято формулы, теоремы и их следствия. Но фарватер развития науки определяют — *категории мышления*. И одна из продуктивных схем практического применения *теории групп* заключается в самóм подходе к решению проблем. К тому или иному объекту — будь то алгебраическое или дифференциальное уравнение, геометрическая фигура или какая-то функция — применяют некоторую группу преобразований и смотрят на реакцию. Если объект остается нечувствителен (инвариантен) к преобразованиям данной группы, то из этого делаются определенные выводы о его свойствах. Другими словами, инвариантность объекта по отношению к той или иной группе преобразований дает полезную информацию о его устройстве [2].

Если функция $f(x_1, \ldots, x_n)$ нечувствительна к любому повороту системы координат, можно утверждать, что

$$f(x) = \hat{f}(x_1^2 + \ldots + x_n^2).$$

Это один из наиболее понятных и тривиальных вариантов. Но изотропность пространства (независимость свойств от направления) дает и менее очевидные

---

[1] Уравнение (1.1) инвариантно по отношению именно к *преобразованиям Лоренца* вида

$$x = \frac{x' + vt'}{\sqrt{1-\beta^2}}, \quad y = y', \quad z = z', \quad t = \frac{1}{\sqrt{1-\beta^2}}\left(t' + \frac{\beta x'}{c}\right),$$

где $\beta = v/c$, v — скорость движения штрихованной системы координат вдоль оси x.

[2] Инвариантность уравнений классической механики к сдвигам по времени — пустячок вроде бы — влечет за собой *закон сохранения энергии*.

следствия, например, выделяет среди других — дифференциальный *оператор Лапласа*

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2},$$

что определяет особую роль последнего в физике [3)].

Инвариантность широко применяется для интегрирования дифференциальных уравнений, а также для вывода фундаментальных законов природы. Последнее иногда производит едва ли не мистическое впечатление, настолько силен *контраст тривиальности причин с нетривиальностью выводов*. Вот несколько примеров [3] на эту тему.

Задача о распределении скоростей молекул газа в свое время была серьезным камнем преткновения. Легенда утверждает, что Максвелл решил проблему за полчаса на экзамене. Правдоподобная реконструкция истории примерно такова.

Чтобы не тратить лишних слов, абстрагируемся от физики. Итак, пусть случайный вектор $x = \{x_1, \ldots, x_n\}$ распределен с неизвестной плотностью $p(x)$, которая удовлетворяет двум свойствам:

(i) *величины* x_i *независимы*,

(ii) $p(x)$ *не зависит от направления* x.

Представляется, что эти свойства не так много говорят о плотности. На самом деле они однозначно определяют ее [4)]. Действительно, из (i) вытекает

$$p(x) = p_1(x_1) \ldots p_n(x_n),$$

а из (ii) следует

$$p(x) = p(x_1^2 + \ldots + x_n^2),$$

т. е. функция $p(x)$, а значит и

$$\ln p(x) = \ln p_1(x) + \ln p_n(x), \tag{1.2}$$

постоянна на сферах

$$x^2 = x_1^2 + \ldots + x_n^2 = \text{const}. \tag{1.3}$$

[3)] Широко известны уравнения: *теплопроводности* $\Delta u = \gamma \dfrac{\partial u}{\partial t}$, *Лапласа* $\Delta u = 0$, *Пуассона* $\Delta u = f$, *волновое* $\Delta u = \gamma \dfrac{\partial^2 u}{\partial^2 t}$.

[4)] Разумеется, с точностью до нормировок.

Другими словами, функции (1.2) и (1.3) имеют одни и те же поверхности уровня, а это возможно, лишь когда их градиенты коллинеарны, т. е.

$$\nabla \ln p(x) = \lambda \nabla x^2,$$

что дает n равенств

$$\frac{p_i'(x_i)}{p_i(x)} + 2\lambda x_i = 0,$$

интегрирование которых приводит к

$$p_i(x_i) = k_i e^{-\lambda x_i^2}.$$

Константы определяются нормировкой и заданием, например, второго момента σ^2. Окончательно

$$p(x) = (2\pi\sigma^2)^{-n/2} \exp\left\{-\frac{x_1^2 + \ldots + x_n^2}{\sqrt{2\pi\sigma^2}}\right\}. \tag{1.4}$$

Вывод (1.4) заслуживает того, чтобы в него вжиться. Преобразования, не меняющие уравнений движения, тех или иных функций, решений, критических значений, — обычно легко находятся. Но при этом кажется, что все это тривиально и не стоит выеденного яйца. Поэтому главная проблема заключается в преодолении пессимизма. Пути, ведущие к успеху, большей частью выглядят тупиковыми, что требует сверхъестественного чутья и готовности двигаться, закусив удила, по «дороге в никуда».

Именно в этом и заключался секрет успеха Максвелла, а не в двух последующих строчках взятия градиентов. Можно держать пари, что будь задача поставлена в виде: «какова функция $p(x)$, удовлетворяющая двум условиям (i), (ii)», — ее бы решил каждый третий студент, а подобрал бы $p(x)$ — каждый второй. Сложность — в постановке задачи, для чего нужно было задаться вопросом: «Что можно считать известным относительно $p(x)$?». Здесь бы уже любой студент указал (i), (ii). Но тут и происходит сбой. Скептик не может заставить себя думать дальше. Ему кажется, что из такой чепухи ничего нельзя вывести. Максвелл же не стал мудрствовать в поисках оригинальных ответов, — что подавляющую часть исследователей уводит в дебри, — взял очевидные свойства и стал решать задачу, не уступая эмоциям типа «вряд ли такой ерунды достаточно для решения».

Контраст причин и следствий всегда разителен. Грандиозные следствия опираются на ничтожные причины. Но тут ничего удивительного. Причины голые, а следствия в масках.

- Банальный факт

$$\varepsilon_1 - \varepsilon_2 + \varepsilon_2 - \varepsilon_3 + \ldots + \varepsilon_n - \varepsilon_{n+1} = \varepsilon_1 - \varepsilon_{n+1} \tag{1.5}$$

навевает скуку, но полагая $\varepsilon_k = \operatorname{arctg} \ln k$ и учитывая

$$\operatorname{arctg} u - \operatorname{arctg} v = \operatorname{arctg} \frac{u - v}{1 + uv},$$

приходим к

$$\sum_{k=1}^{n} \operatorname{arctg} \left(\frac{\ln (k+1) - \ln k}{1 + \ln k \ln (k+1)} \right) = \operatorname{arctg} (\ln (n+1)). \tag{1.6}$$

Если теперь (1.5) не афишировать, то (1.6) не так легко доказать. И подобных следствий из пустяков — миллион, о чем жизнь то и дело напоминает. То ли Создатель широко пользовался такой техникой, то ли оно само так получилось, но мы вынуждены постоянно иметь дело с фактами типа (1.6). Голые причины вида (1.5) тоже в поле зрения, но их потенциал «не выпирает», связи не видны, и мир — в ловушке кривых зеркал. Следствия дразнят загадочностью, а причины незаметны из-за банальности.

• Красноречивый пример — история открытия омега-минус гиперона. *Гелл-Манн*[5], как-то услышавший об открытии новой элементарной частицы, тут же предсказал — существование еще одной, которая и была обнаружена в экспериментах через три года. Это выглядело даже более эффектно, чем открытие планеты *Нептун*, вычисленной предварительно *Леверье* и *Адамсом*, — хотя в основе лежала причина типа (1.5).

Подоплека заключалась в следующем. Квантовая механика с самого начала успешно справлялась с ситуациями, где колеблется «непонятно что» [3]. Затем продвинулась далеко вперед, и уже описывала элементарные частицы как собственные векторы «неизвестно какого» оператора Шрёдингера[6]. Правда, у неизвестного оператора предполагались известными некоторые свойства — не меняться под действием той или иной группы преобразований.

Так вот, *Гелл-Манн*, занимавшийся изучением некой группы SU_3, сразу увидел, что размерность пространства, в котором действует *неизвестный* оператор Шрёдингера, надо так увеличить (в связи с открытием новой частицы), чтобы соответствующая группа преобразований могла действовать в этом пространстве, и новый собственный вектор (как имидж частицы) мог появиться. Но тогда возникал еще один «лишний» собственный вектор («лишняя» частица). Вот, собственно, и вся подноготная. Потом на волне успеха с омега-минус гипероном *Гелл-Манн*, эксплуатируя ту же группу SU_3, выдвинул теорию *кварков*, которых не могут найти до сих пор.

---

[5] Нобелевский лауреат 1969 г.

[6] Изучение «неизвестно какого» оператора Шрёдингера может показаться сарказмом, но это не совсем так. Для решения многих задач уравнения, описывающие объект изучения, действительно не нужны. Дифференциальное уравнение полезно иметь перед глазами лишь как гарантию того, что в поле зрения попадают все необходимые параметры — см. далее.

• Здесь, пожалуй, уместны две нижеследующие выдержки из статьи *Дайсона*[7]. На данном этапе изложения текст не вполне ясен, но для «намека» это несущественно. Да и понимания здесь особо не требуется. Речь-то идет по существу о наводящих соображениях, которые могли бы и не оправдаться. Но интересен сам теоретико-групповой стиль мышления, позволяющий правдоподобно рассуждать об устройстве Вселенной, не вникая в детали.

«...Минковский в лекции 1908 г. не довел свои аргументы до логического завершения. Он не обратил внимания на инвариантность уравнений Максвелла относительно тривиальной абелевой группы T_4, — сдвигов координат пространства-времени. Естественная группа инвариантности теории Максвелла — не шестимерная группа Лоренца, а десятимерная группа Пуанкаре P — полупрямое произведение G_c и T_4. Соответственно, группа симметрий ньютоновской механики — не шестимерная группа G_∞, а десятимерная группа Галилея G — полупрямое произведение G_∞ и T_4. Ни P, ни G не являются полупростыми группами[8].

Задним числом легко видеть, что логика Минковского должна была привести кого-нибудь к мысли о существовании простой группы D, вырожденным пределом которой будет P, в точности так же, как у полупростой группы G_c вырожденным пределом является группа G_∞. Это группа де Ситтера D, вещественная некомпактная форма простой алгебры Ли B_2. Следуя аргументам Минковского, математики легко могли бы предположить в 1908 г., что истинной группой инвариантности мира должна быть группа D, а не P. В действительности D является группой симметрий расширяющейся Вселенной без материи, радиус кривизны которой R есть линейная функция времени. D вырождается в P в пределе плоского пространства $\lim R \to \infty$, так же как G_c вырождается в G_∞ в ньютоновском пределе $c \to \infty$.

Предположим, кто-то в 1908 г. был достаточно уверен в себе, чтобы принять эту идею всерьез. Тогда он смог бы правильно предсказать расширение Вселенной, открытой экспериментально Хабблом спустя 20 лет. Еще важнее, что это могло бы привести к постулированию кривизны пространства-времени и, следовательно, намного сократить путь к общей теории относительности. К счастью, Эйнштейн сформулировал принцип общей относительности, проделав тяжелый путь, который ему никто не облегчил. Де Ситтер в действительности открыл свою модель расширяющейся Вселенной через год после овладения теорией Эйнштейна.

<...>

В 1844 г. произошли два примечательных события. Гамильтон опубликовал открытие кватернионов, а Грассман издал книгу "Ausdehnungslehre". С запоздалой проницательностью мы видим, что работа Грассмана была более значительным вкладом в математику и содержала элементы многих концепций современной алгебры, включая, как частный случай, векторный анализ. Однако Грассман был простым школьным учителем в Штеттине, в то время как Гамильтон — всемирно

[7] *Dyson F. J.* Missed Opportunities // Bull. Amer. Math. Soc. 1972. **78**. P. 635. Перевод с английского в: УМН. 1980. **35**. Вып. 1.

[8] Определение *полупростых* групп можно найти в [16], но можно считать, что речь идет о *простых* группах (глава 6).

известным математиком... Гиббсу досталось в удел первому в лекции 1886 г. сопоставить идеи Гамильтона и Грассмана...

Не знаю, сколько чистых математиков слышали или читали лекцию Гиббса. Внимательное изучение лекции помогло бы им заметить, что Гиббсу на самом деле не удалось объединить понятия кватерниона и вектора. Напротив, обсудив параллельно эти два понятия, он показал их явную несопоставимость. Его лекция должна была заставить каждого вдумчивого математика спросить себя: „Чем объяснить, что свойства трехмерного пространства представляются одинаково хорошо двумя совершенно разными и несовместимыми алгебраическими структурами?". Будь такой вопрос однажды ясно поставлен, наверное, скоро бы нашелся ответ; и он неизбежно привел бы к полной теории однозначных и двузначных представлений группы трехмерных вращений. Векторы образуют простейшее нетривиальное однозначное представление, а кватернионы — простейшее двузначное представление. Кватернионы — прототипы спинорных представлений в современной терминологии. Развитие теории спинорных представлений, фактически начатое Эли Картаном в 1913 г., завершилось в основном в 30-е годы при существенной помощи физиков Паули и Дирака; оно могло бы начаться приблизительно на 40 лет раньше».

1.2. Группы преобразований

Группы исторически возникли как *группы преобразований* — с *композицией* в качестве *групповой операции*. Чтобы совокупность Φ отображений $f : X \to X$ была группой, требуется[9]:

1. $f(x), g(x) \in \Phi \Rightarrow f(g(x)) \in \Phi$.
2. *Тождественное отображение* $e(x) \equiv x$ *входит в* Φ.
3. *Любое отображение* $f \in \Phi$ *имеет обратное* $f^{-1} \in \Phi$.

Эта конструкция охватывает массу приложений: *проективные преобразования* в геометрии, *преобразования Лоренца* в теории относительности, теория инвариантных преобразований дифференциальных уравнений, *группы Галуа* алгебраических уравнений и т. п. Более того, если группа изначально возникает в другом облике, с определенными трудозатратами можно перейти к изучению групп преобразований. Скажем, от группы действительных чисел *по сложению* можно перейти к изоморфной группе операторов сдвига $f_a(x)$; числу a отвечает функция $f_a(x) = x + a$.

[9] Это, собственно, и есть определение группы, с точностью до изоморфизма, — см. главу 2. Ассоциативность при композиции в качестве групповой операции — обеспечивается автоматически.

• Группу комплексных чисел $\alpha + i\beta$ (без нуля) *по умножению* эквивалентно заменяет группа матриц

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \alpha^2 + \beta^2 \neq 0,$$

с матричным умножением в качестве групповой операции.

Соответствия

$$1 \Leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i \Leftrightarrow \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

легко проверяются. В частности,

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

В то же время любую матрицу можно рассматривать как линейный оператор, а умножению матриц отвечает композиция операторов.

• Примером группы может служить семейство дробно-линейных преобразований

$$x = \frac{ax' + b}{cx' + d}, \quad ad - bc \not\equiv 0, \tag{1.7}$$

эквивалентное группе невырожденных матриц

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

опять-таки с матричным умножением в качестве групповой операции [10)].

1.3. Инвариантность дифференциальных уравнений

О применении групповых методов при изучении дифференциальных уравнений широко известно. Но представления эти носят большей частью упрощенный (и даже искаженный) характер. В то же время положительный эффект соответствующего направления мысли довольно весом, хотя итоги часто выглядят результатом догадок. Рассмотрим несколько примеров.

• Уравнение

$$\frac{dx}{dt} + x - 3t = 0 \tag{1.8}$$

[10)] Композиция преобразований (1.7) оказывается преобразованием того же вида, с коэффициентами, совпадающими с элементами произведения соответствующих матриц. (?)

не меняется под действием преобразований (a — параметр)

$$t = t' - a, \quad x = x' - 3a. \tag{1.9}$$

В штрихованных координатах уравнение (1.8) выглядит точно так же.

Преобразования (1.9) не меняют также функции $z = x - 3t$. «Поэтому» замена $x = z + 3t$ сразу упрощает (1.8), приводя к уравнению с разделяющимися переменными

$$\frac{dz}{z+3} = -dt, \tag{1.10}$$

интегрирование которого дает $z = Ce^{-t} - 3$, или в исходных переменных

$$x = 3t + Ce^{-t} - 3. \tag{1.11}$$

Проделанные манипуляции оставляют двойственное чувство. Причины успеха завуалированы, и слово «поэтому» не случайно взято в кавычки, поскольку логические связи по крайней мере неочевидны. Более того, решение (1.11) не инвариантно по отношению к преобразованиям (1.9). (!) Эта неувязка, правда, — результат недосмотра. Но поначалу всегда полезнее ошибиться, чтобы почувствовать берега.

Из инвариантности уравнения (1.8) по отношению к (1.9) — вытекает другое. Если $x = \varphi(t, C)$ — семейство решений (1.8), то подстановка (1.9) должна оставлять решение решением, но константа при этом может меняться[11] (!), т. е. $x = \varphi(t, C)$ после замены (1.9) обязано перейти в некое штрихованное решение

$$x' = \varphi(t', C'),$$

возникающее из $x' - 3a = \varphi(t' - a, C)$, т. е.

$$3a + \varphi(t' - a, C) = \varphi(t', C') \tag{1.12}$$

при некотором $C' = C'(a, C)$. Решение (1.11) удовлетворяет функциональному соотношению (1.12). Обратный путь (1.12) $\Rightarrow$ (1.11) можно проделать, опираясь на те или иные трюки. Однако простейший вариант — это переход к уравнению (1.10), но он содержит некую логическую шероховатость. Между прочим, логичных объяснений удачным заменам переменных обычно не находится и во многих учебниках по дифференциальным уравнениям. Не говоря о том,

[11] Преобразование (1.9) не меняет *семейства* решений, хотя сами решения могут меняться местами.

что *Ньютон*, *Эйлер*, *Лагранж* — долгое время разрабатывали методы интегрирования диф-уравнений, и все это выглядело набором разрозненных технических приемов, пока общие корни не открыл *Софус Ли*, — (глава 12).

Остановимся еще на нескольких примерах.

- Однородное уравнение

$$\frac{dx}{dt} = \varphi\left(\frac{x}{t}\right)$$

не меняется под действием преобразований $t = at'$, $x = ax'$, которые не меняют также функции $z = x/t$. «Поэтому» переход от переменных (x, t) к переменным (z, t) опять-таки приводит к уравнению с разделяющимися переменными

$$\frac{dz}{dt} = \frac{\varphi(z) - z}{t} \quad \Rightarrow \quad \frac{dz}{\varphi(z) - z} = \frac{dt}{t},$$

интегрирование которого дает

$$t = \exp\left\{\int_0^{x/t} \frac{dz}{\varphi(z) - z} + C\right\}.$$

- Упоминание «инвариантных преобразований» в приведенных примерах может показаться «сбоку бантиком», потому что новая переменная и так напрашивается. Вот пример иного сорта. *Уравнение Абеля второго рода*

$$x\frac{dx}{dt} = \frac{2}{t^3} - \frac{3}{t^2}x \tag{1.13}$$

имеет степенной вид, и здесь естественно ожидать инвариантность по отношению к группе растяжений $x = \alpha x'$, $y = \beta y'$. Подстановка показывает, что для инвариантности (1.13) требуется $\alpha\beta = 1$, т. е.

$$t = kt', \quad x = \frac{1}{k}x'. \tag{1.14}$$

Эти же преобразования не влияют на функцию $z = tx$. «Поэтому» переход от переменных (t, x) к (t, z) упрощает (1.13) и дает интегрируемое уравнение

$$\frac{zdz}{z^2 - 3z + 2} = \frac{dt}{t}. \tag{1.15}$$

Относительно (1.14) инвариантно также *уравнение Риккати*

$$\dot{x} + \alpha x^2 = \beta t^{-2}.$$

Эффект получается аналогичный.

Интересно, что *уравнение Риккати* вида

$$\dot{x} + \alpha x^2 = \beta t^\gamma \tag{1.16}$$

интегрируется в квадратурах, как показал *Лиувилль*, только при $\gamma = 0$, $\gamma = -2$ и $\gamma = \dfrac{4n}{1-2n}$ (n — целое). Результат выглядит удивительным, потому что не ясно, как это можно доказать. Сами интегралы в перечисленных случаях легко находятся (*Д. Бернулли*), но как установить, что других — нет? В контексте группового анализа естественно возникает предположение, что интегрируемый дифур обязан быть нечувствительным к некоторой группе преобразований, обладающей определенными свойствами. Только — легко сказка сказывается.

Разумеется, однопараметрические группы преобразований, каковые пока рассматривались, не исчерпывают возможности. С увеличением числа параметров относительная простота улетучивается. Например, *уравнение Риккати*

$$\dot{x} = \alpha(t)x^2 + \beta(t)x + \gamma(t)$$

не меняет своего вида в случае преобразований

$$x = \frac{ax' + b}{cx' + d}, \quad ad - bc \not\equiv 0,$$

но каковы последствия? Далеко не ясно. Безусловно, инвариантность здесь что-то означает, но что? Как это можно использовать для анализа, решения?

Определенная специфика возникает в связи с уравнениями в частных производных. Рассмотрим задачу о диффузии,

$$u_t = u_{xx}, \quad u(x, 0) = u_0\delta(x), \tag{1.17}$$

при условии обнуления решения $u(x, t)$ на бесконечности.

Соотношения (1.17) не меняются при замене

$$x = e^{-a}x', \quad t = e^{-2a}t', \quad u = e^a u' \tag{1.18}$$

с учетом обычного для дельта-функции свойства $\delta(\mu x) = \delta(x)/\mu$.

Пусть теперь $u = \varphi(x,t)$ — решение (1.17). Поскольку инвариантно к преобразованиям (1.18) не только уравнение диффузии (теплопроводности) $u_t = u_{xx}$, но и «краевое» условие $u(x,0) = u_0\delta(x)$, т. е. задача целиком, то $u' = \varphi(x',t')$ — также обязано быть решением [12)].

Подставляя (1.18) в $u = \varphi(x,t)$, имеем

$$u' = e^{-a}\varphi(e^{-a}x', e^{-2a}t') = \varphi(x',t'),$$

что достигается в случае

$$\varphi(x,t) = \frac{1}{\sqrt{t}}\psi\left(\frac{x}{\sqrt{t}}\right). \tag{1.19}$$

Вводя переменную $\tau = x/\sqrt{t}$ и подставляя (1.19) в $u_t = u_{xx}$, приходим к обыкновенному дифференциальному уравнению

$$2\frac{d^2\psi}{d\tau^2} + \tau\frac{d\psi}{d\tau} + \psi = 0,$$

решая которое с учетом краевых условий (в нуле и на бесконечности), получаем в итоге хорошо известное решение исходной задачи

$$u(x,t) = \frac{1}{2\sqrt{\pi t}}e^{-x^2/(4t)}.$$

Вместо (1.17) по аналогии с предыдущим можно было бы рассматривать только уравнение

$$u_t = u_{xx} \tag{1.20}$$

без краевых условий. Тогда бы в поле зрения попали семейства решений, но уже не параметризуемые константами. Инвариантных преобразований тоже прибавилось бы. Помимо (1.18), а также очевидных групп преобразований

$$x = x' + a, \quad t = t' + a, \quad u = e^a u', \quad u' = u + a\varphi(x,t),$$

где $\varphi(x,t)$ любое частное решение (1.17), — появляется, например, нетривиальная группа

$$\left\{t = t',\ x = x' + 2at',\ u = u'e^{-a^2t' - ax'}\right\}.$$

[12)] В этом заключается отличие данной ситуации от рассмотренных выше примеров, где речь шла не об однозначно решаемых *задачах Коши*, а о дифурах, имеющих *семейства* решений.

Сразу же возникает вопрос, что делать с этим множеством групп, как их свести в одну многопараметрическую, и — стоит ли.

1.4. Методы подобия и размерности

В физике довольно широко используется упрощенный групповой анализ в виде *методов подобия и размерности*. При этом группы часто не упоминаются, а сами методы выглядят совершенно самостоятельными. Как бы там ни было, рецептура весьма эффективна, проста, и в ряду теоретических инструментов физики заслуживает едва ли не первоочередного употребления, а с точки зрения переноса «трюковой части» на абстрактную основу — заслуживает серьезного внимания. Но пока остановимся на примерах [13], не выходя за рамки физики.

• **Истечение жидкости** из бака — в установившемся режиме определяется тремя параметрами: *плотностью* ρ и *высотой столба* h жидкости, а также *ускорением свободного падения* g, — от которых зависит «остальное». Поэтому, например, вес жидкости Q, вытекающий в единицу времени, есть

$$Q = \varphi(\rho, g, h).$$

Размерности параметров:

$$[\rho] = \frac{M}{L^3}, \quad [g] = \frac{L}{T^2}, \quad [h] = L, \quad [Q] = \frac{ML}{T^2},$$

где M — единица массы, L — длины, T — времени [14]. Поэтому

$$\frac{Q}{\rho g^{3/2} h^{5/2}} = \frac{\varphi(\rho, g, h)}{\rho g^{3/2} h^{5/2}} = \psi(\rho, g, h)$$

— безразмерная величина. Но так как безразмерную константу из ρ, g, h образовать невозможно, то $\psi(\rho, g, h)$ от ρ, g, h не зависит, а значит, является некой константой k. В результате:

$$Q = k\rho g^{3/2} h^{5/2}.$$

При включении в список исходных параметров радиуса r сливного отверстия — получилось бы $k = k(r/h)$. Константа, правда, остается все равно неизвестной, но становится ясным качественное свойство: пропорциональное изменение радиуса и высоты на поток не влияет.

---

[13] Детали и физические комментарии см. в [1, 25], где рассматривается масса других интересных задач.

[14] Обозначение $[x]$ для размерности величины x предложено *Максвеллом*.

• **Движение жидкости.** Простейшие задачи гидродинамики часто определяются четырьмя параметрами: *плотностью* ρ, *коэффициентом вязкости* μ, характерным линейным *размером* l и характерной (часто средней) *скоростью* v. Из

$$\rho,\ \mu,\ l,\ v \tag{1.21}$$

можно образовать только одну безразмерную величину

$$\mathsf{R} = \frac{lv\rho}{\mu},$$

называемую *числом Рейнольдса*. Поэтому в любой задаче (подзадаче), определяемой параметрами (1.21), все безразмерные величины будут функциями только числа Рейнольдса.

Задач подобного рода довольно много. Например, движение жидкости в трубах с определением практически важных характеристик, таких как падение давления и сопротивление трубы на единицу длины. Это могут быть и задачи о движении твердого тела (скажем, подводной лодки) в жидкости. В этом случае сила F сопротивления жидкости будет (по той же технологии)

$$F = k(\mathsf{R})\rho v^2 l^2.$$

• Если заранее ясно, что период τ колебаний маятника может зависеть лишь от m, g, l, то проблема сводится к поиску комбинации из m, g, l, имеющей размерность времени. Такая комбинация единственна: $\sqrt{l/g}$, масса m оказывается ни при чем. Поэтому $\tau = k\sqrt{l/g}$, где k — некая безразмерная константа.

• Качественный анализ механизма *флаттер-эффекта*[15] показывает, что ситуация определяется параметрами (вариант движения в жидкости)

$$E,\ \mu,\ m,\ \rho,\ l,\ v, \tag{1.22}$$

где E и μ — *модули Юнга и сдвига*, m — *масса* движущегося тела, ρ — *плотность* жидкости, l — характерный *размер*, v — *критическая скорость*.

Знание «модулей» и их размерностей — необязательно. Здесь важна схема. Из набора (1.22) конструируются три безразмерных параметра

$$\frac{\rho v^2}{E},\quad \frac{\mu}{E},\quad \frac{m}{\rho l^3},$$

каждый из которых можно выразить как неизвестную функцию двух остальных. Отсюда

$$v = \sqrt{\frac{E}{\rho}}\,\varphi\left(\frac{\mu}{E}, \frac{m}{\rho l^3}\right). \tag{1.23}$$

[15] Особого рода динамическая неустойчивость взрывного характера при движении твердого тела в жидкой или газовой среде.

Конечно, неизвестная функция φ частично омрачает успех, но формула (1.23) является значительным шагом в понимании закономерностей флаттера. Сразу ясно, например, что ослабление жесткости в n раз (модулей E и μ) уменьшает критическую скорость в $\sqrt{n}$ раз.

Кроме того, функция φ может быть восстановлена в гидродинамических экспериментах либо при обдувании дешевых моделей самолетов в аэродинамических трубах. Именно поэтому название методики помимо размерности упоминает *подобие*. Дело в том, что «полуфабрикаты» теории размерности, хотя и содержат неизвестные величины и функции, — дают прозрачные ориентиры для экспериментального исследования, которое, как оказывается, можно проводить на игрушечных моделях, в том или ином смысле *подобных* реальным объектам.

• Оценим массу M камней, необходимую для перекрытия реки. Пусть m обозначает массу камней, засыпаемых в единицу времени, l — характерный размер фиксированного профиля реки, ρ — плотность воды, v — скорость течения, g — ускорение свободного падения. Возможны три безразмерные комбинации:

$$\frac{m}{M}\sqrt{\frac{l}{g}}, \quad \frac{lg}{v^2}, \quad \frac{m}{v\rho l^2}.$$

Искомая масса M в результате:

$$M = m\sqrt{\frac{l}{g}}\,\psi\left(\frac{lg}{v^2}, \frac{m}{v\rho l^2}\right).$$

Остается на дешевом макете провести эксперимент для компенсации недостающей информации о функции ψ.

(!) Обратим внимание, что на практике восстанавливать функцию ψ, вообще говоря, не требуется. «Секрет» эксперимента заключен в безразмерных параметрах. Скажем, макет русла реки имеет характерный размер l, в 10^4 раз меньший реального. Тогда, чтобы не менять параметр lg/v^2, скорость течения v надо уменьшить в 100 раз, после чего для поддержания значения параметра $m/(v\rho l^2)$ скорость засыпки m необходимо уменьшить в 10^{10} раз. В этом случае значение ψ не изменится, а $m\sqrt{l/g}$, и соответственно M, уменьшится в 10^{12} раз.

Подобные задачи весьма важны при возведении плотин и строительстве ГЭС. Необходимую для «засыпки» массу приходится подвозить заранее, и надо знать «сколько». На всякий случай подвозят в несколько раз больше теоретического расчета [16]. Говорят, возле некоторых плотин так и лежат горы привезенного про запас.

Продолжать можно до бесконечности. В подобном ключе решаются задачи, к которым иначе не видно как подступиться. Турбу-

[16] Разумеется, проведенный анализ игнорирует ряд факторов, которые в принципе легко учесть.

лентность, взрывные явления, распространение пламени, затухание ударных волн и т. п. Выглядит эффектно и походит на «лихие» методы физиков, которые без колебаний делят на нуль, если это сулит выгоды [17]. Но «методика» имеет под собой вполне логичную основу.

Отсутствие дифференциальных уравнений, описывающих задачу, — иллюзорно. Уравнения — за кадром. Но они наяву и не нужны, потому что «методика» не ставит целью дать исчерпывающее решение, ограничиваясь выявлением характера зависимостей и оставляя константы, а иногда и функции, для дополнительного исследования, если в том есть утилитарная или «диссертационная» потребность. Происходит ограничение *теоретико-групповым ингредиентом задачи*, что до некоторой степени скрыто за особым словоупотреблением.

Чтобы почувствовать закулисную специфику, рассмотрим движение маятника,

$$m\ddot{x} + kx = 0, \quad x(0) = x_0 \quad (\textit{маятник на пружине}), \tag{1.24}$$

либо

$$J\ddot{\varphi} + mgl \sin\varphi = 0, \quad \varphi(0) = \varphi_0 \quad (\textit{подвешенный маятник}),$$

что в случае *момента инерции* $J = ml^2$ переходит в

$$\ddot{\varphi} + \frac{g}{l} \sin\varphi = 0, \quad \varphi(0) = \varphi_0. \tag{1.25}$$

Задача (1.24) характеризуется переменными

$$x,\ x_0,\ t,\ k,\ m,$$

из которых можно образовать только две (независимые) безразмерные комбинации:

$$\frac{x}{x_0} \quad \text{и} \quad t\sqrt{\frac{k}{m}}.$$

Поэтому

$$x = x_0 f\left(t\sqrt{\frac{k}{m}}\right).$$

[17] По определению, честный человек большой подлости при малой выгоде — не сделает. Физик же всегда готов на некорректные действия (имеются в виду математические) — и в этом его сила.

Любое характерное время, например период колебаний τ, определяется равенством

$$\tau = \sqrt{\frac{m}{k}}\,\nu(x_0, k, m).$$

Из переменных x_0, k, m безразмерная комбинация не образуется, поэтому

$$\nu(x_0, k, m) = \text{const} \quad \Rightarrow \quad \tau = \nu\sqrt{\frac{m}{k}}.$$

Вариант (1.25) тот же рецепт приводит к решению

$$\varphi = \varphi\left(t\sqrt{\frac{g}{l}},\ \varphi_0\right).$$

Так что нелинейность уравнений не является препятствием для методики.

(!) Наличие дифференциальных уравнений на стартовых позициях в данном случае придает манипуляциям некоторую солидность, но если вдуматься, то ясно, что дифуры здесь играют роль декораций. Они лишь подсказывают, какие параметры в изучаемой ситуации существенны. И если последнее ясно из других соображений, дифуры оказываются ни при чем.

1.5. Связь с групповым анализом

Закономерно встает вопрос: кроется ли за *методикой согласования размерностей* таинство природы, или физика наводит тень на плетень? — И да и нет.

Скажем, в задаче (1.24), т. е.

$$m\frac{d^2x}{dt^2} + kx = 0, \quad x(0) = x_0, \tag{1.26}$$

будь она поставлена в абстрактной форме, без какой бы то ни было интерпретации переменных, — ничто не мешает приписать x некую размерность $[x] = X$, и далее:

$$[t] = T, \quad [m] = M, \quad [k] = \frac{M}{T^2}. \tag{1.27}$$

Таким образом, размерности $[x]$, $[t]$, $[m]$ задаются произвольно, $[k]$ выбирается так, чтобы слагаемые в (1.26) измерялись в одних единицах. Далее путь аналогичен. Те же безразмерные комбинации, тот же результат. Поэтому никакая физика в случае (1.26) не требуется.

Более того, сам разговор о размерностях совершенно необязателен. Он просто является удобным мнемоническим приемом, который помогает понять, к какой группе преобразований инвариантно уравнение (1.26) и как эту информацию удобно далее использовать. Иными словами, согласование размерностей — это эквивалентный язык для работы с определенными группами преобразований. В данном случае уравнение (1.26) инвариантно (нечувствительно) к заменам [18)]

$$\begin{cases} m = \alpha m', \\ x = \beta x', \\ t = \gamma t', \\ k = \dfrac{\alpha}{\gamma^2} k', \end{cases} \tag{1.28}$$

прозрачно соответствующим размерностям (1.27).

Дифференциальные уравнения в подоплеке необязательны. Для обычного квадратного уравнения

$$x^2 - 2ax + b = 0 \tag{1.29}$$

можно задать произвольно размерность $[x] = X$, получив, как следствие, $[a] = X$, $[b] = X^2$. Далее индикатор размерности позволяет частично контролировать правильность формул. Например,

$$x_{1,2} = a \pm \sqrt{a^2 - b}$$

проходит контроль соответствия размерности. Некоторые формулы сразу отсеиваются.

То же самое получается, если заметить, что уравнение (1.29) не меняется (по сути) при замене ($k > 0$)

$$\left\{ \begin{array}{l} x = kx' \\ a = ka' \\ b = k^2 b' \end{array} \right\}, \qquad k > 0, \tag{1.30}$$

[18)] Все «греческие» параметры — положительны.

которая однозначно перекликается с рассмотренными выше размерностями. Формула для корней уравнения также обязана быть инвариантной к замене (1.30) — и это требование равносильно согласованию размерностей.

Так что сказанное пока — не в пользу «таинства». Все сводится к специфическим группам преобразований, хотя надо признать, что «язык размерностей» приходится кстати. Кроме того, теория размерности учит, что (!) *конкретно решаемую задачу полезно погружать в параметрическое семейство, не оставаясь в плену частных случаев* типа $\ddot{x} + 2x = 0$ или $x^2 + 3x - 2 = 0$. «Шевеление констант» проливает дополнительный свет [19].

Вернемся, например, к уравнению (1.13), которое после замены констант параметрами a, b приобретает вид

$$x\frac{dx}{dt} = \frac{a}{t^3} - \frac{b}{t^2}x. \tag{1.31}$$

Если $[x] = L$, $[t] = T$, то для согласования размерностей в самом уравнении (1.31) требуется: $[a] = L^2T^2$, $[b] = LT$.

Ограничимся поиском какого либо частного решения. Комбинация xt/b безразмерна, поэтому

$$x = \frac{b}{t}\varphi(a, b, t),$$

а поскольку из a, b, t можно образовать только одну безразмерную величину $\dfrac{a}{b^2}$, то

$$x = \frac{b}{t}\psi\left(\frac{a}{b^2}\right). \tag{1.32}$$

Подставляя (1.32) в (1.31), приходим к необходимости $b^2\psi^2 - b^2\psi + a = 0$, откуда

$$\psi_{1,2}\left(\frac{a}{b^2}\right) = \frac{1 \pm \sqrt{1 - 4a/b^2}}{2},$$

что в итоге дает два частных решения [20] $x = \dfrac{b}{t}\psi_{1,2}$.

Что же касается «секунд и килограммов», то они вроде бы необязательны. Вместо размерностей можно говорить о группах

[19] Групповой анализ с позиций *групп Ли* (глава 12) обычно отделяет параметры от переменных и параметры не трогает.

[20] О *продолжимости решений* — см. [4, т. 2].

преобразований. Но это только половина правды. С помощью размерностей решается, например, задача о высоте брызг при движении торпедного катера. Уравнений нет, но зависимости устанавливаются. «Чудо» объясняется наличием айсберга физики со всеми фундаментальными законами механики и термодинамики, что позволяет результативно говорить о задачах, не выписывая уравнений. А также делать содержательные выводы о свойствах и структуре этих уравнений, не имея возможности их предъявить. Вот показательный пример [25].

Теплоотдача в потоке жидкости. Задача была решена *Рэлеем* (1915) и породила «детективную загадку». Количество тепла H, отдаваемое телом в единицу времени, определяют следующие параметры: характерный размер l тела, скорость обтекания v, разность температур Δ тела и жидкости, теплоемкость c и теплопроводность λ жидкости[21].

Иными словами,

$$H = \varphi(l, v, \Delta, c, \lambda).$$

В качестве базовых единиц измерения были выбраны: L (длина), T (время), C° (температура в градусах), Q (количество тепла). Из переменных, размерности которых: $[H] = Q/T$,

$$[l] = L, \quad [v] = \frac{L}{T}, \quad [\Delta] = C^\circ, \quad [c] = \frac{Q}{L^3 C^\circ}, \quad [\lambda] = \frac{Q}{LC^\circ T}, \tag{1.33}$$

образуются только две безразмерных комбинации,

$$\frac{H}{\lambda l \Delta} \quad \text{и} \quad \frac{lvc}{\lambda}.$$

Следовательно,

$$H = \lambda l \Delta \cdot \psi\left(\frac{lvc}{\lambda}\right). \tag{1.34}$$

Это и есть *формула Рэлея*, инициировавшая парадокс.

Суть претензий к (1.34) сводилась к следующему. Температура и количество тепла имеют, вообще говоря, размерность энергии. Поэтому если из списка *Рэлея* базовых единиц измерения исключить градусы, включив единицу массы M, — размерности переменных меняются:

$$[l] = L, \quad [v] = \frac{L}{T}, \quad [\Delta] = \frac{ML^2}{T^2}, \quad [c] = \frac{1}{L^3}, \quad [\lambda] = \frac{1}{LT},$$

[21] Мы избегаем физических уточнений. Детали см. в [25].

и теперь из l, v, Δ, c, λ можно образовать уже две безразмерные величины:

$$\frac{lvc}{\lambda} \quad \text{и} \quad cl^3.$$

В результате вместо (1.34) получается формула

$$H = \lambda l \Delta \cdot \psi\left(\frac{lvc}{\lambda},\ cl^3\right), \tag{1.35}$$

гораздо менее информативная. Выходит, что углубление знаний о природе тепла размывает добытый ранее результат (1.34), полученный на основе более поверхностного анализа. Удивительно, что причина парадокса современниками *Рэлея* так и не была вскрыта, несмотря на дискуссию. Между тем ответ совсем прост. С учетом эквивалентности калорий, градусов и механической энергии, — список параметров (1.33) должен быть формально пополнен двумя обменными коэффициентами: *механическим эквивалентом тепла* J $\left([J] = ML^2/(T^2Q)\right)$ и *постоянной Больцмана* k $\left([k] = ML^2/(T^2C^\circ)\right)$, — которые позволяют эту эквивалентность использовать. И тогда из пополненного списка (1.33) образуются уже две безразмерные комбинации $\frac{lvc}{\lambda}$ и $\frac{Jcl^3}{k}$, в результате чего итоговая формула принимает вид:

$$H = \lambda l \Delta \cdot \psi\left(\frac{lvc}{\lambda},\ \frac{Jcl^3}{k}\right). \tag{1.36}$$

Теперь остается учесть, что в рассматриваемом физическом процессе переход механической энергии в тепловую (и наоборот) не происходит. Поэтому значение J не существенно. Но тогда функция ψ в (1.36) не зависит от J, а значит, и от второго аргумента, что возвращает (1.36) к исходной версии (1.34).

Пример обращает внимание на ряд важных обстоятельств, неважно, идет речь о физике или о другой области. В частности, наглядно проявляются «относительность» базовой системы единиц измерения и принципиальная роль обменных коэффициентов (физических констант). Участвуют ли последние в «разыгрываемом спектакле» — определяется их присутствием в дифференциальных уравнениях, описывающих изучаемое явление. Но если происходит заочный анализ (в отсутствие диф-уравнений), то включение/исключение «обменных коэффициентов» в список переменных задачи определяется пониманием физики процесса.

Базовая система единиц измерения может быть выбрана более-менее произвольно. От крайнего случая «все переменные задачи

имеют индивидуальные размерности»[22] до декларации «все величины безразмерны». Последнее, конечно, даром не дается. Как, скажем, происходит уменьшение числа базовых единиц измерения. Фиксация, допустим, скорости света c ($[c] = L/T$) в качестве безразмерной величины уравнивает в правах L и T, — и тогда длина будет измеряться в секундах либо время — в метрах (кому как больше нравится), а число базовых механических единиц (L, T, M) уменьшится с трех до двух.

Не останавливаясь на этом, можно зафиксировать еще какую-нибудь физическую постоянную, например, — *гравитационную* γ, размерность которой

$$[\gamma] = \frac{L^3}{MT^2}.$$

Размерностью массы тогда будет L^3/T^2. А если учесть ранее принятое $L \sim T$, то остается всего одна единица измерения. Фиксация еще одной постоянной — понятие размерности вообще ликвидирует (вместе с Палатой мер и весов). Все начинает измеряться в абстрактных единицах.

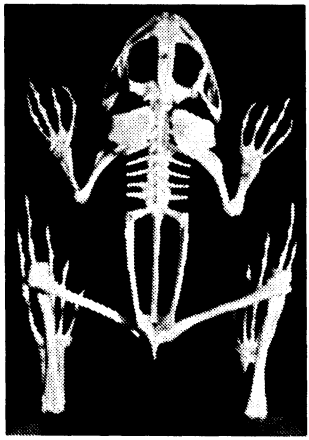
1.6. Симметрия Мироздания

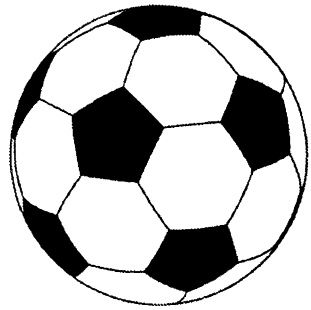
Бытовое представление о симметрии возникает из визуальных образов и ассоциируется с геометрией. Гармония зеркальных отражений и поворотов, простых орнаментов и замысловатых кружев, — вот что питает иррациональное чувство. Но ментальное углубление в подноготную фактов раздвигает горизонты так широко, что первоначальные впечатления рассыпаются в пыль.

Симметрия[23], в широком смысле слова, начинает интерпретироваться как *инвариантность свойств*, *структур*, *форм* — по отношению к той или иной группе преобразований. Подобная нечувствительность к преобразованиям бывает глубоко скрыта, и найти, «что и по отношению к чему — не меняется», иногда оказывается предметом научного открытия. На виду остается геометрическая

[22] Но тогда потребуется множество обменных коэффициентов.

[23] От греч. *symmetria* — соразмерность.





симметрия, да и то — не вся. За кадром же в поле зрения попадают «неожиданные экспонаты».

Симметрична, как выясняется, музыкальная мелодия, ибо остается узнаваемой — будь сыграна в любой октаве и на любом инструменте. Причем наличие уха человеческого, как инструмента восприятия, непринципиально, потому что сдвиг мелодии вдоль звукоряда инвариантен не «из-за уха», а из-за логарифмирования частот, после которого неважно — бас или сопрано. Симметрична любая автономная система $\dot{x} = f(x)$, потому что инвариантна к переносу точки отсчета во времени.

Симметрично все, что закономерно. Что происходит одинаково при изменении части условий. Так устроен Мир, управляемый законами. Так движется Сознание, направляемое рамками симметричного Бытия.

Симметрично все, где видится гармония. Явная и неявная. Безотчетно воспринимаемая и трудно объяснимая. В теории чисел, например, многие формулы *Рамануджана*, обладавшего мистическим даром поиска уникальных числовых законов, — дразнят потусторонней загадочностью. Здесь не место углубляться в детали, но даже самые простые его находки типа

$$\sqrt{1+2\sqrt{1+3\sqrt{1+\ldots}}} = 3,$$

$$\sqrt{8-\sqrt{8+\sqrt{8-\ldots}}} = 1+2\sqrt{3}\sin 20^\circ,$$

$$\sqrt[3]{\sqrt[3]{2}-1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$$

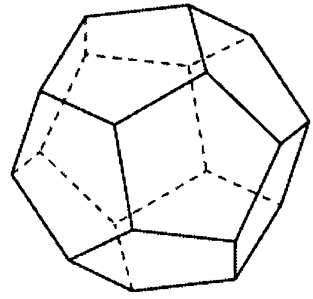
вызывают удивление. Проверка равенств не так сложна, но их же надо было найти (!), что противится материалистическому обоснованию.

Но даже если отбросить интуитивные ощущения, которые не всегда удается легализовать «алгебраически», — Мир остается симметричным, потому что любой закон природы свидетельствует о той или иной инвариантности к изменению «внешних» условий. Однако подобная широта взглядов приносит мало конкретной пользы. Более конструктивно изучение частных разновидностей симметрий, особенно тех, которые определяют фундаментальные свойства Пространства и Времени. И здесь снова, но уже на втором витке, происходит разворот в сторону геометрии.

В первую очередь изучают *группу движений* — преобразований, сохраняющих расстояния. Все движения подразделяются на: *повороты*, *отражения*, *переносы* и композиции отражений и переносов. Это, конечно, теорема — но она лежит вне рамок данного контекста.

На плоскости группа движений, оставляющих неподвижной некоторую точку O, включает только повороты вокруг O и отражения относительно прямых, проходящих через O. Она имеет *подгруппу поворотов* C_n на углы $2k\pi/n$, $k = 0, 1, \ldots, n-1$. *Группа диэдра* D_n включает все повороты из C_n и n отражений относительно прямых, проходящих через точку O и составляющих друг с другом равные углы. Группа D_n изоморфна *группе самосовмещений* правильного n-угольника.

Правильные многогранники, с точки зрения инвариантности по отношению к пространственным поворотам и отражениям, — более сложны для анализа, ибо требуют пространственного воображения и привлечения техники группового анализа. Но сама их классификация может быть легко проведена на другой основе.



Правильный многогранник характеризуется тем, что в каждой вершине сходится одно и то же число K ребер и одно и то же число N ребер

ограничивает каждую грань. Если V обозначает число вершин, R — ребер, G — граней многогранника, то

$$N \cdot G = 2R, \quad K \cdot V = 2R,$$

что после подстановки в *формулу Эйлера* $V - R + G = 2$ (см., например, [3]), приводит к уравнению

$$\left(\frac{2}{K} - 1 + \frac{2}{N}\right) R = 2.$$

Все возможные решения легко определяются прямым перебором[24]:

$K = 3$, $N = 3$ — *тетраэдр*,

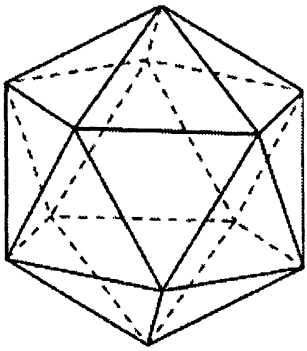
$K = 3$, $N = 4$ — *куб*,

$K = 3$, $N = 5$ — *додекаэдр*,

$K = 4$, $N = 3$ — *октаэдр*,

$K = 5$, $N = 3$ — *икосаэдр*.

Вот, собственно, и все, если полагаться на принцип «прокукарекал, а там пусть хоть не рассветает». Формально задача решена, но загадка остается, что свидетельствует «...о существовании неразгаданных механизмов и скрытых пружин. Результат... стоит как-то особняком, сам по себе, ни с чем не перекликается, никаких вселенских закономерностей не выражает, хотя кажется, что должен» [3].



Теоретико-групповой подход помещает задачу в среду родственных фактов. Многогранников больше не получается, но результаты уже не стоят особняком, перекликаясь и резонируя с другими фактами. Группа икосаэдра, например, оказывается связанной с проблемой неразрешимости алгебраических уравнений в радикалах. Однако подробное рассмотрение геометрических манипуляций

[24] Перебор ограничивается целочисленными решениями неравенства

$$\frac{2}{K} + \frac{2}{N} > 1$$

при очевидном ограничении $K, N > 2$.

с правильными многогранниками требует совсем другого темпа рассуждений, наиболее подходящего для индивидуального обдумывания, нежели для книжного изложения, рассчитанного на среднестатистический вариант восприятия.

Многочисленные разновидности симметрий, которые физически воплощаются в кристаллических структурах, — относят обычно к свойствам физического пространства, но это создает определенную путаницу. Ибо, если говорить о широком диапазоне масштабов и точек зрения, — никто не знает, что такое физическое пространство. Подразумевается обычно $\mathbb{R}^3$, но это лишь чистый холст. Когда декларируют, например, что природа не содержит в себе винта, то это не относится к $\mathbb{R}^3$, куда помещается штопор [25]. Другое дело, что описание фундаментальных явлений (да и то не всех) не меняется при смене левой системы координат на правую. Но это свойство процессов, а не вмещающего пространства, и здесь — зона ответственности физики.

Рождение физических законов происходит своеобразными путями, на которых математическая корректность только мешает. Возьмем в качестве примера электродинамику. *Уравнения Максвелла* в вакууме имеют вид

$$\operatorname{rot} E = -\alpha \frac{\partial H}{\partial t}, \quad \operatorname{rot} H = \beta \frac{\partial E}{\partial t}, \tag{1.37}$$

где E и H — напряженности электрического и магнитного поля, а коэффициенты α и β определяются выбором системы единиц. Следствием (1.37) оказывается волновое уравнение [26]

$$\alpha\beta \frac{\partial^2 E}{\partial t^2} = \frac{\partial^2 E}{\partial x^2} + \frac{\partial^2 E}{\partial y^2} + \frac{\partial^2 E}{\partial z^2}, \tag{1.38}$$

ставшее для *Максвелла* большой неожиданностью, и он в результате предположил, что электромагнитные возмущения распространяются в виде волн. Дальнейшее хорошо известно: опыты *Герца*, затем гипотеза *Максвелла* об электромагнитной

[25] «Винтовая асимметрия» окружающего мира (люди в большинстве праворуки, часы ходят по часовой стрелке, улитки одинаково закручены) — на первый взгляд порождается асимметрией внешних причин типа вращения Земли. И разное закручивание водоворотов в Северном и Южном полушариях — это наглядно подтверждает. Но почему Земля «ввинчивает буравчик» к Северному полюсу? Анализ таких цепочек причинно-следственных связей рано или поздно должен упереться в какой-нибудь асимметричный закон глубинной ниши, либо подойти к выводу о существовании другой «Земли», где преобладает леворукость.

[26] Аналогично для H.

природе света — из-за совпадения скорости распространения волн (1.38) со скоростью света, $1/(\alpha\beta) = c^2$.

В этом сюжете математика играет разве что наводящую роль. Вывод (1.38) из (1.37), опирающийся вроде бы на элементарные выкладки, уязвим с точки зрения логики. И дело вовсе не в необходимости промежуточного дифференцирования, которое может наткнуться на какую-нибудь негладкость. Каждое из уравнений (1.37) предполагает (за кадром), что в правой части стоит причина, а не следствие. Примерно как в $m\ddot{x} = F$ сила порождает ускорение, но не ускорение — силу. Это очень серьезное препятствие для свободного манипулирования уравнениями.

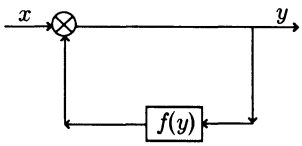


Рис. 1.1

Если предостережение кажется надуманным, имеет смысл обратиться к примерам из области бифуркаций (см., например, [3]). Динамический блок f (в дискретном времени), дающий на выходе сигнал $y[k] - y[k-1]$ при входном сигнале $y[k]$, будучи включен в обратную связь (рис. 1.1), предсказывает будущее (!): $y[k-1] = x[k]$, что вытекает из балансового соотношения

$$x[k] + y[k] - y[k-1] = y[k].$$

В таких ситуациях, чтобы удержаться в рамках дозволенного, надо переходить на более тонкое описание динамики, учитывая влияние паразитных параметров, запуск процесса и другие привходящие факторы, возможность пренебрежения которыми зависит от обстоятельств. Такая же песня возникает в связи с переходом от (1.37) к (1.38), что подтверждено может быть только экспериментом, и что вроде бы подтверждается [27]. Если теперь (1.38) принять за фундаментальный закон природы, то можно изучать его инвариантность относительно различных групп преобразований, но это будет симметрия уравнения (физического процесса), а не *физического пространства.*

[27] Если не говорить об использовании явно надуманного понятия времени, ибо время во Вселенной — не более чем математический фокус. По крайней мере, в том исполнении, которое общепринято. Разумеется, это не мешает выдвигать физические гипотезы и ставить эксперименты. Надуманность пространства спрятана чуть глубже, и дает о себе знать каждый раз при выходе за пределы привычного диапазона.

В то же время свойства модельного (математического) пространства могут служить путеводной звездой, вмещая либо не вмещая те или иные группы преобразований и фокусируя на них внимание безотносительно к описанию физических процессов. «Неуклюжесть» этих групп может свидетельствовать об ограниченности принятых точек зрения и подталкивать к расширению представлений. На стерильно математическом языке это можно интерпретировать как вложение «плохих групп в хорошие» с возможными философскими и физическими выводами [28]. При этом, как следствие, могут расти размерности, что вовсе необязательно связывать со спекуляциями о размерности реального пространства, ибо причины роста — заключаются в механизмах «вложений» и увеличении числа степеней свободы.

Например, концепция электрона как точечного заряда, движущегося в $\mathbb{R}^3$, оказалась несостоятельной еще до появления квантовой механики. Выяснилось, что электрону надо бы приписать момент количества движения (*спин*), причем модель «вращающейся пули» совершенно не годилась. Выходила странная вещь — момент есть, вращения нет. Квантовая механика кое-как увязала концы с концами, допуская возможность измерения только «±»-проекции «момента» ($\pm\hbar/2$) на избранную ось, и оставляя *спин* равномерно размазанным по другим направлениям. Таким образом, *спин* — это математический трюк, загадка Вселенной, которая движется вместе с каждым электроном. Но так или иначе, из непонятного описания — обеспечивающего все же соответствие экспериментальным данным — становится ясно, что электрон не является обыкновенным объектом в $\mathbb{R}^3$. *Уравнение Шрёдингера* пришлось модифицировать.

1.7. Парадоксы симметрии

Пузырек воздуха в стоячей воде, не испытывая на себе сил, несимметричных относительно вертикальной оси, обязан подниматься, казалось бы, строго вертикально. Но при числах *Рейнольдса* $\mathrm{R} > 50$ он движется по спирали (!), что противоречит, на первый взгляд, *принципу достаточного основания*.

Парадокс, тем не менее, копеечный. Симметрия причин должна приводить к симметрии следствий, но диапазон возможной реализации такой закономерности довольно широк. Система уравнений $\begin{cases} x+y=3, \\ xy=2 \end{cases}$ симметрична относительно

[28] Такое чаще удается, конечно, задним числом (см. раздел 1.1).

перестановки переменных, но решение $\{1, 2\}$ — несимметрично. Баланс обеспечивается наличием другого решения $\{2, 1\}$.

Это, правда, математика. В реальной физической системе пришлось бы объяснять, почему система предпочитает, скажем, $\{2, 1\}$. Такая же история возникает в связи с «пузырьком». Возможны три гипотетических решения: вертикальное всплытие и две спирали, закрученные в разные стороны. Симметрия комплекта налицо, но как система реализует конкретный выбор? Вертикальное всплытие отсеивается как неустойчивое, а лево- или правовинтовая спираль получается в результате воздействия причин, находящихся за кадром. Это может быть чистая случайность, если в экспериментах обе спирали возникают попеременно, либо глубинная причина типа асимметрии Галактики. Но в любом случае странное поведение пузырька не более удивительно, чем левостороннее расположение сердца.

Однако среди гидродинамических парадоксов [1] есть гораздо менее понятные. Скажем, *парадокс Дюбуа*, вступающий будто бы в противоречие с принципом относительности: при определенных условиях *сопротивление тела в потоке оказывается существенно меньше сопротивления при движении того же тела в той же среде, с той же скоростью*. В результате обдувание самолетов в аэродинамических трубах дает большую ошибку относительно реальных полетов в атмосфере.

Стандартные объяснения в том или ином виде ссылаются на зачатки турбулентности, которые имеет движущаяся среда. Далее обычно идет скороговорка насчет пограничного слоя, в котором «все бывает». Пограничный слой в самом деле обладает удивительными свойствами[29], но гидро- и аэродинамика слишком уж переполнены «чудесами», чтобы их объяснения каждый раз принимать за чистую монету. Тут получается та самая история, когда теоретик объясняет, почему $A > B$, а когда выясняется, что $A < B$, говорит: «это тем более понятно», и начинает рассуждать не менее убедительно в противоположно направлении. У гидродинамики наготове также есть масса инструментов и методов. Не хватает ориентиров — когда какие факторы учитывать и какие уравнения применять.

Как бы там ни было, но *парадокс Дюбуа* достаточно эффектен, чтобы лишний раз задуматься об устройстве мира. Противоречие

[29] Достаточно обратить внимание на *парадокс Эйфеля* об убывании сопротивления сферы с возрастанием скорости потока [1].

возникает как диссонанс практики с *уравнениями Навье—Стокса*, каковых, ясное дело, не хватает, чтобы уловить действующий механизм. За уравнениями, конечно, дело не станет. Их можно подобрать как для «$A > B$», так и для «$A < B$». Хорошо было бы научиться такие вещи делать заранее.

Но проблема здесь не только в отставании теории. Парадоксальностью искрит сам факт. Мировоззренческая сила принципа относительности настолько велика, что любое явление «подрывающего характера» вызывает глубинный резонанс чувств, и статус парадокса здесь, пожалуй, сохранится независимо от убедительности теоретических объяснений.

Так или иначе, соображения симметрии будоражат мысль, оказываясь тем полезнее, чем противоречивее выводы — будь то разногласия практики с теорией либо интуицией. Проблемы порождают даже элементарные ошибки. Скажем, для компенсации неравноплечности весов гирю можно один раз класть на левую чашу, другой раз — на правую. «Симметрия» манипуляций создает иллюзию, что сумма двух взвешиваний будет правильной. Продавец, однако, проигрывает, ибо $(a/b) + (b/a) > 2$ при $a \neq b$. Это тривиальный пример. Но есть более глубокие заблуждения той же природы (математической неосведомленности интуиции). Таковы многие парадоксы теории вероятностей [4, т. 4].

Помимо выявления имеющейся в задаче симметрии — мысль целесообразно направлять также в противоположном направлении симметризации задач.

Дан угол ABC и прямая MN (рис. 1.2). Надо построить квадрат, две вершины которого лежат на сторонах угла, две — на прямой.

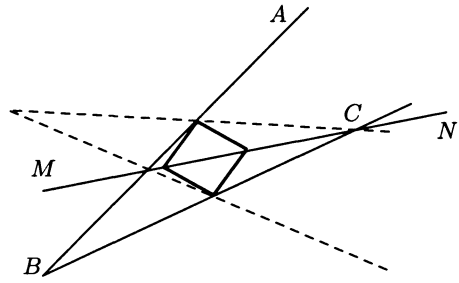


Рис. 1.2

Заметим, требуемый квадрат зеркально симметричен относительно MN. Отсюда ясно, что тот же самый квадрат решает симметричную задачу, в которой угол зеркально симметричен относительно MN. Поэтому вершины квадрата обязаны лежать в точках пересечения сторон угла ABC со сторонами пунктирного муляжа.

Подобного сорта задач рассеяно по литературе великое множество. Но идея представляется далеко не исчерпанной, особенно за пределами геометрии.

1.8. Проективная геометрия

Внутреннее чутье резонирует при столкновении с симметрией внешнего мира. Но многое все-таки остается незамеченным. Проективная геометрия позволяет вскрыть замаскированную гармонию, не данную в ощущениях. Исходные положения дисциплины достаточно просты, что приятно контрастирует с нетривиальностью выводов.

Центральное проектирование плоскости $\boldsymbol{P}$ в плоскость $\boldsymbol{P}'$ из точки O, не лежащей ни на $\boldsymbol{P}$, ни на $\boldsymbol{P}'$, заключается в сопоставлении точкам $A \in \boldsymbol{P}$ точек $A' \in \boldsymbol{P}'$, так чтобы A, A', O лежали на одной прямой [30]. *Проективное преобразование* допускает также параллельное проектирование (центр O в бесконечности).

(!) Данное определение пока с изъяном. Если плоскости $\boldsymbol{P}$ и $\boldsymbol{P}'$ не параллельны, преобразование оказывается неопределенным для некоторых точек плоскости $\boldsymbol{P}$. Точнее говоря, плоскость $\boldsymbol{P}''$, проходящая через центр O и параллельная $\boldsymbol{P}'$, — пересекается с $\boldsymbol{P}$ по прямой $\boldsymbol{L}$, и ни одна точка $\boldsymbol{L} \subset \boldsymbol{P}$ «никуда не проектируется», т. е. проектируется в бесконечность.

Поэтому прямые, лежащие в плоскости $\boldsymbol{P}$ и пересекающиеся в некоторой точке $C \in \boldsymbol{L}$, переходят в параллельные прямые на плоскости $\boldsymbol{P}'$, а параллельные на $\boldsymbol{P}$ — в пересекающиеся [31] прямые плоскости $\boldsymbol{P}'$. Выход из положения обеспечивает пополнение любой рассматриваемой плоскости *бесконечно удаленными точками*, совокупность которых (декларативно) образует *бесконечно удаленную прямую.*

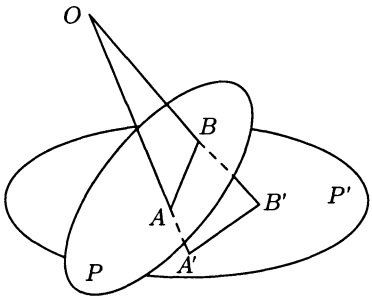


Рис. 1.3

При таком соглашении центральное проектирование переводит прямую $\boldsymbol{L}$ в бесконечно удаленную прямую пополненной

[30] При центральном проектировании прямые переходят в прямые, но параллельность может не сохраняться.

[31] В некоторой точке прямой $\boldsymbol{L}'$, по которой $\boldsymbol{P}'$ пересекается с плоскостью $\boldsymbol{P}'''$, параллельной $\boldsymbol{P}$ и проходящей через центр O.

плоскости $\boldsymbol{P}'$, а бесконечно удаленную прямую пополненной плоскости $\boldsymbol{P}$ — в прямую $\boldsymbol{L}'$. В итоге центральное проектирование становится всюду определенным и взаимно однозначным, что избавляет от исключений, создавая необходимые удобства для развития теории.

Плоскость, пополненная указанным выше образом, называется *проективной*. Располагая этим понятием, можно дать эквивалентное определение *проективного преобразования как преобразования проективной плоскости, переводящего любую прямую в прямую*. В таком варианте определения очевидно, что проективные преобразования составляют группу.

Пополнение плоскости явно фиктивными элементами заслуживает «философского внимания». Взаимоотношения бесконечно удаленной прямой с остальной атрибутикой определены и не вызывают казусов. Больше ничего не требуется. Это лишний раз подчеркивает то обстоятельство, что для «существования» в математике нужна лишь непротиворечивость.

Свойства проективных преобразований:

• Четырехугольники *проективно эквивалентны* друг другу, т. е. переходят друг в друга при подходящих преобразованиях, причем можно обеспечить любой порядок соответствия вершин.

• *Двойное отношение* $\dfrac{AC}{BC} : \dfrac{AD}{BD}$ четырех точек A, B, C, D, лежащих на одной прямой, — не меняется при проективных преобразованиях.

• Проективные преобразования, вообще говоря, не сохраняют окружностей, но любая данная окружность и не пересекающая ее прямая могут быть переведены в окружность и бесконечно удаленную прямую, а любая окружность с выделенной точкой A внутри, — может быть переведена в окружность с центром, в который переходит точка A.

Проективная геометрия богата красивыми задачами [28]. Но здесь не место для демонстраций, потому что много — не поместится, а мало — не даст представления. Поэтому ограничимся маленькой иллюстрацией самого́ принципа решения. Если взять точки, делящие стороны треугольника в отношении $1 : n$, и соединить их с вершинами, — получится фигура, изображенная на рис. 1.4.

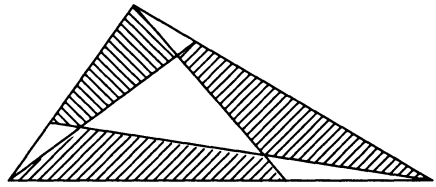


Рис. 1.4

Прямое доказательство равенства площадей заштрихованных четырехугольников — неприятная задача. В рамках проективной геометрии она тривиальна. При параллельном проектировании (центр проектирования в бесконечности) пропорции деления отрезков сохраняются, равные площади переходят в равные, а любой треугольник можно перевести в равносторонний, для которого утверждение о равенстве площадей очевидно.

В так называемой *Эрлангенской программе Ф. Клейн* предложил классификацию различных геометрий по принципу их инвариантности к различным группам преобразований. Группа движений порождает евклидову геометрию. Проективная — только что была рассмотрена. Подгруппа проективных преобразований с инвариантным коническим сечением выделяет *неевклидову геометрию Лобачевского*. Разновидности геометрий весьма многочисленны [28]. Топологию порождает группа *гомеоморфизмов*.

Глава 2

Основные понятия

2.1. Определения, примеры и авансы

К абстрактным понятиям можно двигаться исподволь, гомеопатическими шагами, но короткий путь все же — хирургический.

2.1.1. ***Группой*** G *называется конечная или бесконечная совокупность элементов, на которой задана* ***групповая операция*** «$\cdot$», *сопоставляющая любой паре элементов* $a, b \in G$ *некоторый элемент* c *из той же совокупности* G:

$$a \cdot b = c.$$

При этом групповая операция, называемая обычно умножением, обязана удовлетворять трем условиям:

- $p \cdot (q \cdot r) = (p \cdot q) \cdot r$ (*ассоциативность*) [1].
- *В группе существует единичный элемент* [2] 1, *обладающий свойством* $1 \cdot x = x \cdot 1 = x$ *для любого* $x \in G$.
- *Каждый элемент* $x \in G$ *имеет обратный* x^{-1}:

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

Понятие группы, таким образом, относится к алгебраическим структурам с одной бинарной операцией. Разнообразие возможных требований выделяет различные другие понятия. Множество с операцией, от которой требуется только ассоциативность, называется ***полугруппой***. Полугруппа с единицей — ***моноид***. Моноид, в котором каждый элемент обратим, — это уже ***группа***.

---

[1] Благодаря ассоциативности скобки в любом произведении можно убрать или, наоборот, произвольно расставить.

[2] Обозначение «1» не всегда удобно, особенно, когда единица группы участвует в рассуждениях вместе с числом 1. По этой причине для единицы в теории групп часто используется специальный знак «e», — что имеет свои минусы. Мы предпочитаем «1», допуская двоякое толкование и полагаясь на контекст.

Три аксиомы п. 2.1.1 порождают колоссальное разнообразие. Теория необозрима. Некоторые задачи принципиально не решаются[3], доказательства некоторых теорем занимают сотни страниц, а самые простые результаты плохо укладываются в голову.

Для обозначения групповой операции далее могут использоваться различные знаки ($*$, $\otimes$, $\circ$), а также отсутствие какого бы то ни было знака, как при обычном умножении. Широкий ассортимент обозначений удобен при одновременном рассмотрении нескольких групп с разными групповыми операциями. Но это в принципе. Практически целесообразно полагаться на контекст, максимально упрощая обозначения в ущерб строгости. Поэтому по мере привыкания удобнее всего знаки группового умножения опускать.

2.1.2. *Группу G, содержащую n элементов, называют* ***конечной****, а $|G| = n$ — ее* ***порядком****. Порядок $|G|$ может быть бесконечным.*

Подмножество элементов $H \subset G$, образующих группу, — при той же групповой операции, что и в G, — называется ***подгруппой***. Подгруппы — это строительные блоки, из которых собрана группа, — поэтому изучение их структуры во многом характеризует свойства группы и, как правило, находится в центре внимания.

2.1.3. Лемма. *Подмножество $H \subset G$ является подгруппой в томм*[4] *случае, если из $a, b \in H$ следует $ab^{-1} \in H$.*

◀ В случае $a = b$ получаем $aa^{-1} = 1 \in H$. Далее,

$$a \in H \Rightarrow 1 \cdot a^{-1} = a^{-1} \in H.$$

Наконец, $a, b \in H \Rightarrow ab = a(b^{-1})^{-1} \in H$. ▶

2.1.4. Лемма. *Подмножество $H \subset G$ является подгруппой в томм случае, если*

$$a, b \in H \Rightarrow ab \in H \quad \text{и} \quad a \in H \Rightarrow a^{-1} \in H.$$

Групповое произведение $x * \ldots * x$ с n сомножителями обозначают как x^n, полагая $x^0 = 1$. Очевидно, $x^m * x^n = x^{m+n}$. Группа G, в которой все элементы могут быть получены путем последователь-

[3] *Проблема тождества слов*, например.

[4] См. «Обозначения».

ного возведения в степень одного элемента a,

$$G = \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots, a^n, \ldots\},$$

называется ***циклической***.

• Если все степени a^k $(k \geqslant 0)$ различны, группа G бесконечна. Если же $a^k = a^q$, $k < q$, то $a^{q-k} = 1$. Фиксировав наименьший положительный показатель, при котором $a^n = 1$, легко приходим к выводу, что группа G исчерпывается степенями

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

которые все различны, причем для $m = sn + r$ $(0 \leqslant r < n)$

$$a^m = a^r. \quad (?)$$

• Если циклическая группа конечна, то среди $a, a^2, \ldots, a^{n-1}$ обязательно есть a^{-1}. В бесконечной циклической группе ни одна из положительных степеней a^k не совпадает с a^{-1}. Поэтому иногда говорят, что бесконечная циклическая группа имеет две образующих: a и a^{-1}.

В общем случае минимальное n в равенстве $b^n = 1$ называют ***порядком*** или ***периодом*** элемента b и обозначают через $|b|$. В случае $b^n \neq 1$ при любом $n > 0$ — считают $|b| = \infty$.

Если порядки всех элементов группы G (кроме единичного) бесконечны, — говорят, что G — ***группа без кручения***. Если же порядки всех элементов группы конечны, группу называют ***периодической***.

Упражнения

При первоначальном знакомстве с предметом решение упражнений необходимо по разным причинам: от привыкания к объекту до запоминания хотя бы части терминов.

• Для любых элементов группы: $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

• К групповой операции достаточно предъявить два требования: ассоциативность и разрешимость уравнений

$$a \cdot x = b, \quad y \cdot a = b,$$

при любых $a, b \in G$. Получится эквивалентное определение группы.

• В исходном определении достаточно требовать существования левой единицы и правой: $1_l \cdot x = x$, $x \cdot 1_r = x$. Равенство $1_l = 1_r$ вытекает из ассоциативности групповой операции.

• Конечная группа порядка N является циклической в том случае, когда в ней есть элемент порядка N.

• Всякая группа простого порядка — циклическая.

• Всякая подгруппа циклической группы есть снова циклическая группа.

• Подгруппы циклической группы порядка n находятся во взаимно однозначном соответствии с делителями n.

• Совокупность всех степеней любого элемента $g \in G$ является циклической подгруппой $\{g\}$ группы G, $|\{g\}| = |g|$.

• Если g_α при изменении α пробегает все элементы группы G и g_0 произвольный элемент G, то $g_0 \cdot g_\alpha$ (рáвно как и $g_\alpha \cdot g_0$) также пробегает все элементы группы.

• Если элементы a, b перестановочны, $a \cdot b = b \cdot a$, то $|a \cdot b| = |a| \cdot |b|$.

• Если элементы a, b перестановочны и $|a| = m$, $|b| = n$, то в группе всегда есть элемент — не обязательно равный произведению $a \cdot b$, — порядок которого совпадает с наименьшим общим кратным чисел m и n.

• Любая конечная группа G четного порядка имеет элемент 2-го порядка.

◄ Подмножества $\{g, g^{-1}\} \subset G$ имеют не по два элемента, а по одному, если либо $g = 1$, либо $g^2 = 1$. Далее остается заметить, что G представляет собой объединение подмножеств $\{g, g^{-1}\}$. ►

Групповую операцию, как уже отмечалось, называют *умножением*, и часто вообще обходятся без знака. Это соответствует *мультипликативной точке зрения*. Для ***абелевых*** (*коммутативных*) *групп*, в которых, по определению, $a \cdot b = b \cdot a$, обычно используется *аддитивная терминология*. Групповая операция при этом называется *сложением* и обозначается знаком $+$, а единицу именуют нулем.

Перемена точки зрения, технически равноценная, все же меняет освещение предмета, в результате чего некоторые результаты интуитивно ясны в мультипликативной аранжировке, некоторые — в аддитивной. За этим интересно проследить в процессе освоения теории групп. Это хороший пример, показывающий насколько заблуждения и прозрения зависят от ассоциаций, вызываемых обозначениями.

Примеры групп:

• Положительные рациональные числа (без нуля) по отношению к операции умножения.

• Группа целых чисел $\mathbb{Z}$ по отношению к сложению.

• $\mathbb{R}^n$ по отношению к сложению векторов.

• Совокупность невырожденных матриц по отношению к матричному умножению.

• Множество «самосовмещений» тетраэдра (куба, октаэдра, икосаэдра, додекаэдра) по отношению к последовательному выполнению преобразований (вращений, отражений).

• Совокупность верхних (нижних) треугольных матриц *с ненулевыми элементами диагонали*:

$$\begin{bmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ 0 & t_{22} & \dots & t_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & t_{nn} \end{bmatrix}, \qquad \left(\begin{bmatrix} t_{11} & 0 & \dots & 0 \\ t_{21} & t_{22} & \dots & \dots \\ \dots & \dots & \dots & 0 \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{bmatrix} \right).$$

Произведение треугольных матриц одного типа — есть треугольная матрица того же типа. Обратная к треугольной — тоже треугольная матрица, соответственно, верхняя или нижняя.

• Совокупность функций

$$x,\ \frac{1}{x},\ 1-x,\ \frac{1}{1-x},\ \frac{x}{1-x},\ \frac{1-x}{x}$$

по отношению к композиции. (**?**)

• **Аддитивная группа $\mathbb{Z}_p^+$ вычетов по модулю p**, где p простое число. Ее элементами являются числа $0, 1, 2, \dots, p-1$, а групповое произведение $a \circ b$ равно остатку от деления обычной суммы $a+b$ на p, т. е.

$$a \circ b = a + b \pmod{p}.$$

Проверка групповых свойств тривиальна. Единицей группы служит нуль.

• **Мультипликативная группа $\mathbb{Z}_p^\times$ вычетов по модулю p**, где p простое число. Ее элементами являются $p-1$ чисел $1, 2, \dots, p-1$,

а групповое произведение $a * b$ равно остатку от деления обычного произведения ab на p, т. е.

$$a * b = ab \pmod{p}.$$

Группа $\mathbb{Z}_p^\times$, очевидно, абелева. Проверка групповых свойств связана с некоторыми хлопотами.

◄ Первые две аксиомы группы очевидны. Ассоциативность ясна, поскольку $a * b * \ldots * h$, как и в случае двух сомножителей, равно остатку от деления обычного произведения $ab \ldots h$ на p. Обоснование третьей аксиомы (существование обратного элемента) — не так просто.

Единица обратна сама себе. Далее надо доказать, что любое число x из $\{2, \ldots, p-1\}$ имеет обратное. Рассмотрим p целых чисел,

$$x, x^2, \ldots, x^p.$$

Ни одно из этих чисел не делится на p, поскольку p простое, а $x < p$. Разделив каждое x^k на p, получим p остатков, строго меньших p. Поэтому хотя бы два числа, скажем x^n и x^m, при делении на p дают один и тот же остаток. Поэтому[5)]

$$x^n - x^m = x^m \left(x^{n-m} - 1\right) = 0 \pmod{p},$$

а так как $x^m \neq 0 \pmod{p}$, то $x^{n-m} - 1 = 0 \pmod{p}$.

Пусть y обозначает остаток от деления числа x^{n-m-1} на p, т. е.

$$x^{n-m-1} = y \pmod{p}.$$

Умножая обе части последнего равенства (*сравнения*) на x, получаем

$$x^{n-m} = xy \pmod{p}.$$

Но, как уже показано, x^{n-m} при делении на p дает в остатке единицу. Следовательно, $xy = 1 \pmod{p}$. Поэтому $y = x^{-1}$. ►

Посмотрим теперь, какие отсюда можно извлечь дивиденды. *Если некоторая группа имеет порядок n, то любой ее элемент k, «умноженный» n раз сам на себя, обязательно дает единичный элемент.* Это известный в теории групп результат[6)]. Применяя его к группе $\mathbb{Z}_p^\times$, в которой $p-1$ элементов, получаем:

$$k * \ldots * k = 1,$$

[5)] Запись $x = a \pmod{p}$ означает: «x при делении на p дает в остатке $a < p$». Если же $a \geqslant p$, то $x = a \pmod{p}$ подразумевает: «x и a при делении на p дают одинаковый остаток».

[6)] См. далее — теорема 2.3.2. Факт, между прочим, достаточно прост для упражнения.

где $p-1$ сомножителей, что означает делимость $k^{p-1}-1$ на p, и называется **малой теоремой Ферма**.

Другая жемчужина теории чисел — **теорема Вильсона**: *если p простое число, то $(p-1)!+1$ делится на p.*

◄ Пусть $k \in G_p$. Если $k * k = 1$, то $k^2 - 1 = (k-1)(k+1)$ делится на p. А так как $1 \leqslant k \leqslant p-1$, то либо $k = 1$, либо $k = p-1$. Поэтому среди

$$2, 3, \ldots, p-2$$

нет элементов, которые являются обратными сами себе. Таким образом, все элементы $2, 3, \ldots, p-2$ разбиваются на пары взаимно обратных. Поэтому

$$2 * 3 * \cdot * (p-2) = 1.$$

Отсюда

$$1 * 2 * \cdot * (p-1) = p-1.$$

Но это и есть *теорема Вильсона*[7]. ►

(!) *Приведенные доказательства можно «переложить» на арифметический язык, избавившись от групповой идеологии. И это не так уж сильно удлинит рассуждения. Однако доказательства превратятся в рецепты, которые работают, но не ясно — почему*[8]. *В этом, собственно, и заключена главная выгода стерилизации задач от числовой специфики. Плюс к тому, как только становится ясно, что объект изучения является группой, к анализу подключается арсенал готовых инструментов и результатов.*

2.2. Группа подстановок

Группы подстановок играют ключевую роль при изучении конечных групп, поскольку *других конечных групп не бывает.* Точнее говоря, *конечные группы с точностью до изоморфизма исчерпываются подгруппами группы подстановок* (***теорема Кэли***). Рассмотрение предмета обычно начинается с *перестановок* (не подстановок), что создает в головах некоторую путаницу.

[7] Результат не так прост, как видится с групповой точки зрения. Теорему впервые опубликовал *Варинг* со ссылкой на *Вильсона*. Высказана она была в виде гипотезы. Лишь через некоторое время доказательство удалось найти *Лагранжу*.

[8] Что не там страшно, где уже доказано, а там — где только предстоит.

Стандартный способ описания *перестановок* n предметов сводится нумерацией к перестановкам чисел от 1 до n. Результаты записываются в виде строк $(j_1\ j_2\ \dots\ j_n)$.

Все $n!$ перестановок из n символов можно расположить в таком порядке, что каждая следующая перестановка будет получаться из предыдущей одной *транспозицией*[9]. (**?**) (Стандартное доказательство получается с помощью индукции.)

Запись одной ***перестановки*** под другой,

$$\sigma = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \tag{2.1}$$

определяет ***подстановку***[10], при которой каждое j_k переходит в i_k. Порядок записи столбцов в (2.1), разумеется, не играет роли.

Произведение (композиция) подстановок $\sigma_1 \cdot \sigma_2$ определяется как последовательное применение σ_2, потом σ_1. Множество $\mathbf{S}_n$ *всех* подстановок вида (2.1) с композицией в качестве групповой операции — называется *симметрической группой n-й степени*, $|\mathbf{S}_n| = n!$, единица группы — тождественная подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$. Обратной к (2.1) является подстановка

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Любые *группы подстановок являются подгруппами* $\mathbf{S}_n$. Вместо $\mathbf{S}_n$ иногда удобнее говорить об изоморфной группе отображений $\mathrm{Sym}(G)$, $n = |G|$, где за кадром подразумеваются перестановки элементов группы G, а не чисел $1, \dots, n$, — изоморфизм достигается нумерацией элементов группы.

Циклической подстановкой (*циклом*) $(i_1 i_2 \dots i_k)$ *длины* k называется подстановка, переводящая i_1 в i_2, i_2 в i_3, ..., i_{k-1} в i_k,

[9] *Транспозиция* меняет местами два символа, «не трогая» остальных.

[10] Разница, таким образом, заключена в следующем. *Перестановка* — это результат упорядочения предметов, *подстановка* — это преобразование, переводящее одну перестановку в другую.

наконец, i_k в i_1. Цикл все равно откуда начинать. Поэтому, например [11],

$$(i_1 i_2 \dots i_k) = (i_2 \dots i_k i_1).$$

Любая подстановка (2.1) представи́ма в виде произведения циклов. Для этого достаточно взять любое число j_1, посмотреть, в какое j_2 оно переводится, затем выяснить, во что переходит j_2, и так далее до тех пор, пока не встретится j_q, переходящее в j_1. В результате выделяется сомножитель (цикл)

$$(j_1 j_2 \dots j_q).$$

Затем среди $1, \dots, n$ берется любое число, не входящее в найденные уже циклы, и повторяются прежние манипуляции. И так — до исчерпания всех чисел $1, \dots, n$. В результате, например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 2 & 3 & 1 & 4 & 5 & 8 \end{pmatrix} = (175)\,(2643)\,(8).$$

Восьмерка в данном случае просто остается на месте. Циклы, понятное дело, получаются непересекающимися, и потому их произведение не зависит от порядка сомножителей.

Любой цикл представи́м в виде произведения *транспозиций* — *циклов длины* 2, что следует из

$$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k).$$

Это еще раз доказывает, что любая подстановка представи́ма произведением *транспозиций*.

Четность перестановок и подстановок. Будем говорить, что два числа в перестановке образуют *беспорядок*, если большее число стоит впереди меньшего. Перестановка называется *четной* (*нечетной*), если число беспорядков [12] в ней четно (нечетно).

Заметим теперь, что любая подстановка (2.1) в результате подходящей перестановки столбцов всегда может быть записана в стан-

[11] В принципе, цикл было бы «правильно» изображать в виде чисел, записанных по кругу. Но «правильные» пути не всегда удобны.

[12] Для определения суммарного числа *беспорядков* числа просматриваются в порядке записи, для каждого числа подсчитывается, сколько чисел, меньших данного, стоит правее, — и все результаты складываются.

дартном виде

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \tag{2.2}$$

в результате чего между *подстановками* и *перестановками* устанавливается взаимно однозначное соответствие — по второй строке (2.2). Соответственно, подстановки делятся на *четные* и *нечетные*.

Всякая подстановка разлагается в произведение транспозиций, причем — разными способами. Однако *число транспозиций в представлении четной (нечетной) подстановки — обязательно четно (нечетно)*. **(?)**

В симметрической группе $\mathbf{S_n}$ подгруппу $\mathbf{A_n}$ всех четных подстановок называют *знакопеременной группой* степени n. Нечетные подстановки группу не образуют.

Группа подстановок G называется *транзитивной*, если для любых двух ее элементов i, j найдется подстановка из G, переводящая i в j. Транзитивность является принципиальным понятием, которое часто подразделяет изучаемые явления на «удобные» и «неудобные».

Если, в случае простого n, транзитивная группа $G \subset \mathbf{S_n}$ содержит хотя бы одну транспозицию, то $G = \mathbf{S_n}$. **(?)**

2.3. Смежные классы

Если H подгруппа группы G, то множество элементов

$$g_1 \cdot H = \{g_1 h : h \in H\}, \quad g_1 \in G, \quad \text{но} \quad g_1 \notin H,$$

не пересекается с H.

◄ В противном случае нашлись бы элементы $h', h'' \in H$, такие что

$$g_1 \cdot h' = h''.$$

Но тогда $g_1 = h'' \cdot (h')^{-1}$, что противоречит предположению $g_1 \notin H$. ►

Аналогично проверяется, что $g_2 \cdot H$ — при условии $g_2 \notin H$, $g_2 \notin g_1 \cdot H$, — не пересекается ни с H, ни с $g_1 \cdot H$.

Продолжая этот процесс до исчерпания всех элементов *конечной* группы, получим разбиение G на p непересекающихся совокупностей:

$$H, \quad g_1 \cdot H, \quad g_2 \cdot H, \quad \ldots, \quad g_{p-1} \cdot H. \tag{2.3}$$

Число p называют ***индексом подгруппы*** H. Распространено обозначение $p = |G : H|$. В силу взаимной однозначности

$$gH \leftrightarrow Hg^{-1},$$

индекс $|G : H|$ не зависит от того, какие смежные классы имеются в виду, левые или правые.

Из (2.3) вытекает

$$|G| = p\,|H|, \quad \text{т. е.} \quad |G| = |H| \cdot |G : H|,$$

что влечет за собой справедливость следующего результата.

2.3.1. Теорема Лагранжа. *Порядок любой подгруппы конечной группы является делителем порядка группы.*

Теорема Лагранжа обращается лишь частично. Если простое p делит порядок группы $n = |G|$, то в G есть элемент порядка p (*теорема Коши*), а если p^k делит $n = |G|$, то G имеет подгруппу порядка p^k (см. *теоремы Силова*). Группа порядка 12 обязана иметь подгруппу четвертого порядка, но не шестого.

Следствие теоремы 2.3.1: *группа простого порядка не имеет нетривиальных подгрупп* [13], *и является циклической* [14].

2.3.2. ***Теорема.*** *Любой элемент a любой конечной группы G произвольного порядка $n = |G|$ — удовлетворяет условию* $\boxed{a^n = 1}$.

◀ Пусть элемент $a \in G$ имеет порядок $q = |a|$, что означает $a^q = 1$, причем $H = \{a, a^2, \ldots, a^q\}$ — подгруппа G. Поэтому $n = pq$. В итоге

$$a^n = (a^q)^p = 1. \quad \blacktriangleright$$

[13] Кроме $\{1\}$ и самой себя.

[14] В противном случае нашелся бы элемент $a \in G$, такой что $a^q = 1$, $q < |G|$. Но тогда бы у G была нетривиальная подгруппа $\{a, a^2, \ldots, a^q\}$.

Из теоремы 2.3.2, кстати, следует $a^{-1} = a^{n-1}$ для любого $a \in G$, при условии $|G| = n$.

Множества $g_k \cdot H$ в (2.3) называют ***левыми смежными классами*** по подгруппе H. Аналогично определяются ***правые смежные классы***, как $H \cdot g_k$. Ни один смежный класс, кроме самой подгруппы H, не образует группу, поскольку не содержит единичного элемента. В коммутативных (абелевых) группах левые и правые смежные классы, разумеется, совпадают. Но подобное совпадение встречается и в некоммутативном случае (см. *инвариантные подгруппы*), что, собственно, и составляет наименее тривиальную часть теории.

Для интуитивного усвоения понятия смежных классов естественно опираться на примеры. Один из относительно привычных вариантов — линейные пространства с операцией сложения векторов. Линейное пространство X разбивается на *классы смежности* по линейному многообразию $H \subset X$ следующим образом. Считается, что два элемента принадлежат одному и тому же классу, если и только если $x_1 - x_2 \in H$. Два класса смежности либо совпадают, либо не пересекаются.

Если X плоскость, H прямая (проходящая через нуль), то классы смежности это прямые в плоскости X, параллельные H.

Сразу имеет смысл вспомнить, как в функциональном анализе сюжет развивается дальше. Совокупность всех классов смежности образует *фактор-пространство* X/H, наделяемое структурой линейного пространства следующим образом. Если классы L_1 и L_2 имеют представителями x_1 и x_2, то суммой $L_1 + L_2$ объявляется класс, которому принадлежит элемент $x_1 + x_2$. Размерность фактор-пространства X/H (конечная или бесконечная) называется *коразмерностью*, или *дефектом*, подпространства H в X.

При изучении линейных операторов в *банаховом пространстве* E это некоторым образом «выстреливает». Рассматривается *ядро* $\ker A$, или *нуль-пространство* оператора A, — представляющее собой множество элементов x, для которых $Ax = 0$, — и *образ* R_A: множество элементов $y = Ax$. Далее вводится фактор-пространство $\operatorname{coker} A = E/\mathrm{R}_A$, называемое *коядром* оператора A, и т. п.

Комментарий из [4, т. 5]: «Конечно, все эти „керы“ и „кокеры“ не способствуют популярности математики, но здесь надо понимать, что это не более чем торжественная терминология для простых, хотя и непривычных понятий. Да и нужны они по большому счету лишь на той стадии, когда тяга к функциональному анализу становится хронической» — здесь должен быть поправлен. В теории групп «*фактор-конструкции*» играют стержневую роль.

2.4. Нормальные делители и фактор-группы

Совокупность элементов

$$g^{-1} \cdot h \cdot g,$$

где h пробегает все элементы подгруппы $H \subset G$, а g фиксированный элемент группы G, — является подгруппой [15], как говорят, ***подобной***, или ***сопряженной***, подгруппе H.

2.4.1. *Если все подобные H подгруппы совпадают с самой H, т. е. при любом $g \in G$*

$$g^{-1} \cdot H \cdot g = H, \tag{2.4}$$

*то H называют **инвариантной подгруппой**, или **нормальным делителем** группы G, или просто **нормальной** подгруппой, — и пишут* [16] $H \lhd G$.

Заметим, что (2.4) равносильно требованию

$$g \cdot H = H \cdot g, \tag{2.5}$$

т. е. левые смежные классы по инвариантной подгруппе обязаны совпадать с правыми.

Если H — нормальная подгруппа группы G, то запись

$$x = y \pmod{H}, \quad x, y \in G,$$

означает, что x и y лежат в одном и том же смежном классе [17] по H. В частности, $x = 0 \pmod{H} \Rightarrow x \in H$ (подразумевается *аддитивная интерпретация*).

• Пусть G — группа невырожденных $n \times n$ матриц, $H \subset G$ — подгруппа матриц, имеющих детерминант, равный 1. Поскольку

$$|C^{-1}AC| = |C^{-1}| \cdot |A| \cdot |C| = 1, \quad A \in H, \quad C \in G,$$

[15] Проверяется элементарно.

[16] Употребляется также обозначение $H \trianglelefteq G$. Но равенство $H = G$ мы допускаем и в том и в другом случае.

[17] Это равносильно требованию $x, y \in G \Rightarrow xy^{-1} \in H$ (либо $x - y \in H$ в аддитивной интерпретации). Факт — в русле леммы 2.1.3.

подгруппа H инвариантна. Смежные классы по H состоят из всех матриц с одинаковым определителем.

• Пусть

$$H = \left\{ \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix} : z \in \mathbb{Z} \right\}$$

— подгруппа[18] матриц из группы $G = \mathbf{SL}_2(\mathbb{Q})$. Пусть $g = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$. Тогда

$$g \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix} g^{-1} = \begin{bmatrix} 1 & 3z \\ 0 & 1 \end{bmatrix}.$$

Поэтому $gHg^{-1} \subset H$, но $gHg^{-1} \neq H$.

• Подгруппа матриц

$$\left\{ \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix} : z \in \mathbb{Q} \right\}$$

— нормальна в группе

$$\left\{ \begin{bmatrix} u & v \\ 0 & w \end{bmatrix} : u, v, w \in \mathbb{Q} \right\}. \quad \textbf{(?)}$$

Пусть H — инвариантная подгруппа G. Произведение смежных классов[19] $f \cdot H$ и $g \cdot H$ — определяется естественным образом как

$$(f \cdot H) \cdot (g \cdot H) = f \cdot (H \cdot g) \cdot H = (f \cdot g) \cdot H,$$

в силу (2.5) и очевидного $H \cdot H = H$. Таким образом, произведение смежных классов снова дает смежный класс. Кроме того, $(g \cdot H) \cdot (g^{-1} \cdot H) = H$. Следовательно, совокупность смежных классов по инвариантной подгруппе H является группой, которую называют ***фактор-группой*** и обозначают как G/H. Из вышесказанного ясно, что единицей G/H служит подгруппа H. В случае $|G| < \infty$ порядок G/H равен индексу группы H.

Группа, не имеющая нетривиальных инвариантных подгрупп[20], называется ***простой***. Простые группы наиболее сложны для изучения, поскольку представляют собой как бы единый клубок, в котором невозможно выделить структурные части.

---

[18] Фактически H изоморфна группе $\mathbb{Z}$.

[19] В силу инвариантности — неважно каких, левых или правых.

[20] Тривиальными являются единичная подгруппа и сама группа.

Нормальные группы и сопутствующие понятия, играющие в теории групп ключевую роль, требуют освоения и осмысления, каковых можно достичь только размышлением над задачами.

• Если H и J — подгруппы G, то множество

$$HJ = \{hj : h \in H,\ j \in J\}$$

не обязано быть подгруппой. Но если одна из подгрупп H, J — нормальна, то HJ — подгруппа G. А если обе H и J — нормальны, то HJ — нормальная подгруппа. (?)

• Если подгруппа $F \subset G$ содержит *нормальную подгруппу* $N \subset G$, т. е.

$$N \subset F \subset G, \tag{2.6}$$

то N нормальна также в F. Но если в цепочке (2.6) F — нормальный делитель G, а N — нормальный делитель F, подгруппа N не обязана быть нормальной в G. (?)

• Всякая подгруппа индекса 2 — нормальна.

◄ В силу $|G : N| = 2$ есть только два смежных класса: сама подгруппа $N \subset G$ и, скажем, левый класс gN, где $g \notin N$. Тогда правый смежный класс Ng либо совпадает с N (чего не может быть), либо совпадает с gN, что и реализуется, завершая доказательство. ►

• Если $N \subset G$ — нормальная подгруппа группы G индекса n, то $g^n \in N$ для любого $g \in G$.

◄ Поскольку фактор-группа G/N имеет порядок n, то $(gN)^n = 1$ для любого $g \in G$. Далее «выстреливает» нормальность N:

$$(gN)^n = g^n N \ \Rightarrow\ g^n \in N. \quad ►$$

• Пересечение нормальных делителей является нормальным делителем.

• Всякая подгруппа абелевой группы является нормальным делителем.

• Если U, V нормальные подгруппы G, и $U \bigcap V = \{1\}$, то $uv = vu$ для любых $u \in U$, $v \in V$. (?)

2.5. Классы сопряженных элементов

Элементы x и y при условии $y = gxg^{-1}$ для некоторого $g \in G$, называют ***сопряженными***. Множество x^G всех сопряженных x элементов называют ***классом сопряженных элементов***,

$$x^G = \{gxg^{-1} : g \in G\}.$$

Подгруппа $H \subset G$ нормальна в **томм** *случае, когда она является объединением классов сопряженных элементов, т. е. когда H вместе с каждым своим элементом x содержит все элементы, сопряженные x.*

• В абелевой группе любой класс сопряженных элементов состоит из одного элемента.

• В $\mathbf{S}_n$ подстановки сопряжены в **томм** случае, когда они имеют одинаковую циклическую структуру. Подстановки

$$P = (i_1 i_2 \ldots)(j_1 j_2 \ldots)(\ldots)\ldots,$$
$$P' = (i'_1 i'_2 \ldots)(j'_1 j'_2 \ldots)(\ldots)\ldots$$

с циклами одинаковой длины, выписанными друг под другом, сопрягаются с помощью подстановки

$$Q = \begin{pmatrix} i_1 & i_2 & \ldots & j_1 & j_2 & \ldots \\ i'_1 & i'_2 & \ldots & j'_1 & j'_2 & \ldots \end{pmatrix},$$

что легко проверяется.

В частности, подстановки (12)(345) и (24)(513) сопряжены в $\mathbf{S}_5$.

• Матрицы сопряжены в **томм** случае, когда приводятся к одинаковой жордановой форме.

2.6. Автоморфизмы и гомоморфизмы

Прикладной потенциал теории групп тривиален до гениальности. *При изучении объекта полезно следить за группой его автоморфизмов, т. е. преобразований, на которые объект «не реагирует»* [21]. Но обо всем по порядку.

Две группы G и G' называются *изоморфными*, если между их элементами можно установить взаимно однозначное соответствие $\varphi : G \to G'$, такое что [22]

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{2.7}$$

Изоморфные группы *эквивалентны*, $G \sim G'$, с точки зрения их групповых свойств, хотя природа элементов и операций может

[21] Что можно сказать о человеке, на которого не влияет повышение в должности, и который «не совершит большой подлости при малой выгоде»?

[22] Равенство (2.7) было бы корректнее писать в виде $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$, где точка обозначает умножение в G, а «$\circ$» — в G'.

быть различна[23]. Изоморфное отображение группы на себя называется *автоморфизмом*. Автоморфизмы $G \to G$ образуют ***группу автоморфизмов***, обозначаемую $\mathrm{Aut}\, G$.

Если в данном выше определении изоморфизма отображение $\varphi : G \to G'$ не обязательно обратимо, но по-прежнему удовлетворяет условию (2.7), — то говорят о *гомоморфном* отображении группы G в G', а φ называют ***гомоморфизмом***[24].

Сюръективный (накрывающий) гомоморфизм $\varphi : G \to G'$, отображающий G *на* G', называется ***эпиморфизмом***, а всякое гомоморфное отображение группы *в себя*, — ***эндоморфизмом***. Терминология слишком пестра, чтобы ее сразу всю запоминать, но *изоморфизм*, *автоморфизм* и *гомоморфизм* желательно расположить в памяти «на виду».

Упражнения

• Гомоморфный образ подгруппы является подгруппой.

• Гомоморфизм $\varphi_f(g) = f^{-1} \cdot g \cdot f$ при любом фиксированном f является автоморфизмом. Совокупность $\{\varphi_f\}$ образует ***группу*** так называемых ***внутренних автоморфизмов*** $\mathrm{Int}\, G$.

• Изоморфизм сохраняет все групповые свойства. Гомоморфизм может кое-что терять, преобразуя, например, группу без кручения в периодическую, либо некоммутативную группу в коммутативную. Конечность, коммутативность, цикличность — сохраняются при любом гомеоморфизме.

При гомоморфном отображении G в G' единица в G переходит в единицу группы G'. Совокупность всех элементов из G, переходящих в единицу группы G', называется *ядром гомоморфизма* $\varphi : G \to G'$ и обозначается как $\ker \varphi$.

> *Гомоморфизмы играют в теории групп ключевую роль, в связи с чем требуют к себе пристального внимания.*

[23] Группы вращений куба и октаэдра — изоморфны.

[24] При гомоморфизме различные элементы из G могут переходить в один элемент группы G'.

Если $H \subset G$ — нормальная подгруппа, то преобразование каждого элемента $g \in G$ в смежный класс $g \cdot H$ является гомоморфным отображением G на фактор-группу G/H, которое называется ***естественным гомоморфизмом*** G на G/H. Ядром этого гомоморфизма служит подгруппа H.

2.6.1. Теорема о гомоморфизме. *Если гомоморфизм φ отображает G на G', то $H = \ker\varphi$ — инвариантная подгруппа в G, а группа G' изоморфна фактор-группе G/H.*

◀ Покажем сначала, что ядро гомоморфизма обязано быть инвариантной подгруппой. Это вытекает из импликации [25]:

$$h \in H \quad \Rightarrow \quad \varphi(g^{-1}hg) = \varphi(g^{-1}) \circ \varphi(h) \circ \varphi(g) = \varphi^{-1}(g) \circ \varphi(g) = 1',$$

т. е. $g^{-1}hg$ при любом g также принадлежит H.

Рассмотрим далее отображение $\omega : G/H \to G'$, работающее по правилу:

$$\omega(xH) = \varphi(x).$$

Легко проверяется, что ω — искомый изоморфизм G/H на G'. Действительно, $\varphi(x) = \varphi(y)$ влечет за собой $\omega(xH) = \omega(yH)$, т. е. ω в самом деле отображает $G/H \to G'$. Ясно также, что ω сохраняет умножение и отображает *на*. Далее, $\varphi(x) = \varphi(y) \Rightarrow x^{-1}y \in H$, поэтому ω *инъективно* (взаимно однозначно). ▶

Таким образом, *с точностью до изоморфизма естественные гомоморфизмы исчерпывают все гомоморфизмы группы.* Доказательство теоремы 2.6.1 показывает, что любой гомоморфизм $\varphi : G \to G'$ есть композиция

$$\boxed{\varphi = \omega \circ \nu,}$$

где ν — естественный гомоморфизм, ω — изоморфизм.

2.6.2. Теорема о соответствии. *Пусть гомоморфизм φ отображает G на G'; $H = \ker\varphi$; и $\mathcal{K} = \{K : H \subset K \subset G\}$ обозначает совокупность всех подгрупп $K \subset G$, содержащих H. Тогда соответствие $K \leftrightarrow \varphi(K)$ является биекцией [26] между $\mathcal{K}$ и всеми подгруппами G'.*

---

[25] $1'$ обозначает единицу группы G'.

[26] *Биекцией* называется *взаимно однозначное отображение «на»*, т. е. инъективное и одновременно сюръективное преобразование $X \to X$, множество которых обозначают $\mathrm{Sym}(X)$.

При этом соответствующие друг другу группы одновременно нормальны, а фактор-группы по ним — изоморфны, т. е.

$$H \subset K \lhd G \quad \Leftrightarrow \quad \varphi(K) \lhd G', \quad G/K \sim G'/\varphi(K).$$

◀ Прообраз $\varphi^{-1}(K')$ любой подгруппы $K' \subset G'$ содержит H, поскольку $\varphi^{-1}(1) = H$. Поэтому $\varphi^{-1}(K') \in \mathcal{K}$. Далее, в предположении

$$K' \neq K'', \quad \varphi(K') = \varphi(K''), \tag{2.8}$$

по любому $x \in K'$ можно указать такое $y \in K''$, что $\varphi(x) = \varphi(y)$, т. е.

$$\varphi(x)\varphi^{-1}(y) = 1 \quad \Rightarrow \quad \varphi(xy^{-1}) = 1,$$

откуда

$$xy^{-1} \in H \subset K'' \quad \Rightarrow \quad K' \subset K''.$$

Аналогично устанавливается $K'' \subset K'$, что в итоге обеспечивает равенство $K' = K''$ и приводит к противоречию с (2.8). Тем самым доказано, что соответствие $K \to \varphi(K)$ является биекцией, т. е. взаимно однозначным «отображением на».

Покажем теперь одновременную нормальность K и $\varphi(K)$. Если $K \lhd G$, то

$$gKg^{-1} = K \quad \Rightarrow \quad \varphi(g)\varphi(K)\varphi(g^{-1}) = \varphi(K).$$

А поскольку $\varphi(G) = G'$, то когда g пробегает всю группу G, $\varphi(g)$ пробегает всю группу G', что гарантирует нормальность $\varphi(K)$.

Изоморфность фактор-групп устанавливается с помощью вспомогательного эпиморфизма $\xi : G \to G'/\varphi(K)$, определяемого как $\xi(g) = \varphi(g)\varphi(K)$. Легко проверяется $K = \ker \xi$, откуда по теореме 2.6.1 $G/K \sim G'/\varphi(K)$. ►

Гомоморфизмы в теории групп применяются весьма часто, причем в большинстве случаев использование инструмента носит тривиальный характер, — но требует привычки. Вот элементарный пример.

2.6.3. Теорема Кэли. *Любая конечная группа G изоморфна некоторой подгруппе симметрической группы подстановок $\mathbf{S}_n$, где $n = |G|$.*

◀ Введем отображения $\gamma_a : G \to G$, сопоставляющие любому $x \in G$ элемент ax (левое умножение на a). Легко видеть, что γ_a составляют группу (?), причем $\gamma_1(x) \equiv x$, откуда следует, что преобразование $a \mapsto \gamma_a(x)$ есть гомеоморфизм $G \to \mathrm{Sym}(G)$. Далее остается лишь пронумеровать элементы группы G, чтобы перейти от $\mathrm{Sym}(G)$ к $\mathbf{S}_n$. ►

Тривиальный характер многих доказательств в теории групп часто порождает двойственное чувство. Изначально — «не ясно, как

подступиться», потом — «зачем было ломать копья». Причина в том, что без привычки не ясно, «как это делается».

Однако надо признать, что выработать привычку не так легко, поскольку область неудобна для подсознания. Обычный рецепт выделения какого-либо наглядного примера в качестве эталона здесь плохо работает. Скажем, подстановки достаточно просты и наглядны вроде бы, — но законы, управляющие ими, включают все сложности теории конечных групп. Поэтому оптимизм в связи с теоремой Кэли быстро тает при столкновении с действительностью.

2.7. О роли инвариантов

Роль инвариантов подчеркивалась в главе 1 на примере изучения дифференциальных уравнений. Но эта роль сквозная. Инварианты всегда сопровождают групповые изыскания в том или ином виде. В одних постановках задач ищутся подгруппы преобразований «ничего не меняющие», в других — выясняется, «какая часть» изучаемого явления нечувствительна к данной группе. При этом довольно часто групповой аспект остается за кадром.

Семь монет лежат гербом вверх. Можно ли, переворачивая по две монеты, уложить в итоге все гербом вниз? Задача, конечно, для детского сада. Нельзя. Потому что при переворачиваниях сохраняется четность числа монет, лежащих гербом вверх. Инвариант — четность. Всевозможные переворачивания — группа. Вариации в подобном направлении встречаются довольно сложные.

Можно ли шар разрезать на части, и сложить из них куб? Разрезы — произвольные гладкие поверхности[27]. К решению быстро приводит обнаружение «ингредиента задачи», нечувствительного к разрезам. Границы каждой i-й части разобьем на участки трех категорий: выпуклые, вогнутые и плоские, — и пусть их площади, соответственно, S_1, S_2, S_3. Положим

$$I_i = S_1 - S_2.$$

Сумма

$$I = \sum_i I_i,$$

[27] Некоторые детали мы обходим стороной, не говоря о разбиениях с использованием *аксиомы выбора*, которые приводят к парадоксам типа *Банаха—Тарского* [3].

как легко видеть, инвариант, потому что любой выпуклый участок границы на разрезе — вогнут по отношению к соседнему (при разрезании) куску. Поскольку

$$I(\text{шара}) = 4\pi R^2, \quad I(\text{куба}) = 0,$$

ответ — *отрицательный.*

Попытка аналогичным образом рассмотреть тетраэдр и куб ничего не дает. Но здесь работает другой инвариант, уже нетривиальный. В итоге достигается решение *третьей проблемы Гильберта.*

Равновеликие многоугольники равносоставлены, т. е. один из них можно разрезать на меньшие многоугольники и сложить из них другой. Этот факт существенно упрощает учение о площадях. При определении же объемов многогранников в $\mathbb{R}^3$ приходится использовать сложный предельный переход. Необходимость это или равновеликие многогранники тоже равносоставлены? В этом вопросе, собственно, и заключалась *третья проблема Гильберта*, которую отрицательно решил *Дэн* (1900). Таким образом, оказалось, что при переходе от $\mathbb{R}^2$ к $\mathbb{R}^3$ ситуация принципиально меняется.

Для решения проблемы необходимо привлечение дополнительных технических средств. Напомним, базисом называют совокупность линейно независимых векторов $\{e_1, \ldots, e_n, \ldots\}$, с помощью которых однозначно выражается любой вектор x рассматриваемого пространства

$$x = \sum_i x_i e_i. \tag{2.9}$$

При этом x_i называют координатами вектора x.

Для построения обычного базиса в конечномерном пространстве берется любая система B линейно независимых векторов и к ней добавляется вектор, который линейно не выражается через B. На каком-то шаге процесс заканчивается — иначе возникает противоречие с конечномерностью.

При наличии *аксиомы выбора* такая процедура может быть реализована также в бесконечномерном случае, как в счетном варианте (2.9), так и в несчетном (с континуальным индексом i). В несчетном варианте необходимые рассуждения несколько усложняются, но суть остается примерно та же. Получаемые таким образом базисы называются *базисами Гамеля.*

Дополнительное разнообразие ситуаций определяется возможностью вводить ограничения на допустимые координаты. Требовать, скажем, их рациональности. В последнем случае действительная прямая становится бесконечномерным векторным пространством из-за рациональной несоизмеримости многих чисел. Например, 3 и $\sqrt{2}$ линейно независимы, поскольку

$$\lambda_1 3 + \lambda_2 \sqrt{2} = 0$$

невозможно при рациональных λ_i.

Разрывная линейная функция. Рассмотрим функциональное уравнение

$$\varphi(x+y)=\varphi(x)+\varphi(y). \tag{2.10}$$

Возьмем любой базис Гамеля на действительной прямой, выберем некоторый базисный вектор e_λ, например, $e_\lambda=\sqrt{5}$ или $e_\lambda=\pi$, или даже $e_\lambda=1$, и положим

$$\varphi(x)=kx_\lambda, \tag{2.11}$$

что даст функцию, удовлетворяющую (2.10).

Конкретного решения (2.10) на самом деле, конечно, не дано. Если $e_\lambda=\sqrt{5}$, то мы не можем даже сказать, чему равно, например, значение $\varphi(4)$, потому что x_λ зависит не только от e_λ, но и от всего базиса [28]. Тем не менее конструктивно способен работать сам факт существования такой функции.

Решение третьей проблемы Гильберта. Введем понятие *псевдовеса* многогранника M,

$$P(M)=\sum_i l_i\varphi(\lambda_i), \tag{2.12}$$

где суммирование идет по всем ребрам длины l_i, λ_i — двугранный угол при i-м ребре, а φ — функция вида (2.11). Точнее говоря, пусть θ — двугранный угол при ребре правильного тетраэдра. Достроим множество $\{\theta,\pi\}$ до *базиса Гамеля* (легко проверяется, что π и θ несоизмеримы) и положим

$$\varphi(\lambda)=\lambda_\theta,$$

т. е. $\varphi(\lambda)$ равно θ-й координате в разложении по базису. Вычислять значения $\varphi(\lambda)$ мы можем лишь в двух ситуациях [29]

$$\varphi(c\theta)=c \quad \text{и} \quad \varphi(c\pi)=0$$

для рациональных c, что как раз достаточно для наших целей.

Необходимый результат вытекает из неравенства

$$P(\text{куба})\neq P(\text{тетраэдра}),$$

поскольку

$$P(\text{куба})=\varphi\left(\frac{\pi}{2}\right)\sum_i l_i^k=0, \tag{2.13}$$

$$P(\text{тетраэдра})=\varphi(\theta)\sum_i l_i^T=\sum_i l_i^T\neq 0. \tag{2.14}$$

---

[28] Если в базис входит какое-либо рациональное число e_β, то $\varphi(4)=0$, если не входит, то $\varphi(4)=?$

[29] Значения $\varphi(\lambda)$ для других углов λ мы не можем знать из-за произвола достройки базиса, но эти значения нам и не нужны.

Причины вполне очевидны. При разрезании куба или тетраэдра на меньшие многогранники и суммировании псевдовесов этих меньших многогранников, вычисленных по формуле (2.12), получается тот же самый псевдовес исходного многогранника. Это происходит потому, что суммирование по всем новым ребрам (появившимся в результате разрезания) дает нуль, ибо если некоторое l лежит внутри M и служит ребром (или частью ребра) новых многогранников, то

$$l\{\varphi(\lambda_1)+\ldots+\varphi(\lambda_s)\}=l\varphi(\lambda_1+\ldots+\lambda_s)=l\varphi(2\pi)=0,$$

если же l лежит на грани M, то опять получается нуль

$$l\{\varphi(\lambda_1)+\ldots+\varphi(\lambda_s)\}=l\varphi(\lambda_1+\ldots+\lambda_s)=l\varphi(\pi)=0.$$

Наконец, если l совпадает с ребром исходного многогранника, то $\lambda_1+\ldots+\lambda_s$ равно $\pi/2$ в случае куба, и θ в случае тетраэдра. Таким образом, псевдовес не зависит от способа разрезания и может просто вычисляться по формулам (2.13), (2.14).

2.8. Дополнения

- *Последовательность* гомоморфизмов

$$G' \xrightarrow{\varphi} G \xrightarrow{\psi} G'' \tag{2.15}$$

называют *точной*, если образ $\operatorname{im}\varphi=\varphi(G')$ совпадает с ядром $\ker\psi$. Тот же принцип используется и для более длинных последовательностей

$$G_1 \xrightarrow{\varphi_1} G_2 \to \ldots \to G_{n-1} \xrightarrow{\varphi_{n-1}} G_n.$$

В этом случае точную последовательность определяет согласованность всех звеньев:

$$\operatorname{im}\varphi_{j-1}=\ker\varphi_j.$$

Распространенный трюк: добавление к (2.15) еще двух тривиальных гомоморфизмов[30]:

$$0 \to G' \xrightarrow{\varphi} G \xrightarrow{\psi} G'' \to 0. \tag{2.16}$$

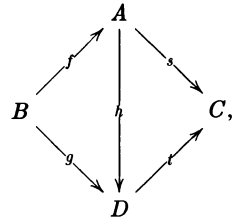
При этом точность последовательности (2.16) означает, помимо $\operatorname{im}\varphi=\ker\psi$, *инъективность* φ и *сюръективность* ψ.

Таким образом, *инъективность* φ и *сюръективность* ψ можно не упоминать, ибо они оказываются зашифрованы в (2.16). Экономия копеечная, но «фокус» эффективно препятствует освоению предмета.

Разъяснение дается для облегчения чтения другой литературы.

[30] Подразумевается аддитивный язык, с нулем вместо единицы.

• Среди инструментов, действенно запутывающих суть дела, можно отметить *коммутативные диаграммы*. Например,



где малые буквы — суть отображения, означает: если от одного объекта к другому можно пройти (вдоль стрелок) разными путями, то соответствующие композиции отображений совпадают. В данном случае: $fh = g$, $fs = gt \ldots$ Иногда это эффективно, но часто используется как графическое украшение и затуманивает изложение.

• О подводной части айсберга теории групп можно судить по недавно завершившейся эпопее в одном из теоретических секторов. Вот выдержка из статьи *Горенстейна* «Грандиозная теорема» в журнале Scientific American (издание на русском языке) № 2, 1986.

«Классификация простых конечных групп занимает столь необычное положение в анналах математики не только благодаря непомерно длинному доказательству, но и благодаря интригующему характеру решения. В процессе многолетних исследований постепенно открывались бесконечные семейства простых групп (и в конце концов были построены все 18 таких семейств), но время от времени обнаруживались и совершенно нерегулярные простые группы, которые не укладывались ни в одно семейство и были поэтому названы *спорадическими* группами. Первые пять таких загадочных простых групп были открыты *Э. Матье* в 60-е годы XIX века: наименьшая из групп Матье содержит ровно $8 \times 9 \times 10 \times 11$, т. е. 7 920 элементов. Шестая спорадическая группа, состоящая из 175 560 элементов, была обнаружена лишь спустя целое столетие *З. Янко*, работавшим тогда в Университете Монаш (Австралия).

После этого на свет стали появляться новые странные спорадические создания — примерно по одному в год, не отставая от интенсивных теоретических исследований 60-х и 70-х годов. Эти открытия вызвали среди математиков необычайное волнение, которое достигло высшей точки в 1982 году, когда *Р. Гриссмладший*, работавший в то время в Институте перспективных исследований, построил группу, названную „монстром“ за то, что число ее элементов равно

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000,

или приближенно $8 \cdot 10^{53}$. В конце концов было открыто 26 *спорадических* простых групп. *Группа-монстр* оказалась среди них самой большой, однако в ее структуре обнаружилось так много внутренних симметрий, что *Грисс* переименовал ее в „дружественного гиганта“.

Найти простую группу — это одно, и наградой служит само открытие, но доказать, что обнаружены все такие группы, — это совсем другое дело. Однако именно в этом состоит утверждение классификационной теоремы: „мир" простых конечных групп содержит 18 регулярных бесконечных семейств групп и 26 спорадических групп — и никаких других! Вот для доказательства этого утверждения и понадобилось 500 статей, занимающих около 15 тысяч журнальных страниц».

• «В тему» ложится доказательство простой с виду теоремы *Фейта—Томпсона*: *Любая конечная группа нечетного порядка разрешима*[31], — занимающее целый номер журнала[32].

[31] Разрешимые группы рассматриваются в главе 6.

[32] *Feit W., Thompson J. G.* Solvability of groups of odd order // Pacific J. Math. 1963. **13**. 775–1029.

Глава 3

Различные инструменты

В главе рассматриваются некоторые понятия и факты, степень бесполезности которых несколько выше предыдущего уровня. Но детали бывают важны не сами по себе, а для создания подходящей атмосферы.

3.1. Действие группы на множестве

3.1.1. *Действие группы G на множестве X определяется как преобразование $gx : G \times X \to X$, удовлетворяющее требованиям*:

(i) $1 \cdot x = x$, $\forall\, x \in X$,

(ii) $(g_1 g_2)x = g_1(g_2 x)$, $\forall\, x \in X$, $g_1 g_2 \in G$.

Тем самым можно считать, что вводится *левое действие* — умножение точек $x \in X$ на элементы $g \in G$. При этом оба знака умножения (групповой и «буферный» между G и X) мы опускаем, чтобы не отвлекать внимания. *Правое действие* xg определяется через левое как $g^{-1}x$.

Итак, каждый элемент $g \in G$ определяет преобразование

$$\omega_g : X \to X,$$

причем каждое ω_g является *биекцией*.

Иными словами, группе G ставится в соответствие подгруппа преобразований из *группы биекций* $\mathrm{Sym}(X)$, в которой умножение есть композиция. Точнее говоря, *действием группы* оказывается гомоморфизм $\omega : G \to \mathrm{Sym}(X)$. Частично получается тавтология, но это дает язык, открывающий дополнительные возможности.

Примеры

• *Симметрическая группа* $\mathbf{S_n}$, рáвно как и любая ее подгруппа, действует на $X = \{1, \ldots, n\}$. Действие *подстановок* приводит к *перестановкам*.

• Любая подгруппа $H \subset G$ действует на самой группе G, например, левым умножением: hx, $h \in H$, $x \in G$.

- Действие группы G на самой себе можно определить сопряжением,

$$G \times G \to G \quad \Leftrightarrow \quad gx \mapsto g^{-1}xg.$$

- *Группа автоморфизмов* $\mathrm{Aut}(G)$ действует на G.

3.2. Стабилизаторы

3.2.1. ***Стабилизатором*** *элемента* $x \in X$ *называется множество* [1)]

$$\mathrm{Stab}(x) = \{g \in G : gx = x\}.$$

Стабилизатор является подгруппой, необязательно нормальной.

3.2.2. *Стабилизаторы элементов* x *и* $y = gx$ *связаны как*

$$\mathrm{Stab}(y) = g\mathrm{Stab}(x)g^{-1}.$$

◀ Если $h \in \mathrm{Stab}(x)$, т. е. $hx = x$, то $(ghg^{-1})y = ghx = gx = y$. Поэтому

$$g\mathrm{Stab}(x)g^{-1} \subset \mathrm{Stab}(y).$$

Обратно, если $h \in \mathrm{Stab}(y)$, т. е. $hy = y$, то $(g^{-1}hg)x = g^{-1}hy = g^{-1}y = x$. Откуда

$$\mathrm{Stab}(y) \subset g\mathrm{Stab}(x)g^{-1}. \quad ▶$$

Если группа G действует на самой себе с помощью сопряжения, то

$$\mathrm{Stab}(x) = \{g \in G : gx = xg\},$$
$$\mathrm{Stab}(S) = \{g \in G : gSg^{-1} = S\}.$$

В этом случае группу

$$\mathfrak{u}(x) = \mathrm{Stab}(x)$$

называют *централизатором* элемента x, а

$$\mathcal{N}(S) = \mathrm{Stab}(S)$$

— *нормализатором* подмножества $S \subset G$.

[1)] То есть множество элементов группы, оставляющих элемент x неподвижным.

Во избежание путаницы исходным определением *централизатора* $\mathfrak{ц}(x)$ лучше считать [2]

$$\boxed{\mathfrak{ц}(x) = \{g \in G : gxg^{-1} = x\},}$$

т. е. $\mathfrak{ц}(x)$ — это совокупность тех $g \in G$, которые в случае преобразования gxg^{-1} оставляют точку $x \in G$ на месте.

При этом становится очевидной определенная двойственность понятия $\mathfrak{ц}(x)$ и *класса сопряженных элементов*

$$x^G = \{gxg^{-1} : g \in G\},$$

из которой легко выводится формула

$$|G| = |\mathfrak{ц}(x)| \cdot |x^G|. \tag{3.1}$$

Пересечение

$$\mathfrak{ц}(G) = \bigcap_{x \in G} \mathfrak{ц}(x)$$

называют ***центром*** G. Иными словами, $\mathfrak{ц}(G)$ — есть множество тех элементов группы G, которые коммутируют со всеми остальными,

$$\mathfrak{ц}(G) = \{g : gx = xg,\ \forall\, x \in G\},$$

т. е.

$$\mathfrak{ц}(G) = \{g : gxg^{-1} = x,\ \forall\, x \in G\}.$$

Любой центр является нормальной подгруппой [3] G, причем коммутативной. Центр абелевой группы совпадает со всей группой. Чем меньше центр, тем умножение «менее перестановочно».

Нормализатор всей группы является ее центром, $\mathcal{N}(G) = \mathfrak{ц}(G)$.

3.3. Орбиты

3.3.1. ***Орбитой*** *элемента* $x \in X$ *называется множество*

$$\mathrm{Orb}(x) = \{gx : g \in G\}.$$

[2] Поскольку использование стабилизатора в определении не делает должного акцента на том обстоятельстве, что речь обязательно должна идти о действии группы на самой себе *с помощью сопряжения*.

[3] Возможно, содержащей лишь единицу.

Различные орбиты не могут пересекаться. (?) В случае

$$\mathrm{Orb}(x^*) = \{x^*\}$$

элемент $x^* \in X$ называется *неподвижной точкой действия.*

Если $g \in G$ имеет порядок n, то

$$\mathrm{Orb}(x) = \{x, gx, \ldots, g^{n-1}x\},$$

но перечисленные элементы не обязаны быть все различны.

3.3.2. ***Подмножество*** $S \subset X$ ***называют устойчивым*** *к действию группы* G *на* X*, если*

$$x \in S,\ g \in G \quad \Rightarrow \quad gx \in S.$$

• Орбита $\mathrm{Orb}(a)$ — наименьшее устойчивое множество, содержащее точку a.

• Подмножество $S \subset X$ устойчиво в томм случае, когда оно представляет собой объединение орбит.

• В группе, действующей на себе сопряжением, орбиты оказываются *классами сопряженных элементов*,

$$\mathrm{Orb}(x) = \{gxg^{-1} : g \in G\}.$$

При этом $\mathrm{Orb}(x) = \{x\}$ в томм случае, когда элемент x лежит в центре $\mathfrak{u}(G)$, а подгруппа $H \subset G$ нормальна в томм случае, когда она — есть объединение орбит (классов сопряженных элементов).

Транзитивные группы. Действие группы G считается *транзитивным*, если в X имеется только одна орбита[4], т. е. орбита любой точки исчерпывает все X. Пусть речь идет о *транзитивной группе* подстановок $G \subset \mathbf{S_n}$, действующей на множестве $X = \{1, \ldots, n\}$. Транзитивность действия G в данном случае равносильна возможности указать для любых $i, j \in X$ такую подстановку $g \in G$, что $gi = j$.

Пусть G/H — множество *левых смежных классов* gH группы G по подгруппе H. Тогда

$$g_j g_i^{-1}(g_i H) = g_j H.$$

Поэтому: *любая группа* G *действует транзитивно на* G/H.

[4] *Группу* G в этом случае называют ***транзитивной***.

3.4. Конечные p-группы

3.4.1. *Группа G называется* **p-группой**, *если число p — простое, и порядок группы $|G| = p^k$.*

Если конечная группа G разбита на *классы сопряженных элементов* $x_1^G, \ldots, x_m^G$, то

$$|G| = |\mathfrak{u}(G)| + \sum_{x_i \notin \mathfrak{u}(G)} |x_i^G|, \tag{3.2}$$

что очевидно в силу $x^G = \{x\}$ при условии $x \in \mathfrak{u}(G)$.

Напомним также — см. (3.1) — связь

$$|G| = |\mathfrak{u}(x_i)| \cdot |x_i^G|,$$

справедливую при любом i.

3.4.2. *Подгруппа $H \subset G$ порядка $|H| = p^k$ — при максимально возможном k — называется максимальной, или силовской p-подгруппой.*

3.4.3. Лемма. *Всякая p-группа имеет нетривиальный центр.*

◄ Либо вся группа совпадает с центром — и тогда все доказано, либо

$$p^k = |G| = |\mathfrak{u}(G)| + pq,$$

в силу (3.2), и тогда $|\mathfrak{u}(G)|$ делится на p, что означает $|\mathfrak{u}(G)| > 1$. ►

3.4.4. Лемма. *Группа G порядка p^r имеет нормальные подгруппы порядков p^k при любых $k \leqslant r$.*

◄ Для $r = 1$ утверждение очевидно. Далее воспользуемся индукцией.

В $\mathfrak{u}(G)$ есть элемент g порядка p. Поэтому $H = \{1, g, g^2, \ldots, g^{p-1}\}$ — нормальная подгруппа порядка p. Следовательно, $|G/H| = p^{r-1}$. А раз утверждение справедливо для G/H, т. е. для $r - 1$, то теорема 2.6.2 гарантирует, что оно справедливо и для G, т. е. для r. ►

3.5. Теоремы Силова

При изучении конечных групп важную роль играют p-подгруппы. Оказывается, *для каждой степени p^k, делящей порядок группы, существует подгруппа порядка p^k. Если p^{k+1} также делит порядок*

группы, то всякая подгруппа порядка p^k содержится в некоторой подгруппе порядка p^{k+1}. Наконец, максимальные p-подгруппы попарно сопряжены друг с другом, и их число равно $1 \pmod p$.

Перечисленные результаты с некоторыми допусками обычно распределяются по трем *теоремам Силова.*

3.5.1. Теорема существования. *Если p простое и p^k делит $|G|$, то в G существует подгруппа порядка p^k.*

◀ Согласно лемме 3.4.4, достаточно установить существование максимальной p-подгруппы. Поэтому изначально можно считать $|G| = p^k q$, где q не делится на p. Далее применяем индукцию по порядку группы. Для $|G| = 1$ утверждение очевидно. В предположении справедливости утверждения для $t < k$ разобьем G на классы сопряженных элементов $x_1^G, \ldots, x_m^G$.

Если при некотором j порядок $|x_j^G| \neq 1$ не делится на p, то в силу

$$|\mathfrak{u}(x_j)| \cdot |x_j^G| = |G| = p^k q$$

на p^k делится порядок $|\mathfrak{u}(x_j)|$. А поскольку $|\mathfrak{u}(x_j)| < |G|$ (иначе все доказано), то по индуктивному предположению $\mathfrak{u}(x_j)$ содержит p-подгруппу порядка p^k.

В случае, когда все нетривиальные $|x_j^G|$ делятся на p, в силу (3.2) на p делится и $|\mathfrak{u}(G)|$. Это означает (по индуктивному предположению), что в $\mathfrak{u}(G)$ имеется силовская подгруппа $\mathfrak{u}'$ порядка p^t, $t \leqslant k$. Фактор-группа $G/\mathfrak{u}'$ имеет порядок p^{k-t}, и опять-таки по индуктивному предположению в $\mathfrak{u}'$ имеется силовская подгруппа порядка p^{k-t}, образ которой при *естественном гомоморфизме* будет в G *максимальной* p-подгруппой. ►

3.5.2. Теорема вложения. *Всякая p-подгруппа порядка p^k содержится в некоторой силовской подгруппе.*

3.5.3. Теорема сопряжения. *Все силовские p-подгруппы сопряжены друг с другом*[5]. *Число силовских подгрупп $s_p = 1 \pmod p$, причем s_p делит порядок группы.*

Доказательства последних двух теорем[6] не приводятся, чтобы не создавать атмосферу технической рутины. Кроме того, их (доказательства) можно найти

[5] Иными словами, *с точностью до сопряжения* силовская группа всегда одна. Соответственно, если силовская подгруппа нормальна, то она единственна уже без оговорок. И обратно, если силовская подгруппа единственна, то она нормальна.

[6] Доказательство теоремы 3.5.2 сильно коррелирует с леммой 3.4.4, которая к тому же в некоторой степени дополняет теорему.

во многих учебных руководствах [11, 16], причем речь идет о достаточно простых рассуждениях — с оговоркой насчет непривычности используемых категорий мышления. См. также раздел 3.6, где задачи вплотную подводят к соответствующим обоснованиям.

Теоремы Силова играют важную роль в теории конечных групп, позволяя в той или иной степени выяснить устройство изучаемой группы. Например, в случае $|G| = 63 = 3^2 \cdot 7$ теорема 3.5.1 гарантирует существование в G подгрупп порядков $3, 9, 7$.

Остановимся более подробно на ситуации $|G| = pq$, где $p < q$ — простые числа. Теорема 3.5.1 говорит о существовании подгрупп порядка p и q, но интересно посмотреть, к чему это приводит в итоге. По теореме 3.5.3 число силовских q-подгрупп равно $lq + 1$ и делит pq, — но тогда q-подгруппа единственна, причем нормальна (см. примечание к теореме 3.5.3).

Что касается p-подгрупп, то их число равно $kp + 1$ и делит q, что в ситуации

$$q \neq 1 \pmod{p}$$

также ведет к единственности и нормальности p-подгруппы. В результате группа G неизбежно оказывается *абелевой*, изоморфной *группе вычетов по модулю* pq. В особом случае

$$q = 1 \pmod{p}$$

группа G оказывается *неабелевой*, и рассуждение чуть более запутано [11].

3.6. Задачи

• Если $H \subset \mathfrak{ц}(G)$ и фактор-группа G/H циклична, то группа G — коммутативна.

• *Всякая* p*-группа, имеющая порядок* p^2*, коммутативна.*

◄ Центр $\mathfrak{ц}(G)$ нетривиален (лемма 3.4.3). Поэтому фактор-группа $G/\mathfrak{ц}(G)$ имеет порядок либо 1, либо p, — и потому циклична. ►

• Любая группа порядка $2p$ (простое $p > 2$) либо циклична, либо изоморфна группе *диэдра*.

• Если группа G, действующая *транзитивно* на множестве X, *коммутативна*, — то любой элемент $g \neq 1$ *сдвигает* любой элемент из X, т. е. $gx \neq x$.

◄ В предположении противного,

$$gx = x \;\Rightarrow\; ghx = hgx = hx. \;\blacktriangleright$$

• Следует ли из $a^4 = 1$, $b^3 = 1$ равенство $(ab)^{12} = 1$? (Не следует, см. главу 7.)

• Пусть H — нормальная (конечная) подгруппа группы G, а элемент g имеет конечный порядок и не коммутирует ни с одним элементом из H (разумеется, кроме 1). Тогда $h \mapsto g^{-1}h^{-1}gh$ — биекция: $H \to H$.

Глава 4

Абелевы группы

Абелевы группы достаточно важны практически и податливы теоретически. Но усвоению нередко мешает иллюзия элементарности коммутативного варианта, который не так уж тривиален, как выглядит. Тем не менее детальные доказательства «в рамках общего образования» здесь не обязательны. Достаточно общей картины с акцентами на отличиях. Так или иначе, многие подробности ниже опускаются — восполнить недостающее можно по различным источникам [8, 11, 14, 16].

4.1. Коммутативный вариант

Коммутативность групповой операции существенно упрощает исследование. Но надо иметь в виду, что владение общей «мультипликативной» теорией мешает осваивать «аддитивную» [1]. В некотором роде возникают «трудности изучения иностранного языка». Русский мешает учить английский — из-за подсознательного стремления установить соответствие. «Забыв на время один язык» — легче учить другой. Так или иначе, но способность отвлечься от старого помогает изучению нового. Коммутативные группы в этом смысле не исключение. Их удобно рассматривать с чистого листа.

4.1.1. ***Абелевой группой*** *A называется конечная или бесконечная совокупность элементов, на которой задана* ***групповая операция*** *«$+$», сопоставляющая любой паре элементов $a, b \in A$ некоторый элемент c из той же совокупности A:*

$$a + b = c.$$

При этом групповая операция, называемая обычно сложением, коммутативна $(a + b = b + a)$ и обязана удовлетворять трем условиям:

(i) $p + (q + r) = (p + q) + r$ *(ассоциативность)* [2].

---

[1] Напомним, для *абелевых* (*коммутативных*) *групп* обычно используется *аддитивная терминология*: групповая операция называется *сложением* и обозначается знаком $+$, а единица группы именуется и обозначается нулем.

[2] Благодаря ассоциативности скобки в любой сумме можно убрать или, наоборот, произвольно расставить.

(ii) *В группе существует нулевой элемент* 0, *обладающий свойством*

$$0 + x = x + 0 = x$$

для любого $x \in A$.

(iii) *Каждый элемент* $x \in A$ *имеет обратный* $-x$:

$$x + (-x) = x - x = 0.$$

Некоторые опорные факты также полезно переписать на новом языке.

• *Подмножество* $B \subset A$ *является подгруппой* A *в том случае, если из* $a, b \in B$ *следует* $a - b \in B$ (лемма 2.1.3).

• Групповую сумму $x + \ldots + x$ с n слагаемыми обозначают как nx. Группа A, в которой все элементы могут быть получены как ja,

$$A = \{\ldots, -2a, -a, 0, a, 2a, \ldots\},$$

называется ***циклической***.

Минимальное n в равенстве $nb = 0$ называют ***порядком*** или ***периодом*** элемента b и обозначают через $|b|$. В случае $nb \neq 0$ при любом $n > 0$ — считают $|b| = \infty$.

Если порядки всех элементов группы A (кроме единичного) бесконечны, — говорят, что A — ***группа без кручения***. Если же порядки всех элементов группы конечны, группу называют ***периодической***.

• Совокупность всех кратных $\{g\}$ любого элемента $g \in A$ является циклической подгруппой группы A,

$$|\{g\}| = |g|.$$

• Если g_α при изменении α пробегает все элементы группы A, и g_0 произвольный элемент A, то $g_0 + g_\alpha$ также пробегает все элементы группы.

• Понятие сопряженных элементов теряет смысл (рáвно как и понятия *центра* и *коммутанта*). Все подгруппы абелевой группы — нормальные; левые и правые смежные классы совпадают. Сумма смежных классов $f + H$ и $g + H$ определяется как

$$(f + H) + (g + H) = (f + g) + H,$$

потому что $H + H = H$. Таким образом, сумма смежных классов снова дает смежный класс. Кроме того,

$$(g + H) + (-g + H) = H.$$

Следовательно, совокупность смежных классов по инвариантной подгруппе H является группой, которую называют ***фактор-группой*** и обозначают как A/H. Нулем A/H служит подгруппа H.

• В абелевом случае *p-группы* называются — *примарными*.

4.2. Конечнопорожденные группы

В силу коммутативности, суммы элементов абелевой группы A можно записывать в виде

$$\alpha_1 u_1 + \ldots + \alpha_k u_k, \quad \text{все} \quad \alpha_i \in \mathbb{Z}, \quad u_i \in A. \tag{4.1}$$

Если «линейные комбинации» (4.1) исчерпывают все элементы группы[3] A, то конечная совокупность элементов $\{u_1, \ldots, u_k\}$ *порождает* группу A.

При этом *порождающая система* $\{u_1, \ldots, u_k\}$ называется *линейно зависимой*, если

$$\alpha_1 u_1 + \ldots + \alpha_k u_k = 0 \tag{4.2}$$

при некоторых целых $\alpha_1, \ldots, \alpha_k$, не равных нулю «поголовно»; и *линейно независимой* — в противном случае.

Линейно независимую систему порождающих $\{u_1, \ldots, u_k\}$, если таковая существует, называют ***свободной***, а о порождаемой группе говорят как о ***свободной абелевой группе***. Представление любого элемента $x = \alpha_1 u_1 + \ldots + \alpha_k u_k$ в свободной группе — однозначно. Свободную систему порождающих называют также ***базисом***, а целое k — ***рангом группы***.

Роль свободных абелевых групп аналогична роли *свободных групп* общего вида (раздел 7.2). Соответственно, имеет место аналог теоремы 7.2.1.

4.2.1. Теорема. *Всякая конечнопорожденная абелева группа A изоморфна некоторой фактор-группе свободной группы того же ранга.*

◀ Пусть $\{u_1, \ldots, u_n\}$ — система образующих группы A, а $\{x_1, \ldots, x_n\}$ — *базис* свободной группы F. Введем *эпиморфизм* $\varphi : F \to A$, действующий по правилу[4]

$$\varphi(\alpha_1 x_1 + \ldots + \alpha_n x_n) = \alpha_1 u_1 + \ldots + \alpha_n u_n.$$

По теореме 2.6.1 (о гомеоморфизме) фактор-группа $F/\ker\varphi$ изоморфна группе A. ▶

---

[3] То есть любой элемент $x \in A$ представим в виде $x = \alpha_1 u_1 + \ldots + \alpha_k u_k$.

[4] Все комбинации $\alpha_1 x_1 + \ldots + \alpha_n x_n$ в F различны, а $\alpha_1 u_1 + \ldots + \alpha_n u_n$ могут совпадать друг с другом из-за наличия в A линейных связей (4.2).

4.3. Прямое произведение и прямая сумма

В теории групп представляют интерес различные конструкции, с помощью которых из одних групп получаются другие. Прямое произведение — одно из таких приспособлений, которое особенно часто применяется в абелевых группах, где — в случае аддитивной точки зрения — называется *прямой суммой*. Общее определение выглядит так.

4.3.1. *О группе G говорят как о* ***прямом произведении*** *своих подгрупп $H_1, \ldots, H_n$ при условии*:

- *Любые элементы $a \in H_i$, $b \in H_j$, $i \neq j$ коммутируют, $ab = ba$.*
- *Любой элемент $g \in G$ представи́м в виде*

$$g = h_1 \ldots h_n, \qquad h_i \in H_i. \tag{4.3}$$

Требование коммутативности умножения подгрупп в определении 4.3.1 в некотором роде раскрывает карты, показывая, что при переходе к абелевым группам никаких существенных изменений, кроме терминологических, не происходит. За исходное чаще принимается определение [5], в котором перечисленные требования заменяются совокупностью трех условий:

- *Подгруппы $H_1, \ldots, H_n$ нормальны в G.*
- *Совокупность $\{H_1, \ldots, H_n\}$ порождает G.*
- *Разложение* (4.3) *однозначно.*

О *декартовом произведении* $X \times Y$ также говорят как о прямом произведении, полагая элементами группы $X \times Y$ пары (x, y), где $x \in X$, $y \in Y$. Групповая операция определяется как [6]

$$(x_1, y_1)(x_2, y_2) = (x_1 x_2, y_1 y_2).$$

При этом, в отличие от предыдущего случая, групповые операции в X и Y могут быть различны.

Смешение понятий декартова произведения и прямого — объясняется следующим фактом.

---

[5] Возможны также и другие варианты эквивалентных определений [16].

[6] Понятно, с тем же успехом можно говорить о декартовом произведении нескольких групп.

4.3.2. *Если X и Y — подгруппы одной группы G, то прямое и декартово произведение с точностью до изоморфизма порождают одну и ту же группу.*

◄ Изоморфизм φ определяется соответствием

$$xy \xrightarrow{\varphi} (x, y). \quad \blacktriangleright$$

Если $G = X \times Y$, то $G/X \sim Y$. (?)

В ситуации, когда X и Y — подгруппы абелевой группы A, их декартово произведение называют *прямой суммой*, используя обозначение $X \oplus Y$. Абелева группа A (необязательно конечнопорожденная) считается прямой суммой своих подгрупп B_γ, $\gamma \in \Gamma$, когда любой ее элемент $x \in A$ однозначно представим в виде суммы конечного числа элементов, взятых из различных подгрупп B_γ.

• Группа комплексных чисел по сложению является прямой суммой группы действительных чисел и группы мнимых чисел.

• Циклическая группа 15-го порядка, порожденная элементом f, является прямой суммой циклической подгруппы 3-го порядка, порожденной элементом $5f$, и циклической подгруппы 5-го порядка, порожденной элементом $3f$:

$$\langle f \rangle = \langle 5f \rangle \oplus \langle 3f \rangle.$$

4.3.3. *Если X и Y — нормальные подгруппы группы G и*

$$X \cap Y = 1, \quad XY = G, \tag{4.4}$$

то G — изоморфна декартову произведению $X \times Y$.

◄ Любой элемент группы G в силу $XY = G$ может быть записан в виде $g = xy$, $x \in X$, $y \in Y$, причем единственным образом, поскольку $X \cap Y = 1$. Кроме того, из нормальности подгруппы X следует[7)]

$$[x, y] = x(yx^{-1}y^{-1}) \in X.$$

Аналогично, $[x, y] \in Y$. В результате $[x, y] \in X \cap Y = 1$, что означает $xy = yx$.

Искомый изоморфизм $G \mapsto X \times Y$ определяется как $\varphi(g) = (x, y)$. ►

Условие (4.4), как видно из доказательства, равносильно коммутативности элементов из разных подгрупп: $xy = yx$, $x \in X$, $y \in Y$.

[7)] По поводу *коммутаторов* $[x, y]$ см. раздел 6.2.

4.4. Циклическая природа абелевых групп

Допустим, группа G состоит из всевозможных пар (a, b), где a — корни пятой степени из единицы, b — корни седьмой степени, т. е.

$$a = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}, \quad k = 0, \ldots, 4; \quad b = \cos\frac{2k\pi}{7} + i\sin\frac{2k\pi}{7}, \quad k = 0, \ldots, 6,$$

а групповая операция — покоординатное умножение.

Группа $\widehat{G}$ всевозможных пар (a, b) с покомпонентным умножением — состоит из $5 \cdot 7 = 35$ элементов, но циклична ли эта группа? — Циклична, 35 степеней

$$\left(\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}, \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}\right)^s, \quad s = 1, \ldots, 35,$$

исчерпывают (по модулю 2π) все пары, что, вообще говоря, требует обоснования. Но пункт 4.3.2 гарантирует, что группа $\widehat{G}$ изоморфна совокупности попарных произведений $\{ab\}$, для которых цикличность очевидна — образующий элемент:

$$\cos\frac{2\pi}{35} + i\sin\frac{2\pi}{35}.$$

Разобранный пример является прообразом следующего общего результата (в аддитивной интерпретации).

4.4.1. *Прямая сумма двух циклических групп взаимно простых порядков m и n является циклической группой порядка mn.*

Разумеется, *прямая сумма k циклических групп A_j попарно взаимно простых порядков $n_1, \ldots, n_k$ является циклической группой порядка $n_1 \ldots n_k$*. В общем случае, если

$$\text{НОК}\{n_1, \ldots, n_k\} \neq n_1 \ldots n_k,$$

абелева группа $A = A_1 \oplus \ldots \oplus A_k$ не циклична [8)].

Оказывается (!), прямые суммы циклических групп исчерпывают конечнопорожденные абелевы группы.

[8)] Поскольку в A нет элемента порядка $|A| = n_1 \ldots n_k$. В этом случае говорят, что ***показатель группы***

$$d = \min\{k > 0 : kx = 0, \forall x \in A\}$$

меньше порядка $|A|$.

4.4.2. Теорема. *Конечнопорожденная абелева группа является прямой суммой конечного числа бесконечных циклических подгрупп и конечного числа циклических примарных групп* [9].

Результат принято называть *основной теоремой* об абелевых группах с конечным числом образующих. Обоснование теоремы 4.4.2 несложно [16], но несколько утомительно.

Вокруг теоремы 4.4.2 имеется множество вариаций, обнажающих дополнительные ракурсы.

4.4.3. ***Подгруппой кручения*** $\mathrm{tors}(A)$ *абелевой группы* A *называется совокупность элементов* A *конечного порядка* [10].

• *Всякая конечнопорожденная абелева группа* A *является прямой суммой* $\mathrm{tors}(A)$ *и некоторой свободной абелевой группы.*

Таким образом, всякая конечнопорожденная абелева группа A без кручения — свободна (имеет линейно независимую систему образующих, базис).

• *Фактор-группа* $A/\mathrm{tors}(A)$ *является группой без кручения.*

• *Любая подгруппа свободной абелевой подгруппы — свободна.*

4.5. Группы гомологий

Алгебраизация топологии — один из показательных примеров искусственного насаждения групповой идеологии, плодоносящей в «неожиданной области». Представление о том, как это делается, полезно вне зависимости от «прикладных устремлений». Один из простейших способов в этой области основывается на симплициальных разбиениях многообразий.

Симплексы и симплициальные комплексы. *Симплекс* представляет собой обобщение понятия отрезка (1-симплекс), треугольника (2-симплекс), тетраэдра (3-симплекс). Общее определение: k*-мерным симплексом* (k*-симплексом*)

$$s^k = (a_0, \ldots, a_k)$$

[9] *Примарными* считаются абелевы p*-группы* (группы порядка p^k, где p простое число).

[10] Легко проверяется, что такая совокупность действительно является подгруппой. Подгруппу кручения называют также периодической частью группы A.

называется множество точек $x \in \mathbb{R}^n$, таких что

$$x = \sum_{j=0}^{k} \lambda_j a_j, \quad \sum_{j=0}^{k} \lambda_j = 1, \quad \text{все} \quad \lambda_j \geqslant 0,$$

в предположении линейной независимости векторов

$$a_1 - a_0, \ \ldots, \ a_k - a_0,$$

где точки $a_j \in \mathbb{R}^n$ представляют собой *вершины симплекса*, λ_j — *барицентрические координаты* точки x. О гомеоморфных образах симплексов говорят как о *криволинейных симплексах*. Очевидно, симплекс s^k представляет собой выпуклую оболочку своих вершин. Выпуклая оболочка любого подмножества вершин называется *гранью симплекса*.

Симплициальным комплексом $K \subset \mathbb{R}^n$ называют конечное семейство симплексов s_i^k, расположение которых характеризуется тем, что пересечение любых двух s_i^p, s_j^q или пусто, или является гранью как s_i^p, так и s_j^q.

Множество всех точек из $\mathbb{R}^n$, принадлежащих симплексам комплекса K, с топологией, индуцированной из $\mathbb{R}^n$, называют *полиэдром* комплекса K и обозначают $|K|$, а комплекс K именуют *триангуляцией* полиэдра $|K|$. Геометрически очевидно, что любой полиэдр можно сколь угодно мелко триангулировать, делая максимальный диаметр составляющих симплексов сколь угодно малым.

Ориентация. В $\mathbb{R}^3$ упорядоченная тройка некомпланарных векторов a, b, c называется *правой*, если для наблюдателя, расположенного в нуле, обход концов a, b, c в указанном порядке происходит по часовой стрелке. В противном случае тройка a, b, c — *левая*. Соответственно классифицируются базисы. В общем случае $\mathbb{R}^n$ отделить «правое» от «левого» невозможно, но дихотомия остается.

Два базиса $e = \{e_1, \ldots, e_n\}$ и $e' = \{e'_1, \ldots, e'_n\}$ в $\mathbb{R}^n$ считаются *одинаково ориентированными*, если $\det A > 0$ ($e' = Ae$). В случае $\det A < 0$ говорят, что базисы e и e' *противоположно ориентированы*. В результате все базисы распадаются на два класса эквивалентных, *положительно* ориентированных (*одинаково ориентированных* по отношению к фиксированному базису), и — *отрицательно* ориентированных.

О положительной и отрицательной *ориентации симплекса*

$$s^n = (a_0 \ldots a_n) \tag{4.5}$$

говорят в зависимости от того, одинаково или противоположно с избранным базисом $\mathbb{R}^n$ ориентирован базис

$$e_1 = a_1 - a_0, \quad \ldots, \quad e_n = a_n - a_0.$$

Симплекс $(a_{i_0} \ldots a_{i_n})$, построенный на тех же вершинах, что и (4.5), но взятых в другом порядке, будет совпадать либо с s^n, либо с $-s^n$. Четное (нечетное) число перестановок двух вершин симплекса не меняет (меняет) его ориентацию. *Неориентированный симплекс* обозначается далее $|s^n|$.

Коэффициенты инцидентности и оператор Δ. Пусть крышечка над вершиной симплекса исключает эту вершину, т. е.

$$(a_0 \dots \widehat{a}_i \dots a_n) = (a_0 \dots a_{i-1} a_{i+1} \dots a_n).$$

В результате от s^n остается $(n-1)$-мерная грань s^{n-1}.

Рассмотрим теперь ориентированный симплекс s^n и его ориентированную грань s^{n-1}, не содержащую, например, вершину a_i симплекса s^n. Допустим, порядок вершин $a_{i_0}, \dots, a_{i_{n-1}}$ определяет выбранную ориентацию грани $|s^{n-1}|$. При этом порядок

$$a_i, a_{i_0}, \dots, a_{i_{n-1}}$$

вершин симплекса $|s^n|$ определяет либо исходную ориентацию s^n, либо ориентацию $-s^n$. В первом случае *коэффициент инцидентности* $(s^n : s^{n-1})$ считается равным $+1$, во втором — равным -1. Если же s^{n-1} — *не грань* s^n, то $(s^n : s^{n-1}) = 0$.

4.5.1. ***Граница ориентированного симплекса*** *определяется как*

$$\Delta s^n = \sum_{i=0}^{n} (s^n : s_i^{n-1}) s_i^{n-1}.$$

Оператор Δ называется ***граничным.***

Если договориться, что ориентации граней выбираются в соответствии с правилом

$$s^n = (a_0 \dots a_n), \quad s_i^{n-1} = (a_0 \dots \widehat{a}_i \dots a_n),$$

то, как легко проверить,

$$\Delta s^n = \sum_{i=0}^{n} (-1)^i s_i^{n-1}.$$

Граница симплекса — частный случай общего понятия цепи: *r-мерная цепь* x^r комплекса K определяется как формальная сумма

$$x^r = \sum_i \alpha_i s_i^r,$$

где α_i — целочисленные коэффициенты. При этом *граница цепи*,

$$\Delta x^r = \sum_i \alpha_i \Delta s_i^r,$$

является $(r-1)$-мерной цепью.

Если в множестве всех цепей комплекса K ввести операцию сложения цепей (как линейных форм), то это множество становится группой и обозначается $L_r(K)$. Граничный оператор, таким образом, действует из L_r в L_{r-1}.

Циклы. Любая цепь x^r с нулевой границей ($\Delta x^r = 0$) называется *циклом*. Множество r-мерных циклов $Z_r(K)$ является подгруппой группы $L_r(K)$. Другими словами, Z_r — это ядро гомоморфизма

$$\Delta : L_r \to L_{r-1},$$

т. е. $Z_r = \ker \Delta$.

В *группе циклов* $Z_r(K)$ можно выделить *подгруппу* $B_r(K)$ *r-мерных границ*, т. е. множество r-мерных цепей, являющихся границами некоторых $(r+1)$-мерных цепей.

◄ Чтобы проверить, что $B_r(K)$ — действительно подгруппа $Z_r(K)$, достаточно установить [11]

$$\Delta\Delta x^r = 0, \tag{4.6}$$

поскольку ядро любого гомоморфизма $\varphi : G \to H$ — подгруппа G.

Поскольку оператор Δ линеен, (4.6) достаточно проверить в случае, когда x^r — симплекс:

$$\Delta\Delta s^r = \Delta\left[\sum_i (-1)^i (a_0 \dots \widehat{a}_i \dots a_r)\right] =$$

$$= \sum_i (-1)^i \left[\sum_{j<i} (-1)^j (a_0 \dots \widehat{a}_j \dots \widehat{a}_i \dots a_r) + \sum_{j>i} (-1)^{j-1} (a_0 \dots \widehat{a}_i \dots \widehat{a}_j \dots a_r)\right].$$

Легко видеть, что грань $(a_0 \dots \widehat{a}_i \dots \widehat{a}_j \dots a_r)$ входит в сумму дважды: один раз с коэффициентом $(-1)^{i+j}$, другой раз с коэффициентом $(-1)^{i+j-1}$, что в сумме дает нуль. Поэтому $\Delta\Delta s^r = 0$. ►

4.5.2. *Фактор-группа $H_r = Z_r / B_r$ группы циклов Z_r по подгруппе границ B_r называется r-й* ***группой гомологий*** *комплекса K.*

[11] То есть граница границы сама по себе не имеет границы.

Группы H_r, Z_r, B_r введены здесь для комплекса K, тогда как основной интерес представляет изучение самого полиэдра $|K|$. На простых примерах легко видеть, что группы Z_r, B_r при измельчении триангуляции полиэдра $|K|$ разрастаются, но эти изменения в группах Z_r, B_r оказываются тесно связанными, и фактор-группа $H_r = Z_r/B_r$ не меняется. Это общее правило.

4.5.3. *Группа гомологий $H_r(K)$ не зависит от триангуляции, а определяется самим полиэдром. Гомеоморфные полиэдры имеют одинаковые (изоморфные) группы гомологий.*

Соответственно, вычислять группы гомологий можно на основе произвольной триангуляции — наиболее простой и удобной. Достижением топологии явилось обобщение этой техники с криволинейных полиэдров на случай любых компактов [12].

Пример

Рассмотрим в качестве криволинейного полиэдра P *тор* — так называемую *сферу с ручкой* (многообразие, гомеоморфное поверхности бублика). Одномерные циклы x^1 на P — не что иное, как замкнутые ориентированные (с заданным направлением обхода) кривые. Такие кривые (циклы) подразделяются на те, которые ограничивают некоторую область (цикл z на рис. 4.1), и те, которые никакой области не ограничивают, т. е. не принадлежат группе границ (*меридиан* и *параллель* тора, рис. 4.1). Обратим внимание, что цикл, изображенный на рис. 4.2 (равный сумме циклов), ограничивает «область» $A + 2B + C$, в которую «территория» B входит дважды. Поэтому, если говорить точнее, то надо сказать, что все циклы подразделяются на те, которые являются границами некоторых двумерных цепей [13], и те, которые границами не являются.

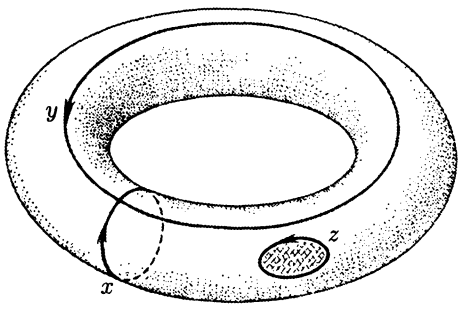


Рис. 4.1

Будем все ограничивающие циклы считать несущественными, а «существенные» — разобьем на *гомологичные циклы*. Циклы x_1 и x_2 называются *гомологичными*,

[12] Помимо определенных здесь симплициальных групп в топологии используются различные другие группы гомологий: *сингулярные гомологии*, *гомологии Виеториса*, *Чеха* и др.

[13] А не областей в обычном понимании этого слова.

если их разность $x_1 - x_2$ — ограничивающий цикл (*гомологичный нулю*) [14]. Эти *классы гомологий* и есть элементы *группы гомологий* H_1. На торе все такие классы гомологий выражаются через класс меридианов x_m и класс параллелей x_p. Если цикл x обходит тор α раз по меридиану и β раз по параллели, то $x = \alpha x_m + \beta x_p$, и потому x_m и x_p — образующие группы H_1, а сама группа H_1 представляет собой прямую сумму [15] $\mathbb{Z} \oplus \mathbb{Z}$.

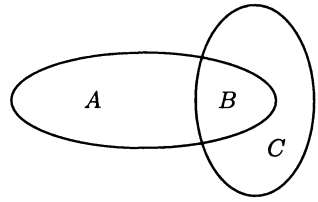


Рис. 4.2

На двумерной сфере S^2 группа гомологий H_1 тривиальна — состоит из единственного, нулевого, класса гомологий — поскольку все одномерные циклы на S^2 гомологичны между собой. Группа гомологий H_2 на S^2 изоморфна $\mathbb{Z}$. (**?**)

4.6. Классификация многообразий

Одной из основных задач топологии является классификация многообразий с точностью до тех или иных разрешенных преобразований. Например, с точностью до гомеоморфизма [16].

Привязка топологических инструментов к теоретико-групповым осуществляется на основе аппроксимации. Сначала определяются *симплициальные отображения*, преобразующие комплексы в комплексы. После этого *непрерывные отображения* $f : |K_1| \to |K_2|$ приближаются (сколь угодно точно за счет измельчения триангуляции) — *симплициальными*. В итоге удается перейти из топологии в алгебру, ибо симплициальное отображение $\varphi : K_\alpha \to K_\beta$ естественным образом индуцирует гомоморфизмы φ_r^* группы $L_r(K_\alpha)$ в группу $L_r(K_\beta)$.

Технологически это происходит следующим образом:

$$\varphi_r^*(s_\alpha^r) = (\varphi(a_0) \dots \varphi(a_r)),$$

если вершины у симплекса $s_\alpha^r = (a_0 \dots a_r)$ различны, и $\varphi_r^*(s_\alpha^r) = 0$ в противном случае. На цепи φ_r^* распространяется линейно.

---

[14] Например, два различных меридиана тора с одинаковой ориентацией — гомологичны друг другу.

[15] Точнее говоря, изоморфна прямой сумме.

[16] Гомеоморфизмом $f : X \to Y$ называют взаимно однозначное (инъективное плюс сюръективное) и непрерывное в обе стороны (непрерывны как f, так и f^{-1}) отображение.

Легко проверяется, что гомоморфизм φ_r^* коммутирует с *граничным оператором*, откуда следует, что φ_r^* переводит циклы в циклы, границы — в границы, а значит, и группу гомологий $H_r(K_\alpha)$ — в группу гомологий $H_r(K_\beta)$.

В итоге группы гомологий $\{H_r\}$ многообразия оказываются топологическими инвариантами, которые не меняются под действием гомеоморфизмов.

Известны и другие топологические инварианты «того же происхождения», например, ***эйлерова характеристика***

$$\chi = \sum (-1)^r K_r,$$

где K_r — число r-мерных симплексов в комплексе K.

4.7. Первая гомотопическая группа

Два *пути* (непрерывных кривых) в *топологическом пространстве* X, имеющих общие концы, называются *гомотопными*, если один из них можно непрерывно деформировать в другой, не двигая концов. Иначе говоря, два пути $\varphi_0(t)$, $\varphi_1(t)$,

$$\varphi_0 : [0, 1] \to X, \quad \varphi_1 : [0, 1] \to X,$$

соединяющих некоторые точки $u, v \in X$, т. е.

$$\varphi_0(0) = \varphi_1(0) = u, \quad \varphi_0(1) = \varphi_1(1) = v,$$

гомотопны, если существует непрерывная *деформация* $\varphi(t, \tau)$,

$$\varphi : [0, 1] \times [0, 1] \to X, \quad \varphi(0, \tau) \equiv u, \quad \varphi(1, \tau) \equiv v,$$

такая что

$$\varphi(t, 0) \equiv \varphi_0(t), \quad \varphi(t, 1) \equiv \varphi_1(t).$$

«Стенографический» вариант в данном случае длиннее разговорного, но тут преимущества лежат в другой плоскости. Когда возникает необходимость конкретно указать деформацию, — ясно, что́ надо указать (в смысле регламента).

Далее рассматриваются *замкнутые пути* (*петли*) с заданным направлением обхода, возможно, самопересекающиеся, которые начинаются и заканчиваются в одной выделенной точке $x_0 \in X$. Отношение *гомотопности* разбивает такие пути на *эквивалентные*

классы. Умножением (групповым) двух путей называется их объединение, после которого можно двигаться по объединенной кривой с соблюдением разрешенных направлений.

На плоскости (рис. 4.3) с вырезанной областью Ω и выделенной точкой x_0 — показано объединение путей A и B. Контур A может быть стянут (деформирован) в точку, контур B — нет. Сделав оборот по A и вернувшись в точку x_0, можно перейти к движению по B (с учетом разрешенных направлений).

На торе полезно себе представить объединение меридиана с параллелью — ни тот, ни другой контур в этом случае невозможно стянуть в точку.

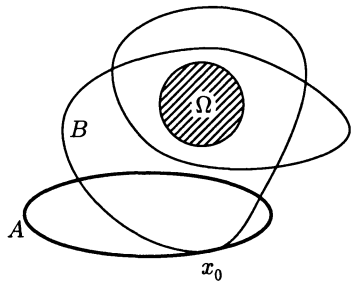


Рис. 4.3

Легко видеть, что множество замкнутых путей с таким умножением образует группу, называемую *фундаментальной*, или *первой гомотопической*, и обозначаемую $\pi_1(X, x_0)$. Единицей этой группы служит класс контуров, стягиваемых в точку x_0.

Замена x_0 любой другой точкой y_0, которую можно соединить с x_0 непрерывным путем, — не меняет группу,

$$\pi_1(X, x_0) \sim \pi_1(X, y_0).$$

Фундаментальная группа является инвариантом [17], характеризующим топологическую структуру пространства X.

[17] Детали будут изложены в томе «Топология».

Глава 5

Теория представлений

В теории представлений изучаемым группам ставятся в соответствие группы матриц, или — линейных операторов. В связи с переходом от «неудобных» групповых операций к «привычному» матричному умножению возникают определенные ожидания, которые не всегда оправдываются [1], но кое-что получает дополнительный импульс.

5.1. Матричные представления

Представлением группы G называют функцию $T(g)$ $(g \in G)$, принимающую значения в группе невырожденных матриц и удовлетворяющую функциональному уравнению

$$\boxed{T(g_1 g_2) = T(g_1)T(g_2),} \tag{5.1}$$

при условии $T(1) = I$, где I — единичная матрица. Если речь идет о *непрерывной группе* G, в которой, так или иначе, определена сходимость элементов, то от функции $T(g)$ требуется еще непрерывность.

Разумеется, в (5.1) имеется в виду

$$T(g_1 * g_2) = T(g_1) \cdot T(g_2),$$

где звездочка обозначает групповую операцию в G, а точка — умножение матриц.

Из (5.1) легко следует

$$T(g^{-1}) = T^{-1}(g)$$

в силу

$$I = T(gg^{-1}) = T(g)T(g^{-1}).$$

[1] Потому что матричное умножение не лучше композиции подстановок. Однако очевидные трудности — толкают иногда к неочевидным.

Поэтому совокупность матриц $\{T(g) : g \in G\}$ в самом деле представляет собой группу, а функция $T(g)$ — *гомоморфизм*.

Представление $T(g)$ в общем случае не обязано разным элементам группы G сопоставлять разные матрицы. В случае $T(g) = I$ только при условии $g = 1$, что означает $\ker T = 1$, — представление $T(g)$ называется *точным*.

Рассматривая матрицы как линейные операторы, естественно говорить о *пространстве представлений* $E = \mathbb{R}^n$, в котором действуют операторы $T(g)$. И вообще, о $T(g)$ с самого начала лучше говорить как о линейных операторах, ибо переход к другому базису меняет матрицы. Матричные же представления T_1 и T_2 считаются *эквивалентными* (*изоморфными*), если они описывают одну и ту же совокупность линейных операторов. Иными словами, если существует такая невырожденная матрица C, что [2)]

$$T_1(g) = C^{-1}T_2(g)C, \quad \forall g \in G.$$

Различие между линейным оператором и матрицей стирается при фиксации базиса. Это обстоятельство принципиально в линейной алгебре [4, т. 3], но оно еще более существенно в теории представлений, где рассматриваются *совокупности* матриц, и важно подчеркнуть, что все матрицы описывают линейные операторы в одном и том же избранном базисе.

Обратим внимание, что линейное представление группы можно интерпретировать как *действие группы* на векторном пространстве, с тем уточнением, что каждому элементу группы сопоставляется не произвольная *биекция*, а линейный оператор.

• Линейным представлением группы подстановок $\mathbf{S}_n$ является группа $(n \times n)$-матриц перестановок. *Матрицей перестановки* называют матрицу, у которой в каждом столбце и каждой строке — ровно один элемент равен 1, остальные нули. Умножение матрицы на матрицу перестановки слева — переставляет строки, справа — столбцы. Например,

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \Rightarrow \quad P \begin{bmatrix} a_{1:} \\ a_{2:} \\ a_{3:} \end{bmatrix} = \begin{bmatrix} a_{1:} \\ a_{3:} \\ a_{2:} \end{bmatrix}.$$

Группа матриц перестановок изоморфна *симметрической группе подстановок* $\mathbf{S}_n$.

[2)] (!) Сопрягающая матрица C — одна и та же для всех элементов группы.

• В качестве линейного представления бесконечной циклической группы

$$G = \{a, a^2, \ldots, a^n, \ldots\}$$

можно взять любую невырожденную матрицу $T(a)$, полагая $T(a^k) = T^k(a)$. Если же циклическая группа имеет порядок n, то на $T(a)$ необходимо наложить ограничение $T^n(a) = I$, которому можно удовлетворить, взяв в качестве $T(a)$ диагональную матрицу с n корнями из единицы на диагонали.

• Представлением группы поворотов на угол ξ является, например,

$$T(\xi) = \begin{bmatrix} \cos\xi & -\sin\xi \\ \sin\xi & \cos\xi \end{bmatrix}.$$

А представлением группы движений плоскости $g(\xi, a, b)$:

$$x' = x\cos\xi - y\sin\xi + a,$$
$$y' = x\sin\xi + y\cos\xi + b,$$

может служить как комплексное

$$T(g) = \begin{bmatrix} e^{i\xi} & a + ib \\ 0 & 1 \end{bmatrix},$$

так и действительное представление

$$T(g) = \begin{bmatrix} \cos\xi & -\sin\xi & a \\ \sin\xi & \cos\xi & b \\ 0 & 0 & 1 \end{bmatrix}.$$

• В случае

$$G = \langle a_1, \ldots, a_n \rangle$$

и наличия в G определяющих соотношений вида $a_1^{\sigma_1} \ldots a_n^{\sigma_n} = 1$ на выбор

$$T(a_1), \ldots, T(a_n)$$

должны быть наложены ограничения $T^{\sigma_1}(a_1) \ldots T^{\sigma_n}(a_n) = I$.

• Если группа G конечна, $|G| = n$, то

$$\forall g \in G: \; T^n(g) = T(g^n) = T(1) = I.$$

Поэтому все собственные значения $\lambda_1, \ldots, \lambda_n$ оператора $T(g)$ являются корнями n-й степени из 1 (при любом $g \in G$).

• Разумеется, возникает вопрос, любая ли группа имеет представление в указанном выше смысле. Первый пример *группы Ли*, нереализуемой в виде группы матриц, указан, по-видимому, *Картаном* [12]. Более простой пример дал *Биркгоф*[3].

[3] *Birkhoff G.* Lie groups isomorphic with no linear group // Bull. Amer. Math. Soc. 1936. 42. 883–888.

5.2. Инвариантные подпространства

Допустим, операторы представления $T(g)$ действуют в E. Подпространство $\mathcal{R} \subset E$ называется *инвариантным*, если для всех $g \in G$: из $x \in \mathcal{R}$ следует $T(g)x \in \mathcal{R}$.

5.2.1. *Представление $T(g)$, имеющее только тривиальные инвариантные подпространства (нулевое и само E), называют* ***неприводимым.***

В случае приводимого представления $T(g)$ имеются два других представления группы G. Одно из них получается как *сужение* операторов $T(g)$ на $\mathcal{R}$, а другое — строится в фактор-пространстве $E/\mathcal{R}$ смежных классов[4] $x + \mathcal{R}$. Таким образом, в случае приводимого представления $T(g)$ оказывается возможным перейти к *представлениям группы* — меньшей размерности. При этом в подходящем базисе

$$T(g) = \begin{bmatrix} T_1(g) & S(g) \\ 0 & T_2(g) \end{bmatrix}. \tag{5.2}$$

Обоснование фактов типа (5.2) — с указанием рецепта выбора базиса — здесь вряд ли уместно, ибо читать главу в любом случае необходимо «с линейной алгеброй в багаже». Разница между одним линейным оператором и совокупностью, конечно, есть. Но в данной ситуации все линейные операторы $T(g)$ имеют одно и то же инвариантное подпространство $\mathcal{R}$, что сводит исследование к стандартным приемам линейного анализа [4, т. 3].

Обнулить блок $S(g)$ в (5.2), вообще говоря, невозможно. Однако если инвариантно не только подпространство $\mathcal{R}$, но и его дополнение, то выбор базиса, в котором

$$T(g) = \begin{bmatrix} T_1(g) & 0 \\ 0 & T_2(g) \end{bmatrix},$$

оказывается возможен. В этом случае говорят, что $T(g)$ является *прямой суммой представлений* $T_1(g)$, $T_2(g)$, и пишут

$$T(g) = T_1(g) \oplus T_2(g).$$

[4] Из инвариантности $\mathcal{R}$ следует, что оператор $T(g)$ переводит смежный класс $x + \mathcal{R}$ в смежный класс $T(g)x + \mathcal{R}$.

Если E распадается в *прямую (ортогональную) сумму инвариантных подпространств*

$$E = \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_n,$$

$T(g)$ разлагается в *ортогональную прямую сумму*

$$T(g) = T_1(g) \oplus \ldots \oplus T_n(g),$$

что соответствует блочно-диагональной записи матрицы $T(g)$ с блоками $T_i(g)$ на диагонали.

5.2.2. *Представление $T(g)$ называется **вполне приводимым**, если оно раскладывается в ортогональную прямую сумму неприводимых представлений*[5].

Матрица вполне приводимого представления в подходящем базисе имеет вид

$$T(g) = \begin{bmatrix} T_1(g) & 0 & \ldots & 0 \\ 0 & T_2(g) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & T_n(g) \end{bmatrix}.$$

5.3. Ортогональные представления

Сопряженным к $T(g)$ называют *представление*[6]

$$T'(g) = T(g^{-1}). \tag{5.3}$$

Представления $T(g)$ и $T'(g)$ группы G изоморфны (еще говорят — эквивалентны).

5.3.1. *Представление $T(g)$ называется **ортогональным** (**унитарным**), если существует скалярное произведение $\langle \cdot, \cdot \rangle$, по отношению к которому $T(g)$ ортогональный (унитарный) оператор при любом $g \in G$.*

---

[5] Что имеет место в томм случае, когда дополнение всякого инвариантного подпространства — также инвариантно.

[6] Свойство $T'(g_1)T'(g_2) = T'(g_1 g_2)$ очевидно. Точное определение сопряженного представления опирается на манипулирование сопряженным пространством E^*, что в данном случае ничего не добавляет по сути. Причины (5.3) раскрываются далее.

В унитарном случае сопряженное представление вычисляется по правилу:

$$\boxed{T'(g) = T^*(g),}$$

где звездочка обозначает *эрмитово сопряжение*[7].

Напомним [4, т. 3], линейное преобразование S называют *ортогональным*, если оно *не меняет длину* векторов,

$$\langle x, x\rangle = \langle Sx, Sx\rangle = \langle x, S^*Sx\rangle = \langle S^*Sx, x\rangle,$$

откуда $S^*S = S^*S = I$, что означает

$$\boxed{S^* = S^{-1},}$$

т. е. для получения обратной — ортогональную матрицу достаточно просто транспонировать.

Унитарное преобразование — это комплексный вариант ортогонального. Внешняя картина остается прежней. Разница лишь в том, что скалярное произведение подразумевает перемножение комплексных векторов,

$$\langle x, y\rangle = \sum_j x_j \bar{y}_j,$$

а транспонирование операторов заменяется эрмитовым сопряжением.

Отмеченное выше равенство $T'(g) = T^*(g)$ в унитарном случае следует из цепочки

$$T'(g) = T(g^{-1}) = T^{-1}(g) = T^*(g).$$

5.3.2. Теорема. *Всякое линейное представление конечной группы ортогонально (унитарно).*

◀ Ограничимся рассмотрением вещественного случая. Пусть в E задано некоторое скалярное произведение $\langle\cdot,\cdot\rangle_0$. Новое скалярное произведение

$$\langle x, y\rangle = \sum_{g\in G} \langle T(g)x, T(g)y\rangle_0$$

инвариантно относительно T. Действительно,

$$\langle T(h)x, T(h)y\rangle = \sum_{g\in G} \langle T(g)T(h)x, T(g)T(h)y\rangle_0 = \sum_{g\in G} \langle T(gh)x, T(gh)y\rangle_0,$$

[7] Сводящееся к транспонированию для действительных матриц. В случае комплексных матриц эрмитово сопряжение означает транспонирование плюс комплексное сопряжение всех элементов.

но когда g пробегает всю группу, то gh также пробегает всю группу. Поэтому

$$\langle T(h)x, T(h)y\rangle = \langle x, y\rangle,$$

т. е. $T(h)$ сохраняет длину вектора при любом $h \in G$. ►

Конечность группы в доказательстве использовалась при суммировании, замена которого *инвариантным интегрированием* [21] позволяет установить аналог теоремы 5.3.2 для *компактных групп*, представления которых также ортогональны (унитарны).

В свою очередь, *всякое ортогональное (унитарное) представление вполне приводимо*, а значит, может быть записано в блочно-диагональном виде [8)].

5.4. Инвариантные операторы

Линейный оператор A, коммутирующий с представлением $T(g)$,

$$AT(g) = T(g)A, \quad \forall g \in G, \tag{5.4}$$

называется *инвариантным*. Смысл термина лучше раскрывает эквивалентная (5.4) запись

$$T^{-1}(g)AT(g) = A, \quad \forall g \in G. \tag{5.5}$$

Это можно интерпретировать следующим образом. Соотношение

$$y = Ax$$

после перехода к другой (штрихованной) системе координат с матрицей перехода $T(g)$,

$$x = T(g)x', \quad y = T(g)y',$$

превращается в

$$y' = T^{-1}(g)AT(g)x'.$$

В случае (5.5) получается, что описание связи «входа x и выхода y» инвариантно по отношению к заменам координат из данной группы.

[8)] Что освобождает от неприятностей, связанных с жордановыми формами. *Полная приводимость* вытекает из того факта, что ортогональное дополнение инвариантного подпространства в случае ортогонального (унитарного) представления — также инвариантное подпространство.

В случае (5.4), *если* x — *собственный вектор оператора* A, *то и* $T(g)x$ — *собственный вектор* A, *отвечающий тому же самому собственному значению* λ.

◀ Если $Ax = \lambda x$, то $AT(g)x = T(g)Ax = \lambda T(g)x$. ▶

Отсюда следует, что *подпространство, натянутое на собственные векторы оператора* A, *отвечающие данному собственному значению* λ, — *является инвариантным для представления* $T(g)$. Поэтому оператор A, перестановочный с *неприводимым* представлением $T(g)$, не может иметь более одного собственного значения[9], т. е. фактически обязан быть скалярным, $A = \lambda I$. Это простой, но достаточно принципиальный результат, называемый обычно *леммой Шура*.

5.4.1. Лемма Шура. *Матрица* A, *коммутирующая со всеми операторами неприводимого представления* $T(g)$, *может быть только скалярной*, $A = \lambda I$.

Из леммы 5.4.1 сразу следует, например, что *неприводимые конечномерные представления абелевых групп — одномерны.*

◀ Действительно,

$$gh = hg \quad \Rightarrow \quad T(g)T(h) = T(h)T(g).$$

Поэтому при фиксированном h оператор $T(h)$ перестановочен с представлением $T(g)$. Следовательно, $T(h) = \lambda(h)I$. Но представление такого типа может быть неприводимым лишь в том случае, когда λ не зависит от h. ▶

Отсюда вытекает, что *у любого комплексного представления абелевой группы существует одномерное инвариантное подпространство.*

Еще одно следствие леммы 5.4.1: *скалярное произведение, инвариантное относительно* $T(g)$, *единственно с точностью до постоянного множителя.*

◀ Пусть $\langle\cdot,\cdot\rangle_1$, $\langle\cdot,\cdot\rangle_2$ — инвариантные скалярные произведения. Поскольку

$$\langle x, y\rangle_1 = \langle Ax, y\rangle_2, \tag{5.6}$$

[9] Иначе оператор A будет иметь нетривиальные *собственные подпространства* [4, т. 3], которые будут инвариантны относительно $T(g)$.

где A подходящий линейный оператор [10], — то

$$\langle TAx, Ty\rangle_2 = \langle Ax, y\rangle_2 = \langle x, y\rangle_1 = \langle Tx, Ty\rangle_1 = \langle ATx, Ty\rangle_2,$$

откуда

$$AT(g) = T(g)A \quad \Rightarrow \quad A = \lambda I,$$

что в итоге дает $\langle x, y\rangle_1 = \lambda\langle x, y\rangle_2$. ►

Приведенные результаты — суть разные лица общего принципа, пронизывающего теорию групп. *Нечувствительность «объекта» к группе преобразований — влечет за собой определенные последствия.*

5.5. Характеры

Характером представления $T(g)$ называется функция

$$\chi_T : G \to \mathbb{C},$$

равная *следу оператора* $T(g)$, т. е.

$$\chi_T(g) = \operatorname{tr} T(g) = \sum_i t_{ii}(g).$$

Характеры являются частным случаем так называемых *центральных функций*, принимающих постоянные значения на *классах сопряженных элементов*. Такое свойство в данном случае очевидно:

$$\chi_T(s^{-1}gs) = \operatorname{tr} T(s^{-1}gs) = \operatorname{tr} T^{-1}(s)T(g)T(s) = \operatorname{tr} T(g) = \chi_T(g).$$

Хитрость, собственно, невелика. Любая функция, не зависящая от матричного представления операторов $T(g)$ (от выбора базиса), будет центральной. Но, оказывается, справедлив более конструктивный результат.

5.5.1. Теорема. *Пусть* $\{T_1(g), \ldots, T_n(g)\}$ *— неприводимые представления группы* G. *Тогда соответствующие характеры*

$$\{\chi_{T_1}(g), \ldots, \chi_{T_n}(g)\}$$

[10] Элементы матрицы A (как в действительном, так и в комплексном случае) определяются из n^2 уравнений $\langle Ae_i, e_j\rangle_2 = \langle e_i, e_j\rangle_1$, где $\{e_i\}$ — базис.

образуют ортонормированный базис в пространстве центральных функций [11].

Теорема 5.5.1 приводит к нескольким следствиям, повышающим статус характеров:

- *Представление характера неприводимо в том и только том случае, когда* $\langle \chi_T, \chi_T \rangle = 1$.
- *Комплексное линейное представление конечной группы определяется с точностью до изоморфизма своим характером.*
- *Число неприводимых комплексных линейных представлений конечной группы равно числу ее классов сопряженных элементов.*

Подробнее с темой можно ознакомиться по небольшой книге *Винберга* [7].

[11] При условии, что скалярное произведение центральных функций определяется как

$$\langle \varphi, \psi \rangle = \frac{1}{n} \sum_{g \in G} \varphi(g) \overline{\psi(g)}.$$

Глава 6

Разрешимые группы

При первом знакомстве с предметом главу лучше не читать, потому что все просто, но не ясно «зачем». Теоремы не фиксируются в памяти, перекатываясь как ртуть. В главе 11 появится мотивация, и тогда к рассматриваемой эквилибристике можно будет вернуться с меньшим предубеждением.

Для простоты, рассматриваемые ниже группы предполагаются конечными, но этого все равно не хватает для «прозрачности». Когда нечто созревало годами, в пять минут его трудно ухватить.

6.1. Нормальные ряды

Центральное в главе понятие *разрешимой группы*, и само название, было связано с проблематикой *разрешимости в радикалах* алгебраических уравнений. Свойство разрешимости свидетельствует об иерархическом устройстве группы в том смысле, что группу можно считать «собранной» из абелевых подгрупп с помощью последовательных *расширений* [1]. Сказанное прояснится далее, пока же необходимо начать с подготовительных понятий.

6.1.1. ***Нормальным рядом*** *называется последовательность подгрупп* [2]

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\}, \tag{6.1}$$

где $G_i \neq G_{i-1}$, n — ***длина***, *а фактор-группы* G_{i-1}/G_i — ***факторы*** *нормального ряда.*

Иными словами, *нормальный ряд* это последовательность вложенных подгрупп

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{1\},$$

---

[1] Группу G называют *расширением* группы A посредством группы B, если A изоморфна некоторой нормальной подгруппе $N \subset G$, а B — изоморфна факторгруппе G/N.

[2] Напомним, $A \rhd B$ означает, что B — нормальная подгруппа A.

где каждая последующая подгруппа G_i является нормальной подгруппой предыдущей G_{i-1}, но не обязана быть нормальной подгруппой[3] G.

6.1.2. *Нормальный ряд*

$$G = F_0 \rhd F_1 \rhd F_2 \rhd \ldots \rhd F_m = \{1\}$$

называется уплотнением ряда (6.1), *если все подгруппы первого ряда встречаются во втором.*

6.1.3. *Нормальный ряд, который нельзя уплотнить, называется —* ***композиционным.***

(!) Факторы композиционного ряда являются *простыми группами* (в частности, циклическими группами простых порядков).

Всякая группа обладает тривиальным нормальным рядом $G \rhd \{1\}$. *Простая группа* не обладает нетривиальными нормальными рядами. Если в G есть нормальная подгруппа $H \subset G$, то ряд $G \rhd H \rhd \{1\}$ нормален.

6.1.4. Теорема Шрейера. *Любые два нормальных ряда группы обладают изоморфными уплотнениями.*

6.1.5. Теорема Жордана—Гёльдера. *Если группа обладает композиционными рядами, то композиционные ряды изоморфны друг другу*[4].

Вторая теорема легко выводится из первой, а первая — несложно доказывается сама по себе [16].

6.1.6. *Группа называется* ***разрешимой****, если она обладает нормальным рядом* ***с абелевыми факторами.***

Таким образом, если в G есть нормальная подгруппа $H \subset G$, то это еще не означает разрешимость G — требуется абелевость факторов

$$G/H \quad \text{и} \quad H = H/\{1\}.$$

---

[3] Иногда такие ряды называют *субнормальными*, оставляя понятие «нормального ряда» за теми ситуациями, где каждая G_i обязана быть еще нормальным делителем группы G. Кроме того, к рассмотрению обычно допускаются ряды с повторениями, $G_i = G_{i-1}$, что вынуждает дополнительно говорить о рядах без повторений. Все это имеет определенный смысл при более детальном изложении предмета.

[4] Формулировка теоремы подразумевает общую ситуацию. Для конечных групп композиционные ряды заведомо существуют.

6.1.7. *Группа разрешима в томм случае, когда все ее композиционные факторы — циклические группы простых порядков.*

6.2. Коммутанты и разрешимость

Произведение

$$aba^{-1}b^{-1}$$

называется ***коммутатором*** элементов a, b — и обозначается $[a, b]$. Очевидно,

$$ab = [a, b]ba,$$

т. е. домножение на $[a, b]$ «переставляет» сомножители. Разумеется, в коммутативном случае $[a, b] = 1$.

Легко убедиться, что

$$[a, b]^{-1} = [b, a], \qquad [a, b^{-1}] = b^{-1}[b, a]b,$$

и вообще, *любой элемент сопряженный с коммутатором,*

$$c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}], \tag{6.2}$$

является коммутатором.

Подгруппа $G^{(1)} = [G, G]$, порожденная в G всевозможными коммутаторами, называется ***коммутантом*** группы G. Иными словами, коммутант $G^{(1)}$ состоит из всевозможных произведений коммутаторов

$$[a_1, b_1] \dots [a_m, b_m], \quad a_j, b_j \in G.$$

Надо иметь в виду, что произведение коммутаторов не обязано быть коммутатором, а коммутант не обязательно состоит из коммутаторов. Однако $[G, G]$ всегда совпадает с множеством «длинных коммутаторов»:

$$g_1 \dots g_k g_1^{-1} \dots g_k^{-1}. \quad (?)$$

При этом есть примеры[5)], в которых значения k, необходимые для исчерпания коммутанта $[G, G]$, неограниченны.

[5)] *Cassidy P. J.* Products of commutators are not always commutators, an example // Amer. Math. Monthly. 1979. **86**. P. 772.

6.2.1. *В силу* (6.2) *коммутант всегда нормален*[6] *и является наименьшей в G подгруппой, фактор-группа по которой абелева.*

Абелевость фактор-групп играет принципиальную роль в теории разрешимых групп, поэтому особо выделим простой, но идеологически важный факт.

6.2.2. Лемма. *Фактор-группа G/N по нормальной подгруппе N является абелевой в том случае, когда*

$$x, y \in G \quad \Rightarrow \quad [x, y] \in N.$$

6.2.3. *Любая подгруппа $N \subset G$, содержащая коммутант $G^{(1)}$, нормальна в G.*

Коммутанты высших порядков, $G^{(k+1)} = (G^{(k)})^{(1)}$, определяют *ряд коммутантов*

$$\begin{gathered} G^{(1)} = [G, G], \\ G^{(2)} = [G^{(1)}, G^{(1)}], \quad \ldots, \quad G^{(k+1)} = [G^{(k)}, G^{(k)}], \quad \ldots, \end{gathered} \tag{6.3}$$

имеющий абелевы факторы. Чтобы ряд (6.3) был нормален, не хватает единственного условия, $G^{(n)} = \{1\}$ при некотором n. Таким образом, *если ряд* (6.3) *обрывается равенством $G^{(n)} = \{1\}$, группа G оказывается разрешимой.*

Верно также обратное. Если существует нормальный ряд (6.1) с абелевыми факторами, то таковым является и ряд коммутантов, причем $G^{(k)} \subset G_k$, что легко устанавливается по индукции[7].

• Вообще говоря, *разрешимую группу G* можно было бы определять как группу, для которой цепочка коммутантов $G, G^{(1)}, G^{(2)}, \ldots$ заканчивается при некотором n единичной группой, $G^{(n)} = \{1\}$. При этом достигается значительная экономия средств. *Нормальные ряды, фактор-группы, абелевость факторов* — все

[6] Нормален также коммутант $[N, N]$ нормальной подгруппы $N \subset G$.

[7] ◀ $G^{(1)} \subset G_1$, поскольку фактор-группа G/G_1 абелева. Далее,

$$G^{(k)} \subset G_k \;\Rightarrow\; (G_k)^{(1)} \subset G_{k+1},$$

поскольку G_k/G_{k+1} абелева. Но тогда $G^{(k+1)} \subset (G_k)^{(1)} \subset G_{k+1}$. ▶

это оказывается лишним. Но экономные пути не дают видеть «окрестности», мешая тем самым пониманию (хотя — когда как).

• *В простой группе*[8] G *все коммутанты совпадают с группой*: $G^{(1)} = G$, $G^{(2)} = G$ и т. д. Поэтому если ряд (6.3) «наталкивается» на простой коммутант $G^{(l)}$, то обрыва цепочки не происходит, поскольку $G^{(k)} = G^{(l)} \neq \{1\}$ при любом $k \geqslant l$.

Простая группа, таким образом, заведомо неразрешима. Однако наличие в G нормальной подгруппы N разрешимость G также не гарантирует — нужна абелевость факторов.

• При гомоморфизме $\varphi : G \to F$ образ коммутанта лежит в коммутанте F, т. е. $\varphi(G^{(1)}) \subset F^{(1)}$. Если же $\varphi(G) = F$, то и $\varphi(G^{(1)}) = F^{(1)}$.

• Гомоморфный образ разрешимой группы — разрешим.

• Любая подгруппа разрешимой подгруппы — разрешима.

◄ Это сразу вытекает из импликации

$$H \subset G \quad \Rightarrow \quad H^{(1)} \subset G^{(1)}, \quad H^{(2)} \subset G^{(2)}, \quad \ldots . \quad \blacktriangleright$$

• Если все нетривиальные подгруппы конечной группы G абелевы, группа G разрешима.

6.2.4. *Группа G, имеющая нормальную подгруппу N, разрешима в томм случае, когда разрешимы обе группы N и G/N.*

6.2.5. *Если N_1 и N_2 — нормальные разрешимые подгруппы группы G, то N_1N_2 — также нормальная разрешимая подгруппа группы G.*

6.3. Простые группы

Наиболее знаменитый пример простой (а значит, неразрешимой) группы — *знакопеременная группа* $\mathbf{A_n}$ при $n \geqslant 5$ — факт, играющий важную роль в *теории Галуа*.

Полная группа симметрий *икосаэдра* изоморфна группе $\mathbf{S_5}$, а подгруппа осевых симметрий — группе четных подстановок $\mathbf{A_5}$. Изоморфизм позволяет, при желании, переходить с одного языка на другой — в поиске удобных путей обсуждения.

[8] *Если абелева группа проста, то это циклическая группа простого порядка.* (?)

6.3.1. Лемма. *При $n \geqslant 3$ группа $\mathbf{A}_n$ порождается тройными циклами.*

◀ Если среди чисел i, j, k, l есть два равных, то $(ij)(kl)$ — тройной цикл. Если же i, j, k, l попарно различны, то, в силу

$$(ij)(kl) = \underbrace{(ij)(il)}\,\underbrace{(li)(kl)},$$

$(ij)(kl)$ — опять-таки тройной цикл. Поэтому любая четная подстановка представима в виде произведения тройных циклов. ▶

6.3.2. Лемма. *Если нормальный делитель N группы $\mathbf{A}_n$ содержит хотя бы один тройной цикл, то $N = \mathbf{A}_n$.*

◀ Все тройные циклы сопряжены (раздел 2.5), а нормальная подгруппа N вместе с каждым своим элементом x содержит все элементы, сопряженные x. Поэтому N порождается всеми тройными циклами. Остается сослаться на предыдущую лемму. ▶

6.3.3. Теорема. *Знакопеременная группа $\mathbf{A}_n$ при $n \geqslant 5$ является простой*[9].

◀ Ограничимся рассмотрением случая[10] $n = 5$ и покажем, что коммутатор

$$[\mathbf{A}_5, \mathbf{A}_5] = \mathbf{A}_5,$$

т. е. любой элемент из $\mathbf{A}_5$ представим в виде $aba^{-1}b^{-1}$, где $a, b \in \mathbf{A}_5$.

Циклы длины 5 в $\mathbf{A}_5$ исчерпываются представлением $(ijklm) = aba^{-1}b^{-1}$, где $a = (ijmkl)$, $b = (ij)(km)$. Циклы длины 3 охватываются разложением $(ijk) = aba^{-1}b^{-1}$, где $a = (ijk)$, $b = (jk)(lm)$, и l, m не входят в список i, j, k. Наконец, произведения $(ij)(kl)$ с попарно различными i, j, k, l укладываются в схему $(ij)(kl) = aba^{-1}b^{-1}$, где $a = (il)(jk)$, $b = (ijk)$. Легко убедиться, что разнообразие возможностей тем самым оказывается исчерпанным. ▶

6.4. Пример

Ниже рассматривается пример разрешимой группы $\{[a, b]\}$, который выглядит несколько вычурным, но именно эта группа пригодится в *теории Галуа*.

---

[9] Группа $\mathbf{A}_3$ также проста, $\mathbf{A}_4$ — нет, поскольку четные подстановки (12)(34), (13)(24), (14)(23), вместе с тождественной — составляют нормальную подгруппу $\mathbf{A}_4$, не содержащую тройных циклов. Заметим также, что $\mathbf{A}_n$ ($n \neq 4$) не исчерпывают простых конечных групп.

[10] Общее доказательство ненамного сложнее.

Множество пар целых чисел (a, b), где a ***взаимно просто с*** n, разобьем на классы $[a, b]$ по модулю n, т. е. (a_1, b_1), (a_2, b_2) принадлежат одному классу, если

$$a_1 = a_2 \pmod{n}, \quad b_1 = b_2 \pmod{n},$$

и введем групповую операцию

$$[a, b][c, d] = [ac, bc + d].$$

Получается действительно группа $\{[a, b]\}$. (?)

Рассмотрим теперь гомоморфизм $\varphi : \{[a, b]\} \to (\mathbb{Z}/n\mathbb{Z})^\times$, действующий по правилу: $[a, b] \mapsto a$. Здесь $(\mathbb{Z}/n\mathbb{Z})^\times$ обозначает мультипликативную группу классов по модулю[11] n, которая состоит из всех положительных чисел, меньших n и взаимно простых с n.

Ядро гомоморфизма φ состоит из элементов $[1, b]$, умножение которых коммутативно в силу $[1, b_1][1, b_2] = [1, b_1 + b_2]$. Поэтому ядро $\ker \varphi$ — абелево. Образ — тоже абелев. Поэтому группа $\{[a, b]\}$ — разрешима.

[11] Если n простое, то $(\mathbb{Z}/n\mathbb{Z})^\times$ совпадает с *мультипликативной группой вычетов* по модулю простого числа.

Глава 7

Определяющие соотношения

7.1. Порождающие множества

Пересечение любой совокупности подгрупп является подгруппой. (?) В том числе пересечение подгрупп, содержащих некое подмножество S группы G. Такое пересечение обозначается как $\langle S\rangle$ и называется подгруппой, *порожденной* множеством S, которое, в свою очередь, именуется *порождающим множеством.*

Легко видеть, что $\langle S\rangle$ состоит из всевозможных произведений

$$g_1^{\alpha_1}\dots g_k^{\alpha_k},$$

где все $g_i \in S$, а «показатели степени» $\alpha_i = \pm 1$.

В ситуации $\langle S\rangle = G$ говорят, что группа G *порождается* множеством S. Выделение в группе «небольшого» *порождающего множества* S обычно имеет целью сузить ассортимент «строительных блоков».

• *Симметрическую группу подстановок* $\mathbf{S_n}$ порождает любое из множеств: всевозможных циклов, *транспозиций*, *упорядоченных транспозиций* (ij), $i < j$, а также транспозиций *Мура—Коксетера*:

$$(12),\quad (23),\dots\quad ((n-1)n).\quad (?)$$

Перечисленное, разумеется, не исчерпывает возможностей. Например, $\mathbf{S_n}$ порождается одной транспозицией (12) и одним циклом $(12\dots n)$.

• *Знакопеременная группа* $\mathbf{A_n}$ порождается множеством 3-циклов.

• Группа поворотов C_n порождается одним поворотом $t = 2\pi/n$, а группа *диэдра* D_n — поворотом t и отражением r относительно одной из осей [1]. В отрыве от содержательной интерпретации на образующие t и r приходится накладывать ограничения типа $t^n = 1$, $r^2 = 1$, а также $(tr)^2 = 1$ — см. далее (раздел 7.3).

[1] Которая переходит в другие оси отражения при поворотах t^k.

7.2. Свободные группы

Свободные группы скучно выглядят, но многое освещают.

Пусть *алфавит* $\mathbb{A}$ содержит пустой символ, никак не обозначаемый, а все остальные символы входят в $\mathbb{A}$ парами: если $a \in \mathbb{A}$, то и $a^{-1} \in \mathbb{A}$, причем

$$aa^{-1} = a^{-1}a = \text{«пустому символу»},$$

т. е. рядом стоящие *обратные друг другу* символы a и a^{-1} можно «сократить».

Элементами так называемой *свободной группы* являются всевозможные слова из букв *алфавита* $\mathbb{A}$, *не содержащие рядом стоящих обратных символов*. Например, a, $daah^{-1}c$, bbb. Произведение определяется как простое слияние слов,

$$abc * ab^{-1} = abcab^{-1},$$

с учетом возможных сокращений:

$$abc^{-1} * cb^{-1}a = abc^{-1}cb^{-1}a = aa.$$

Аксиомы группы легко проверяются. Роль единицы играет пустое слово. Обратным словом, например, для abc — будет $c^{-1}b^{-1}a^{-1}$. Проверка ассоциативности более хлопотна, но это все же задача, по природе своей, для самостоятельного размышления [2)].

Алфавит $\mathbb{A}$ для свободной группы является *порождающим множеством*.

7.2.1. Теорема. *Любая группа G изоморфна некоторой факторгруппе некоторой свободной группы.*

◀ Пусть $S = \{s_\alpha\}$ — некоторое множество образующих для G. Элементам s_α поставим в соответствие символы x_α, и пусть F — свободная группа над алфавитом $\mathbb{A} = \{x_\alpha\}$. Определим далее гомоморфизм φ из F на G, сопоставляя элементам $x_\alpha \dots x_\omega \in F$ элементы $s_\alpha \dots s_\omega \in G$. По *теореме* 2.6.1 *о гомеоморфизме*

$$G \sim F/H,$$

[2)] Проблема заключается в установлении следующего факта: *результат сокращения слова не зависит от порядка сокращений*. В принципе, можно посмотреть у *Куроша* [16].

где H — нормальный делитель группы F, состоящий из слов $x_\alpha \dots x_\omega$, которые гомоморфизмом φ переводятся в слова $s_\alpha \dots s_\omega = 1$. ►

7.3. Тождества в группах

Выше отмечалось, что в группе *диэдра* D_n поворот $t = 2\pi/n$ и отражение r относительно одной из осей удовлетворяют равенствам

$$t^n = 1, \quad r^2 = 1, \quad (tr)^2 = 1. \tag{7.1}$$

Естественно, возникает вопрос: определяют ли тождества (7.1) группу D_n или только «что-то о ней говорят». Задачу можно сформулировать иначе. Пусть в группе с двумя образующими t и r выполняются тождества (7.1). Что это за группа и совпадает ли она с D_n?

◄ В данном случае проблема относительно легко решается. Из $(tr)^2 = 1$ следует: $rtr = t^{-1}$,

$$rt^k r = rt^{k-1}rrtr = rt^{k-1}rt^{-1} = \dots = t^{-k}.$$

Поэтому любое слово из t и r заменами (7.1) приводится к слову (произведению), в котором r встречается не более одного раза. С учетом опять-таки легко выводимого равенства $t^k r = rt^{n-k}$, нетрудно посчитать, что в искомой группе $2n$ элементов, — и потому она изоморфна D_n. ►

Тождества типа (7.1) называют *определяющими соотношениями* группы. Точнее говоря, пусть дано некоторое множество символов $\mathbb{A} = \{a_1, a_2, \dots\}$ и некоторая система соотношений

$$\omega_1 = 1, \quad \dots, \quad \omega_N = 1, \tag{7.2}$$

приравнивающих единице некоторые слова ω_j, записанные в алфавите $\mathbb{A}$. Эти соотношения определяют — с точностью до изоморфизма — группу G как фактор-группу F/H, где F свободная группа над алфавитом $\mathbb{A}$, а ее нормальный делитель H порожден левыми частями соотношений (7.2).

Сказанное выглядит наукообразно, но такое впечатление обманчиво. Конечно, пример соотношений (7.1) создает иллюзию, что о группе *диэдра* D_n можно говорить, не обращаясь к понятиям свободной группы и фактор-группы. Но вопрос в том — откуда начинать. Если изначально речь идет о содержательно определенной

группе D_n, то говорить о соотношениях (7.1) как об *определяющих* — нет необходимости. Если же на (7.1) смотреть как на тождества, определяющие некоторую группу G, — то поневоле приходится стать на описанную выше точку зрения.

При этом рецептура чаще всего ведет в тупик. С одной стороны, задание группы образующими и определяющими соотношениями является универсальным способом. С другой — о так заданной группе в общем случае [3] почти ничего нельзя сказать. Конечна она или бесконечна, коммутативна ли, содержит ли хотя бы один элемент кроме единицы [16]. По этой причине *определяющие соотношения* в большей степени известны сопутствующими «неприятностями». В частности, сюда относится неразрешимая проблема эквивалентности слов в группе, заданной определяющими соотношениями [4].

• Что можно сказать о группе, заданной двумя образующими a, b и соотношениями $a^4 = 1$, $b^3 = 1$? Один из способов частичного решения таких задач — моделирование.

Указанным соотношениям удовлетворяют матрицы

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

При этом элемент $ab = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ имеет бесконечный порядок,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}.$$

Отсюда вытекает, что соответствующая группа по крайней мере бесконечна.

7.4. Определяющие соотношения

В разделе 7.3 речь шла об определяющих соотношениях *в свободной группе*, и там главная проблема заключалась в выяснении того, какую группу эти соотношения определяют. На ту же проблематику возможна другая точка зрения. Рассматриваются конкретные дискретные группы и выясняется, какие соотношения их определяют.

[3] Причем — как правило.

[4] См. [4, т. 6, гл. 4], где есть беглое обсуждение и ссылки.

Пусть $G = \langle S \rangle$, и порождающее множество S состоит из элементов $s_1, \ldots, s_m$. Соотношения

$$g_k(s_1, \ldots, s_m) = 1, \quad k = 1, \ldots, r, \tag{7.3}$$

называются *определяющими*, если любое другое соотношение между порождающими элементами $s_1, \ldots, s_m$ является алгебраическим следствием (7.3). Совокупность порождающих элементов и определяющих соотношений называют *генетическим кодом*, или просто *кодом группы*, знание которого иногда существенно облегчает выяснение различных свойств изучаемых объектов [13].

7.5. Проблема Бернсайда

Для теории групп характерны значительные трудности в ответах на простые с виду вопросы. Один из таких вопросов в 1902 году поставил Бернсайд: *конечна ли конечнопорожденная группа, все элементы которой имеют конечный порядок*[5]. Отрицательный ответ[6] потребовал времени и усилий многих математиков, ибо первичный вопрос породил целую серию задач.

О *проблеме Бернсайда* и ее вариациях можно долго рассказывать. Масштабный поиск, тысячи страниц журнальной и монографической литературы. В таких случаях неискушенный читатель обычно интересуется, а зачем это нужно. Каков практический выход? И такой вопрос возникает каждый раз, когда трудозатраты несоизмеримы с *видимой* пользой. Но на плохо поставленные вопросы лучше не отвечать. Непосредственные выгоды решения сложных задач, как правило, ничтожны. Только не в них дело.

[5] Особо выделив проблему с тождеством в группе $x^n = 1$.

[6] *Голод Е. С.* О ниль-алгебрах и финитно-аппроксимируемых группах // Изв. АН СССР. Сер. Мат. 1964. **28**. С. 273–276.

Глава 8

Алгебраические структуры

Общую алгебру, как и Библию, невозможно читать подряд. Слишком многое пишется впрок, причем не только в расчете на последнюю главу, но и с прицелом в никуда.

Тем не менее сама идея «воспарить над конкретикой» понятна и жизнеспособна. Аналоги обычных арифметических действий имеются далеко за пределами числовых систем. Умножать и складывать можно многочлены, матрицы, выпуклые тела. Докуда простираются аналогии? Теорема Ферма о неразрешимости

$$x^n + y^n = z^n, \quad n > 2,$$

справедлива ли для целочисленных матриц либо многочленов? Обязана ли матрица однозначно раскладываться в произведение «простых сомножителей»?

Такого сорта вопросы не хотелось бы каждый раз решать заново, не видя взаимосвязей предметных областей. Это с одной стороны. С другой — междисциплинарные связи помогали бы видеть новые факты и подталкивали бы мысль в перспективных направлениях. Кроме того, абстрагирование от числовой специфики могло бы способствовать взгляду хотя бы на арифметику с высоты птичьего полета. Последнее крайне желательно, поскольку то и дело в предметных областях возникают попытки обобщить то, что принципиально не обобщается. При этом бесперспективность расширения тех или иных представлений — не видна обычно на приземленном предметном уровне. Алгебраический взгляд дает исчерпывающие ответы. Например:

8.0.1. Теорема Фробениуса [15]. *Поле действительных чисел и поле комплексных чисел являются единственными конечномерными действительными ассоциативно-коммутативными алгебрами без делителей нуля.*

Тело кватернионов является единственной конечномерной действительной ассоциативной, но не коммутативной алгеброй без делителей нуля [1].

На бегу результат выглядит философским развлечением. Но он очерчивает границы возможного и спасает от безнадежных попыток изобрести новое там, где Свыше не предусмотрено. Это, между прочим, гораздо важнее решения конкретных задач, ибо в иерархии научных целей на первом месте стоит понимание того, куда можно и нужно двигаться, минуя «квадратуру круга». Владея инструментом, полезно осознавать его происхождение и возможности. В противном случае интеллектуальная мощь уходит на мистические восторги, подобные тем, которые сопровождали рождение комплексных чисел.

8.1. Куда ведет абстрагирование

Абстракция выглядит тайной, пока привычка не смывает налет мистики. Цивилизация продолжает медитировать над комплексными числами, но ощущение глубины постепенно мелеет. А вот натуральный ряд уже достиг рубежа тривиальности. Но так было не всегда.

Пример аборигенов Сахалина, до недавнего времени имевших разные числительные для круглых предметов и продолговатых, весьма показателен [2]. Нам такое уже трудно представить. Понятие абстрактного числа стало банальностью. Этаким кирпичиком мировоззрения, вообразить отсутствие которого почти невозможно. Поэтому говорить о глубине и величии понятия *Числа* сегодня сложно. Уже никто не понимает — все привыкли. Но есть другие абстракции, которые пока находятся как бы на другой стадии. То ли — в процессе, то ли — не все население с ними имеет дело. И там есть возможность посмотреть на ситуацию свежим взглядом.

- Формула *Кардано* для решения кубического уравнения

$$x^3 + px + q = 0 \tag{8.1}$$

[1] Наконец, *алгебра Кэли* [15] — единственная конечномерная действительная альтернативная, но не ассоциативная алгебра без делителей нуля.

[2] Далее приводятся некоторые фрагменты из [3].

имеет вид

$$x_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{2} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{2} + \frac{p^3}{27}}},$$

при определенном согласовании возможных комбинаций кубических корней.

В случае

$$\frac{q^2}{2} + \frac{p^3}{27} < 0$$

все три корня уравнения (8.1) обязательно вещественны, но рецепт их получения связан с использованием мнимых величин

$$\sqrt{\frac{q^2}{2} + \frac{p^3}{27}}.$$

• Остаток от деления многочлена $P_n(x)$ на $x^2 + px + q$ может быть найден следующим образом. Если

$$x^2 + px + q = (x - a)(x - b),$$

то

$$P_n(x) = (x - a)(x - b)Q_{n-2}(x) + \gamma x + \delta. \tag{8.2}$$

Подставляя в (8.2) $x = a$, потом $x = b$, получаем систему уравнений

$$\begin{cases} P_n(a) = \gamma a + \delta, \\ P_n(b) = \gamma b + \delta \end{cases}$$

для определения γ и δ.

Интересно, что при отсутствии у полинома $x^2 + px + q$ действительных корней решение задачи вынужденно пролегает через использование комплексных чисел $P_n(a)$, $P_n(b)$.

• Еще один пример. Числовая последовательность a_n

$$1, 1, 0, -2, -4, -4, 0, 8, 16, 16, 0, -32, \ldots$$

устроена по правилу

$$a_{n+2} = 2a_{n+1} - 2a_n, \quad a_0 = a_1 = 1. \tag{8.3}$$

Подстановка $a_n = x^n$ в (8.3) приводит к квадратному уравнению

$$x^2 - 2x + 2 = 0,$$

которое имеет комплексные корни $x_1 = 1 + i$, $x_2 = 1 - i$.

Общим решением (8.3) является $a_n = c_1 x_1^n + c_2 x_2^n$. Константы c_1, c_2 определяются из начальных условий ($a_0 = a_1 = 1$). В результате

$$a_n = \frac{(1 + i)^n + (1 - i)^n}{2},$$

или, с учетом обычных тригонометрических ухищрений,

$$a_n = (\sqrt{2})^n \cos \frac{n\pi}{4}. \tag{8.4}$$

Ни условие, ни ответ (8.4) не содержат и намека на комплексные числа. Другое дело, промежуточные вычисления, где мелькает мнимая единица i. Что это — фокус, фикция? Игрушечная модель, без которой можно обойтись, или существенный атрибут исходной задачи?

Первое, что приходит в голову, — это фикция. Вспомогательный прием. И нет, мол, никакого особого смысла выяснять, существуют ли комплексные числа на самом деле. Они существуют как мысленный инструмент. Вот, дескать, и вся правда.

Однако не вся. Тут дело не только в удобствах, которые дают комплексные числа. Здесь затрагивается какой-то глубинный механизм — поначалу неясно какой. Добавление к гармоническому колебанию

$$U(t) = U \cos \omega t$$

фиктивной мнимой части,

$$\widehat{U}(t) = U(\cos \omega t + i \sin \omega t),$$

странным образом резко упрощает теорию колебаний. Как бы обнаруживается счастливое стечение обстоятельств. Законы электродинамики и правила умножения комплексных чисел проявляют неожиданную согласованность.

Или кто скажет, почему ряд

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - \dots .$$

сходится только при $x| < 1$? Никаких особых точек нет, знаменатель в нуль не обращается — на действительной оси. Особая точка есть, правда, в комплексной плоскости, $x = i$ ($|x| = 1$). Но с какой стати точка $x = i$ управляет сходимостью ряда от действительной переменной?

И выходит, что мнимая единица, как тень, все время присутствует за кадром. Надзирает и определяет, хотя явно не вмешивается. Мистика?

Ответ — и прост, и сложен. Прост — потому что легко формулируется и часто повторяется. Сложен — потому что слишком прост. Чтобы уяснить наличие общности в ситуациях «три пальца» и «три дня», человечеству потребовалось очень много времени. Здесь тоже необходимо время, хотя, если разобраться, непонятно — на что.

Все начинается с натурального ряда и введения двух операций: сложения и умножения. Из посаженного семени остальное вырастает само. Сначала естественным образом появляются обратные операции, вычитание и деление, влекущие за собой необходимость введения ряда

$$\ldots, -2, -1, 0, 1, 2, \ldots,$$

потом дробей. Расширение исходного объекта манипуляций происходит сравнительно безболезненно, потому что в окружающем мире есть в избытке готовые интерпретации. А это культивирует не тот источник абстрагирования. Потребность в отрицательных числах имеет гораздо более весомую причину, чем запись долга со знаком минус. Дело в том, что манипулирование числами на определенной стадии выводит на следующий уровень абстракции. Для однотипных действий начинает использоваться символьная запись[3]. Введение буквенных обозначений переводит арифметику на другие рельсы. Формулы типа

$$(a-b)(a+b) = a^2 - b^2$$

фокусируют внимание на операциях. Объекты, т. е. пока числа, остаются за бортом, за кадром. Выводятся из поля зрения. Первостепенными становятся действия, а не объекты их приложения[4]. Тем не менее множество потенциально возможных объектов должно быть не пусто, чтобы рассматриваемые операции имели смысл. Отрицательные и дробные числа нужны для того, чтобы уравнения

$$x + a = b, \quad ax = b$$

всегда решались. Вот, собственно, главная причина. Аналогичная ситуация возникает в связи с извлечением корней, что однозначно приводит к появлению комплексных чисел. При поверхностном

[3] Это колоссальный скачок в мышлении. На него ушли века.

[4] Как бы начинают изучаться глаголы в отрыве от существительных.

взгляде может показаться, что на этом пути появляются только мнимые числа, но это не так. Начатое дело приходится доводить до конца: $\sqrt{-1} = \pm i$, но возникающие объекты должны умножаться и складываться, что легализует числа вида $a + bi$.

Итак, никакого секрета, никакой мистики. Комплексные числа — *такая же реальность, или такая же фикция*, — кому как больше нравится, как отрицательные или дробные числа. Некоторый дискомфорт имеется лишь по причине укоренившейся привычки искать в окружающем мире прообразы типа шкалы термометра, где отрицательные числа находят свое воплощение.

Разумеется, необходимо ответить, почему комплексные числа «неожиданно» всплывают в самых разных областях. Да потому, что вся математика стоит на использовании сложения и умножения, для которых комплексная плоскость — неизбежный финал расширения натурального ряда. Поэтому игровое поле и для бесконечных рядов, и для дифуров, и для теории вероятностей — одно и то же.

Отмеченная выше человеческая потребность в реальных прообразах абстрактных понятий — и плоха, и хороша одновременно. С одной стороны, она мешает видеть ясную логическую картину, с другой — активизирует поиск наглядных инструментов и конструкций. С одной стороны, комплексные числа — это элементы вида

$$z = x + iy, \tag{8.5}$$

удовлетворяющие условию $i^2 = -1$, обычным правилам сложения, умножения, — и этим все сказано. С другой стороны, разочарованное подсознание ищет наглядности — и возникают попытки эквивалентных представлений, что приносит свои плоды типа

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

Итак, постепенное расширение натурального ряда последовательно приводит к появлению отрицательных, рациональных, действительных[5)], наконец, комплексных чисел. Процесс идет под

[5)] С действительными — есть крупная натяжка. Там, вообще говоря, внедряется как бы посторонняя идея непрерывности (неалгебраический вирус). В результате задним числом возникают все эти дополнительные разговоры об алгебраических и трансцендентных числах.

контролем идеологии выполнимости алгебраических операций и однозначно заканчивается на комплексных числах — дальше пути нет.

При увеличении размерности чисел теряются те или иные свойства: при переходе от действительных чисел ($n = 1$) к комплексным ($n = 2$) пропадает упорядоченность, следующий шаг к *кватернионам* ($n = 2^2$) связан с потерей коммутативности умножения, наконец, при переходе к числам Кэли ($n = 2^3$) теряется ассоциативность умножения.

Закономерно возникает вопрос. А что если начинать не с натурального ряда, а с чего-то другого? При этом, правда, становится неясно, что такое сложение и умножение. Но пусть это будут какие-то операции, удовлетворяющие тем же свойствам типа

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

И даже свойства пусть будут другие, и даже операция всего одна... или, наоборот, три... Так происходит прорыв в другую нишу — рождается абстрактная алгебра.

8.2. Кольца, тела, поля

8.2.1. ***Кольцом*** *называется множество X с двумя бинарными операциями, сложения $+$ и умножения $\cdot$, при условии:*

- *X — коммутативная группа по сложению (**аддитивная группа кольца**).*
- *Умножение ассоциативно.*
- *Выполняется дистрибутивный закон,*

$$p \cdot (q + r) = p \cdot q + p \cdot r,$$
$$(q + r) \cdot p = q \cdot p + r \cdot p,$$

определяющий взаимодействие сложения и умножения.

Ряд свойств типа

$$p \cdot (q - r) = p \cdot q - p \cdot r,$$
$$p \cdot 0 = 0 \cdot p = 0,$$

попадают в разряд следствий перечисленного. Элемент $q - r$ определяется как решение уравнения $r + x = q$.

В случае коммутативности умножения кольцо называют *коммутативным*, а если в X есть единица по умножению, говорят о ***кольце с единицей***[6]. Иногда требование ассоциативности умножения опускают в определении, и тогда возникает еще понятие *ассоциативного кольца*.

Примерами колец в первую очередь служат различные числовые системы: действительная прямая $\mathbb{R}$, комплексная плоскость $\mathbb{C}$, множество $\mathbb{Q}$ рациональных чисел, множество $\mathbb{Z}$ целых чисел (включая отрицательные). Менее привычные примеры: множество квадратных матриц и множество многочленов с обычными операциями сложения и умножения.

• *Кольцо многочленов* $R[x]$ подразумевает в качестве элементов формальные выражения

$$P_n(x) = p_0 x^n + \ldots + p_{n-1} x + p_n$$

с коэффициентами p_k из некоторого кольца R (при этом говорят о кольце многочленов *над* R). Природа элементов x несущественна. Операции определяются по обычным правилам сложения и умножения многочленов, что порождает *коммутативное кольцо с единицей*.

• *Кольцо квадратных матриц* также можно рассматривать *над* некоторым кольцом R, подразумевая, что элементы матриц берутся из R. Сложение и умножение матриц при этом происходит по обычным матричным формулам с интерпретацией операций в R.

• Числа вида $a + b\sqrt{2}$ с рациональными (в другом варианте — с целыми) a и b образуют кольцо. Но $a + b\sqrt[3]{2}$ с рациональными a и b кольца не образуют. Кольцо образуют числа вида

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}, \quad a, b, c \in \mathbb{Q}. \quad (?)$$

Интересный пример кольца дает $\mathbb{R}^3$ с обычным сложением векторов и векторным умножением $x \times y$ в качестве второй операции. В этом кольце, как известно [4, т. 1, т. 3],

$$x \times x = 0,$$

[6] $\mathbb{Z}$ — кольцо с единицей, а все четные числа — кольцо без единицы.

и выполняется *тождество Якоби*

$$(a \times b \times c) \times b + (b \times c) \times a = 0.$$

Всякое кольцо, в котором $x^2 = 0$ и справедливо *тождество Якоби* по умножению, называется *лиевым кольцом* (*кольцом Ли*).

Если в произвольном кольце, «не трогая» сложение, заменить умножение *операцией коммутирования*

$$a * b = a \cdot b - b \cdot a,$$

получается *лиево кольцо*. **(?)**

Определение кольца не исключает ситуаций $a \cdot b = 0$ при ненулевых a, b. Такие элементы кольца называются *делителями нуля* (*левыми*, *правыми*). Кольца (а также области кольца) без делителей нуля (при условии $1 \neq 0$) называются *целостными*.

По двум кольцам X, Y можно строить их *прямую сумму* $X \oplus Y$, состоящую из всевозможных пар (x, y), $x \in X$, $y \in Y$. Сложение и умножение в $X \oplus Y$ определяется «покоординатно». В прямой сумме всегда есть делители нуля:

$$(x, 0) \circ (0, y) = (x \cdot 0, 0 * y) = (0, 0).$$

Ненулевое кольцо (не состоящее только из нуля) не может быть группой по умножению из-за $p \cdot 0 = 0 \cdot p = 0$. Однако ненулевые элементы кольца могут составлять *группу по умножению* (*мультипликативную группу*). В этом случае кольцо называется ***телом***. *Тело с коммутативным умножением* называется ***полем***[7]. Поле вместе с любыми двумя элементами a, b содержит также ab, $a + b$, $a - b$ и a/b (при условии $b \neq 0$)[8]. Что такое *подкольца* и *подполя*, объяснять, видимо, не надо.

Структура поля гарантирует разрешимость линейных уравнений, что обычно требуется в приложениях и выделяет поля в особо благоприятные объекты изучения.

[7] В любом поле имеется *единица по умножению*. (?) Эквивалентное определение: *полем* называется ненулевое коммутативное кольцо, в котором разрешимо любое уравнение $ax = b$ при $a \neq 0$.

[8] Элемент $x = a/b$ определяется как решение уравнения $bx = a$.

8.3. Идеалы

Подмножество $I \subset X$ называется *идеалом* кольца X, если оно является подгруппой аддитивной группы кольца[9] и $a \in I$, $x \in X$ влечет за собой $ax \in I$ и $xa \in I$.

• Вообще говоря, рассматривают также *левые* ($a \in I$, $x \in X \Rightarrow ax \in I$) и *правые* ($a \in I$, $x \in X \Rightarrow xa \in I$) идеалы, называя идеалы в данном выше определении — *двусторонними*.

• Подмножество $k\mathbb{Z} = \{kz : z \in \mathbb{Z}\}$ всех целых чисел, кратных некоторому k, — идеал в $\mathbb{Z}$. (?) Аналогичный трюк работает и в других обстоятельствах. Например,

$$k(x)P[x] = \{k(x)p(x) : p(x) \in P[x]\},$$

где $P[x]$ кольцо полиномов, а $k(x)$ фиксированный полином, — идеал в $P[x]$.

• Ненулевое коммутативное кольцо R является полем в томм случае, когда в R нет других идеалов, кроме $\{0\}$ и самого R. (?)

Роль идеалов в теории колец аналогична роли нормальных подгрупп в теории групп. Аналогия сохраняется и по другим направлениям. Во избежание недоразумений дадим все же несколько определений.

Два кольца R и Q называются ***изоморфными***, если между их элементами можно установить взаимно однозначное соответствие $\varphi : R \to Q$, такое что

(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$,

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$

для любых $x, y \in R$.

Изоморфные кольца *эквивалентны* ($R \sim Q$) с точки зрения их алгебраических свойств.

Если в определении изоморфизма отображение $\varphi : R \to Q$ не обязательно взаимно однозначно, говорят о *гомоморфном* отображении кольца R в Q, а φ называют ***гомоморфизмом***. Если речь идет о *кольцах с единицей*, то в дополнение к (i), (ii) предполагается:

[9] Для чего достаточно: $a, b \in I \Rightarrow a - b \in I$ (п. 2.1.3).

$\varphi(1) = 1$. Свойства $\varphi(-x) = -\varphi(x)$, $\varphi(0) = 0$ оказываются следствиями определения.

Сюръективный гомоморфизм $\varphi : R \to Q$, отображающий R *на* Q, называется ***эпиморфизмом.***

Совокупность всех элементов из R, переходящих в нуль кольца Q, называется *ядром гомоморфизма* $\varphi : R \to Q$ и обозначается как $\ker\varphi$. *Ядро* $\ker\varphi \subset R$ *гомоморфизма колец,* $\varphi : R \to Q$, *обязательно является идеалом кольца* R.

• Гомоморфизм одного поля в другое является или изоморфизмом, или переводит все элементы одного поля в нуль — другого. (**?**)

Фактор-кольцом кольца R по идеалу I называется множество

$$R/I = \{r + I : r \in R\}$$

смежных классов по I. Сложение в R/I определяется как в факторгруппе, а умножение — по правилу:

$$(r + I)(s + I) = rs + I \quad (r, s \in R).$$

Смежные классы $r + I$ при этом называют *классами вычетов по модулю идеала*, или короче — *классами вычетов по* I.

• Принадлежность x, y одному и тому же классу $r + I$ записывается как $x = y \pmod I$, что равносильно $x - y = I$.

• Если $x = y \pmod I$ и $u = v \pmod I$, то и

$$xu = yv \pmod I, \quad x + u = y + v \pmod I,$$

т. е. сравнения по модулю можно складывать и умножать.

• Фактор-кольцо является кольцом, но лишь в случае, когда идеал двусторонний [10]. Аналогично тому как фактор-группа есть группа лишь по нормальной подгруппе.

• ***Теорема о гомеоморфизме колец.*** *Фактор-кольцо* $R/\ker\varphi$ *по модулю ядра гомеоморфизма* $\varphi : R \to Q$ *изоморфно образу* $\varphi(R)$.

[10] Что в данном выше определении идеала подразумевается автоматически.

8.3.1. Теорема[11]. *Фактор-кольцо R/I коммутативного кольца с единицей является полем в томм случае, когда I — максимальный идеал*[12].

Аналогия с теоретико-групповым сценарием простирается далее. Нуль и само кольцо R являются идеалами (тривиальными). Кольцо *без нетривиальных* идеалов называется *простым*[13].

Наименьший (по включению) *идеал*, содержащий множество $M \subset R$, считается *порожденным* множеством M. *Идеал* $I(a)$, порожденный одним элементом a, называется *главным*. В коммутативном кольце с единицей

$$I(a) = \{ra : r \in R\}.$$

Если все идеалы в R главные, — R называется *кольцом главных идеалов*, каковым является кольцо $\mathbb{Z}$, а также кольцо всех многочленов от одного переменного с коэффициентами из любого данного поля.

Примеры идеалов:

$$k\mathbb{Z} = \{kz : z \in \mathbb{Z}\},$$

числа кратные k; и

$$k(x)P[x] = \big\{k(x)p(x) : p(x) \in P[x]\big\},$$

полиномы кратные полиному $k(x)$, — создают впечатление, что идеалы «паразитируют» на кратности, не привнося ничего нового. Это не так. Пусть $\mathbb{R}[x]$ обозначает кольцо полиномов от n переменных, т. е.

$$\mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n],$$

и $k_1(x), k_2(x)$ два фиксированных полинома из $\mathbb{R}[x]$. Тогда совокупность полиномов

$$k_1(x)p_1(x) + k_2(x)p_2(x), \quad \forall\, p_1(x), p_2(x) \in \mathbb{R}[x], \tag{8.6}$$

---

[11] Результат фактически обоснован при доказательстве теоремы 9.4.1.

[12] Идеал I в кольце R считается *максимальным*, если не существует идеала I', такого что $I \subset I' \subset R$ $(I \neq I', R)$.

[13] Любое поле — простое кольцо. *Простое коммутативное кольцо с единицей — поле.* ◀ $aR = R$ для любого ненулевого $a \in R$, поскольку кольцо простое. Но тогда найдется такое b, что $ab = 1$, т. е. $b = a^{-1}$. ▶

является *идеалом* в $\mathbb{R}[x]$ — далеко не надуманного характера. Полиномы (8.6) обращаются в нуль на пересечении поверхностей

$$k_1(x_1, \ldots, x_n) = 0, \quad k_2(x_1, \ldots, x_n) = 0,$$

содействуя тем самым изучению $(n-1)$-мерных алгебраических многообразий. «Механизм кратности» здесь не работает. Варианты с выбором большего числа фиксированных полиномов — очевидны.

8.4. Евклидовы кольца

Структура кольца высвечивает в изучаемых объектах лишь определенные ракурсы. Поэтому ассоциации и аналогии бывают обманчивы. Скажем, *основная теорема арифметики* о единственности разложения на простые множители за пределами натурального ряда часто неверна — кольцевой аксиоматики оказывается недостаточно. Кольцо кольцу, так сказать, рознь. Одна из продуктивных идей дополнительной типизации — введение своеобразной нормы.

8.4.1. Определение. *Кольцо R без делителей нуля называется* ***евклидовым****, если*:

(i) *для ненулевых $a \in R$ определена целочисленная норма $N(a) > 0$, $N(0) = 0$, причем*

$$N(ab) \geqslant \max\{N(a), N(b)\};$$

(ii) *для любых $a, b \neq 0$ существует представление $a = qb + r$, в котором либо $r = 0$, либо $N(r) < N(b)$.*

В кольце целых чисел $\mathbb{Z}$ нормой может служить $N(z) = |z|$. В кольце $P[x]$ в качестве нормы годится степень многочлена.

Любое *евклидово кольцо* имеет единицу и является кольцом *главных идеалов*. (?) Все это затевается в основном для теории делимости. В кольце главных идеалов *наибольший общий делитель* $d = (f, g)$ элементов $f, g \in R$ выражается в виде линейной комбинации

$$(f, g) = uf + vg, \quad u, v \in R.$$

В частности, элементы $f, g \in R$ взаимно просты в том случае, когда можно подобрать такие $u, v \in R$, что

$$uf + vg = 1.$$

Обоснование дано в разделе 9.2 на примере многочленов. Схема рассуждений в общем случае не меняется — главным инструментом остается *алгоритм деления Евклида.*

• Любой элемент евклидова кольца единственным образом раскладывается в произведение простых сомножителей. (**?**)

8.5. Поля вычетов

Основные примеры полей: поле действительных чисел $\mathbb{R}$, рациональных $\mathbb{Q}$ и комплексных $\mathbb{C}$. Полем являются дробно-рациональные функции $\dfrac{p(x)}{q(x)}$, где $p(x)$ и $q(x) \neq 0$ — полиномы с действительными коэффициентами. Полями являются также различные *фактор-кольца* (теорема 8.3), составляющие особую статью (полей вычетов).

Если в *аддитивной группе* $\mathbb{Z}_p^+$ *вычетов по модулю* p (число p простое [14]) помимо сложения ввести еще и умножение, полагая $a \cdot b$ равным остатку от деления обычного произведения a и b на p, — то *классы вычетов по модулю* p образуют поле [15], тогда как кольцо $\mathbb{Z}$ поля не образует. Расширенная до поля $\mathbb{Z}\,(\mathrm{mod}\,p)$ группа $\mathbb{Z}_p^+$ является, по сути, фактор-кольцом $\mathbb{Z}/p\mathbb{Z}$.

В рассмотренном случае принципиальную роль играет ***характеристика поля*** P, каковой называется минимальное p в равенстве

$$\underbrace{1+\ldots+1}_{p\text{ раз}} = 0, \tag{8.7}$$

где 1 — единица поля P. Если (8.7) невозможно, P называют ***полем характеристики нуль*** [16].

[14] В случае составного p класс вычетов по модулю p будет кольцом (имеющим делители нуля, $3 \cdot 2 = 0$ в $\mathbb{Z}_6$), но не полем.

[15] Доказательство не так уж просто — см. раздел 2.1. В качестве упражнения: *уравнение* $q \cdot x = 1\ (\mathrm{mod}\,p)$ *разрешимо в* $\mathbb{Z}$, *если* p *простое и* q *не делится на* p. (**?**)

[16] Иными словами, характеристика поля совпадает с порядком единицы аддитивной группы поля, если порядок конечен, и считается равной нулю, если порядок бесконечен.

• Конечное *поле классов вычетов по модулю* p имеет характеристику p.

• *Ненулевая характеристика* p *всегда является простым числом.*

◄ В противном случае $p = s \cdot t$, $s < p$, $t < p$, — в силу $p \cdot 1 = 0$ было бы либо $s \cdot 1 = 0$, либо $t \cdot 1 = 0$, что противоречило бы минимальности p. ►

• Если поле P имеет характеристику p, то $p \cdot x = 0$ для любого $x \in P$.

• Числовые поля $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ имеют *характеристику нуль.*

Поля вычетов могут быть в той или иной степени непохожи на $\mathbb{Z} \pmod p$. Допустим, $p(x)$ — простой элемент (аналог простого числа — *неприводимый полином*) в кольце полиномов $P[x]$. *Если* $f(x) \in P[x]$ *не делится на* $p(x)$, *то в* $P[x]$ *существует полином* $f^{-1}(x)$, *такой что* [17]

$$f(x)f^{-1}(x) = 1 \pmod{p(x)},$$

т. е. $f(x)f^{-1}(x) - 1$ *делится на* $p(x)$.

Поэтому отождествление элементов $f(x), g(x) \in P[x]$, разность которых делится на $p(x)$, превращает кольцо $P[x]$ в *поле вычетов* $P[x] \pmod{p(x)}$. В частности, $\mathbb{R}[x] \pmod{x^2 + 1}$ — есть $\mathbb{C}$ с точностью до изоморфизма.

8.6. Алгебры

Алгеброй A над P называют кольцо, в котором дополнительно определено умножение на «числа» [18] из некоторого поля P, причем

$$\lambda(ab) = (\lambda a)b = a(\lambda b), \quad a, b \in A, \quad \lambda \in P,$$

и *аддитивная группа* кольца является *векторным пространством*, т. е.

$$a, b \in A, \quad \lambda, \mu \in P \quad \Rightarrow \quad \lambda a + \mu b \in A.$$

Размерность упомянутого «векторного пространства» называют *рангом алгебры* A. Алгебры конечного ранга именуют также *гиперкомплексными системами*. Если алгебра является *лиевым кольцом*, то она называется *алгеброй Ли.*

[17] Это *теорема Евклида.*

[18] «Числа» — элементы поля P, не обязательно числового.

Идеал кольца I считается также *идеалом алгебры*, но при условии, что он выдерживает умножение на элементы поля P. Если в фактор-кольце A/I ввести умножение на элементы $\lambda \in P$ по правилу $\lambda(x + I) = \lambda x + I$, получается алгебра над P, называемая *фактор-алгеброй* A по идеалу I.

В определение *гомоморфизма алгебр* $\varphi : A \to B$ помимо обычных требований для гомеоморфизма колец входит условие

$$\varphi(\lambda x) = \lambda\varphi(x), \quad \lambda \in P.$$

Примеры *алгебр* более-менее очевидны. Всякое поле является алгеброй ранга 1 над самим собой [19]. Алгебрами являются $\mathbb{R}^3$ с обычным сложением векторов, векторным умножением $x \times y$ и обычным умножением вектора на число; множество квадратных матриц с элементами из $\mathbb{C}$, обычными операциями сложения и умножения матриц и умножением матрицы на комплексное число.

Особого упоминания заслуживает *алгебра кватернионов* — четырехмерных объектов вида

$$Z = \alpha + i\beta + j\gamma + k\delta,$$

где $\alpha, \beta, \gamma, \delta$ — действительные числа, а $1, i, j, k$ — четыре базисные единицы, удовлетворяющие соотношениям

$$\boxed{i^2 = j^2 = k^2 = ijk = -1,}$$

откуда (с учетом того, что 1 — обычная единица) следует

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -jk = j,$$

что в совокупности дает таблицу умножения базисных элементов, и совпадает с правилами векторного умножения единичных ортов $\{i, j, k\}$ в $\mathbb{R}^3$. Сложение и умножение на число определяется обычным (для векторных пространств) образом. Кватернионы вида $x \cdot 1 + y \cdot i$ образуют *подалгебру*, изоморфную алгебре комплексных чисел над полем — действительных.

Группа кватернионного базиса

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

[19] *Рангом алгебры* называется размерность векторного пространства, которое служит аддитивной группой алгебры.

состоящая из 8 элементов и имеющая 6 подгрупп, служит стандартным примером *гамильтоновой группы*[20].

Единицы $1, i, j, k$ могут быть «изоморфно» представлены матрицами:

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}, \begin{bmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{bmatrix}, \begin{bmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{bmatrix}, \begin{bmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{bmatrix}.$$

Кватернионы представляют интерес в связи с *теоремой Фробениуса* (п. 8.0.1). Естественный вопрос о существовании над $\mathbb{R}$ алгебры ранга больше 2 имеет дихотомический ответ: если коммутативную, то — нет, если некоммутативную, то — да (и вариант всего один — *алгебра кватернионов*).

8.7. Булевы структуры

Булева алгебра известна в широких кругах как вторичная дисциплина по отношению к математической логике [4, т. 6]. Реальное положение дел несколько иное.

Булевой структурой обычно называют множество $\mathcal{B}$ с двумя операциями: «сложения $+$» и «умножения $\times$»[21], удовлетворяющие следующим требованиям:

- Обе операции коммутативны и ассоциативны.
- Операции дистрибутивны одна относительно другой, т. е. помимо обычного (для кольца)
$$(x+y)\times z = x\times z + y\times z,$$
справедливо
$$(x\times y)+z = (x+z)\times(y+z).$$
- В $\mathcal{B}$ существуют элементы 0 и 1:
$$x+0=x, \quad x\times 1 \doteq x.$$
- Любому элементу $x\in\mathcal{B}$ отвечает такой элемент $\bar{x}\in\mathcal{B}$, что:
$$x+\bar{x}=0, \quad x\times\bar{x}=1,$$

[20] Группа называется *гамильтоновой*, если все ее подгруппы нормальны.

[21] Которое, как обычно, обозначается также точкой $\cdot$, либо «никак».

иначе говоря, *обратным* элементу x, как по сложению, так и по умножению, оказывается один и тот же элемент $\bar{x}$. Операцию «$\bar{}$», как правило, называют *отрицанием*, либо *дополнением*.

Операции «сложения» и «умножения», как легко заметить, равноправны с точки зрения аксиоматических требований. По этой причине в булевых структурах действует *принцип двойственности*: *всякая булева теорема при замене*

$$+ \leftrightarrow \times, \quad 0 \leftrightarrow 1$$

переходит в двойственную теорему.

Рассматриваемой области присущ определенный люфт, в пределах которого встречаются различные вариации определений, с добавлением некоторых малосущественных свойств. Помимо этого, значительным вариациям подвержена сама форма определений, в результате чего *булевы алгебры* у разных авторов бывают совсем не похожи друг на друга.

Одна из широко известных модельных реализаций булевой алгебры — матлогика на игровом поле $\{$*истина*, *ложь*$\}$ с дизъюнкцией и конъюнкцией в качестве «сложения» и «умножения». Другая модель, имеющая универсальный характер, множество $\mathcal{B}$ и некоторая система его подмножеств $\mathscr{B}$ с обычными операциями объединения, пересечения и дополнения,

$$x + y \Leftrightarrow x \cup y, \quad xy \Leftrightarrow x \cap y, \quad \bar{x} \Leftrightarrow E \setminus x.$$

Если $\mathscr{B}$ состоит всего из двух подмножеств, $\mathscr{B} = \{\varnothing, \mathcal{B}\}$, возникает ситуация, изоморфная матлогике.

Реализация булевой алгебры как системы подмножеств некоторого множества и универсализм такой модели настраивают на заключении, что этим все сказано. Но это далеко не так. Модели иной природы (хотя и изоморфные теоретико-множественной интерпретации) обнаруживают в тех же структурах совершенно другие аспекты. Например, булева структура возникает при введении операций

$$x + y = \text{НОК}\{x, y\}, \quad x \cdot y = \text{НОД}\{x, y\}, \quad \bar{x} = \frac{N}{x}$$

на *множестве делителей* некоторого числа N, которое представляет собой произведение простых чисел в первой степени. Такая алгебра играет определенную роль в теории чисел.

Близкая к булевым структурам система возникает при введении на отрезке $[0, 1]$ операций:

$$x + y = \max\{x, y\}, \quad x \cdot y = \min\{x, y\}, \quad \overline{x} = 1 - x.$$

Выполняются все аксиомы кроме последней.

Модели подключают к анализу факты, добытые в других областях, и обогащают друг друга, расширяя заодно представления о гибкости и вместимости абстрактной схемы.

Глава 9

Многочлены

Многочлены далее — не самоцель, хотя объект, безусловно, поучительный. Особенно — в тандеме с алгебраическими числами, и вообще — полями. При этом возникают удобные поводы обсудить некоторые аспекты алгебраического стиля мышления, и заодно — разгрузить *теорию Галуа* от технических подробностей, которые иногда представляют самостоятельный интерес.

9.1. Напоминания

Многочленом, или *полиномом*, *над полем* K называется формальное выражение

$$f_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \qquad (9.1)$$

где $a_0, \ldots, a_n \in K$. Далее, как правило, имеются в виду числовые поля. Сумма и произведение многочленов определяются по обычным правилам сложения и умножения (с приведением подобных), что порождает *кольцо* [1] *многочленов* $K[x]$. Природа «переменной» x несущественна, но в принципе x может принадлежать тому же или другому полю, либо оставаться просто символом. Последний вариант дает наиболее общую точку зрения.

На обозначении $K[x]$ имеет смысл задержать внимание: $\mathbb{R}[x]$ — кольцо многочленов всех степеней с действительными коэффициентами, $\mathbb{Q}[x]$ — с рациональными, $\mathbb{Z}[x]$ — с целыми коэффициентами.

Деление «в столбик»,

$$\begin{array}{rl} x^3 - 3x^2 + 5x + 6 & \big|\underline{x - 1} \\ \underline{x^3 - x^2} & x^2 - 2x + 3 \\ \quad -2x^2 + 5x & \\ \quad \underline{-2x^2 + 2x} & \\ \qquad 3x + 6 & \\ \qquad \underline{3x - 3} & \\ \qquad\quad 9 & \end{array}$$

[1] Но не поле.

приводит к тождеству

$$x^3 - 3x^2 + 5x + 6 = (x - 1)(x^2 - 2x + 3) + 9.$$

Легко видеть, что в общем случае деление многочлена (9.1) на $(x - c)$ даст в частном некоторый многочлен $h_{n-1}(x)$ и некоторое число r в остатке, т. е.

$$\begin{array}{l|l} f_n(x) & \underline{x - c} \\ \vdots & h_{n-1}(x) \\ \overline{r}\,, & \end{array}$$

что равносильно тождеству

$$f_n(x) = (x - c)h_{n-1}(x) + r,$$

полагая в котором $x = c$, получаем *теорему Безу*: *остаток* r *при делении* $f_n(x)$ *на* $(x - c)$ *равен* $f_n(c)$, *т. е.*

$$\boxed{r = f_n(c).}$$

Таким образом, если $x = c$ — *корень уравнения* $f_n(x) = 0$, то $r = 0$. В конечном итоге это соображение приводит к разложению

$$f_n(x) = a_0(x - x_1)(x - x_2)\ldots(x - x_n), \tag{9.2}$$

где $x_1, \ldots, x_n$ — корни многочлена $f_n(x)$, которые по *основной теореме алгебры* всегда существуют в комплексной плоскости, — если $f_n(x)$ рассматривается как многочлен над $\mathbb{C}$. В общем случае проблема разрешимости уравнения $f_n(x) = 0$ может иметь другие толкования, см. далее.

При условии $a_0 = 1$ раскрытие скобок и приведение подобных в (9.2) с последующим сопоставлением результата с (9.1) дает *теорему Виета*:

$$\begin{aligned} x_1 + \ldots + x_n &= -a_1, \\ x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n &= a_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1 \ldots x_n &= (-1)^n a_n. \end{aligned} \tag{9.3}$$

• Деление многочлена «в столбик» приемлемо для компьютера в виде *схемы Горнера* на основе представления

$$f_n(c) = (\ldots((c + a_1)c + a_2)c + a_3)c + \ldots + a_{n-1})c + a_n,$$

которое приводит к возможности последовательного выполнения однотипных действий: $b_{k+1} = a_{k+1} + b_k c$ вплоть до

$$b_n = a_n + b_{n-1}c = f_n(c),$$

где b_n — остаток от деления $f_n(x)$ на $x - c$, а $b_1, \ldots, b_{n-1}$ — коэффициенты частного $h_{n-1}(x)$.

• Полином $x^m - 1$ делится на $x^n - 1$ лишь в том случае, когда m делится на n. Действительно, пусть $m = nk + p$, тогда

$$\frac{x^m - 1}{x^n - 1} = x^p \frac{(x^n)^k - 1}{x^n - 1} + \frac{x^p - 1}{x^n - 1}.$$

Далее надо учесть, что $y^k - 1$ всегда делится на $y - 1$,

$$\frac{y^k - 1}{y - 1} = 1 + y + \ldots + y^{k-1}.$$

9.2. Алгоритм Евклида и делимость

Если многочлены $f(x)$, $\varphi(x)$, $\psi(x)$ связаны соотношением

$$f(x) = \varphi(x)\psi(x),$$

то $\varphi(x)$ и $\psi(x)$ считаются *делителями* $f(x)$. *Наибольшим общим делителем* (НОД) многочленов $f(x)$ и $g(x)$ называется такой их общий делитель $d(x) = (f(x), g(x))$, который делится на все другие общие делители многочленов $f(x)$ и $g(x)$.

В обозначении многочленов зависимость от аргумента удобнее опускать. В этом случае, например, $d(x) = (f(x), g(x))$ приобретает вид $d = (f, g)$, что не так загромождает обзор.

При договоренности *о равенстве единице «старших» коэффициентов* рассматриваемых многочленов — НОД, с точностью до $\pm$, определяется однозначно. В случае $d = (f, g) = 1$ многочлены $f(x)$ и $g(x)$ называют *взаимно простыми*.

Если имеются разложения $f(x)$ и $g(x)$ вида (9.2), то (f, g) указывается элементарно, но для этого надо знать все корни многочленов f и g. Универсальный рецепт дает *алгоритм Евклида*, который заключается в следующем.

Сначала $f(x)$ делится на $g(x)$:

$$f = gq_1 + r_2,$$

— после чего $g(x)$ делится на $r_2(x)$:

$$g = r_2q_2 + r_3.$$

Далее остаток $r_2(x)$ делится на $r_3(x)$, — и так до остановки итерационного процесса, которая неизбежна, ибо степень остатка на каждом шаге строго уменьшается. В обозримом виде это можно записать так:

$$\begin{cases} f = gq_1 + r_2, \\ g = r_2q_2 + r_3, \\ r_2 = r_3q_3 + r_4, \\ \dots\dots\dots\dots\dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, \\ r_{n-1} = r_nq_n. \end{cases} \tag{9.4}$$

Последняя строчка означает $r_{n+1} = 0$. Просматривая теперь запись (9.4) сверху вниз, обнаруживаем: общие делители $f(x)$ и $g(x)$ совпадают с общими делителями $g(x)$ и $r_2(x)$, которые, в свою очередь, совпадают с общими делителями $r_2(x)$ и $r_3(x)$, и т. д. В итоге:

$$(f, g) = (g, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n,$$

т. е. r_n оказывается искомым НОД многочленов $f(x)$ и $g(x)$.

Держа описанную схему в поле зрения, легко понять, что

$$(fh, gh) = (f, g)h,$$

а также

$$\boxed{\left(\frac{f}{s}, \frac{g}{s}\right) = \frac{(f, g)}{s},}$$

где $s(x)$ — любой общий делитель $f(x)$ и $g(x)$. В частности,

$$\left(\frac{f}{(f, g)}, \frac{g}{(f, g)}\right) = 1.$$

9.2.1. Теорема. *Всегда можно указать такие многочлены* $u(x), v(x)$, *что* [2]

$$\boxed{f(x)u(x) + g(x)v(x) = d(x),} \tag{9.5}$$

где $d = (f, g)$.

◄ Обоснование легко извлекается из схемы (9.4), просматривая которую (снизу вверх), получаем следующее. Поскольку $r_n = d(x)$, то полагая $u_1(x) = 1$, $v_1(x) = -q_{n-1}(x)$, — из предпоследнего равенства (9.4) имеем

$$d = r_{n-2}u_1 + r_{n-1}v_1.$$

Полагая далее

$$u_2(x) = v_1(x), \quad v_2(x) = u_1(x) - v_1(x)q_{n-1}(x),$$

получаем

$$d = r_{n-3}u_2 + r_{n-2}v_2.$$

Продолжая подниматься вдоль (9.4), в итоге приходим к (9.5). ►

(!) *При этом можно считать, что степени многочленов* $u(x)$, $v(x)$ *строго меньше — соответственно — степеней* $g(x)$ *и* $f(x)$, *разумеется в предположении, что степени многочленов* $f(x)$ *и* $g(x)$ *ненулевые.*

Из теоремы 9.2.1, в частности, следует: *многочлены* $f(x)$ *и* $g(x)$ *взаимно просты в том случае, когда можно подобрать такие многочлены* $u(x)$ *и* $v(x)$, *что*

$$f(x)u(x) + g(x)v(x) = 1. \tag{9.6}$$

• Фактически указать полиномы $u(x)$ и $v(x)$, удовлетворяющие (9.6), можно с помощью метода неопределенных коэффициентов [3]. Если речь идет об указании $u(x)$ и $v(x)$, удовлетворяющих (9.5), то после деления $f(x)$ и $g(x)$ на НОД $d(x)$ (определяемый алгоритмом Евклида) задача сводится к ситуации (9.6).

• Свойство (9.6) довольно широко используется в различных теоретических и прикладных конструкциях. Вот, например, универсальный механизм *избавления от иррациональности в знаменателе* дроби $\dfrac{h(\alpha)}{g(\alpha)}$, где α — корень некоторого

[2] Обычная трактовка (9.5): НОД $d = (f, g)$ «линейно» выражается через полиномы $f(x)$ и $g(x)$.

[3] Коэффициенты $u(x)$, $v(x)$ полагаются неизвестными, после чего коэффициенты полинома $f(x)u(x) + g(x)v(x)$ приравниваются коэффициентам полинома 1.

многочлена $f(x)$, причем все многочлены $f(x)$, $h(x)$, $g(x)$ имеют рациональные коэффициенты, а $f(x)$ и $g(x)$ взаимно просты.

Используя (9.6), получаем

$$\frac{h(\alpha)}{g(\alpha)} = \frac{h(\alpha)v(\alpha)}{1 - f(\alpha)u(\alpha)} = h(\alpha)v(\alpha),$$

поскольку $f(\alpha) = 0$.

• Теорема 9.2.1 фактически сохраняется и для целых чисел. НОД двух целых чисел m и n, не равных одновременно нулю, всегда может быть записан в виде

$$\text{НОД}\,(m, n) = mu + nv, \quad u, v \in \mathbb{Z}.$$

В частности, m и n взаимно просты в томм случае, когда существуют такие числа $u, v \in \mathbb{Z}$, что

$$mu + nv = 1.$$

9.3. Приводимость многочленов

Полином $f_n(x)$ называется *приводимым* над полем K, если он раскладывается в произведение двух многочленов ненулевой степени.

• Многочлен $x^2 + 1$ приводим в (над) $\mathbb{C}$,

$$x^2 + 1 = (x - i)(x + i),$$

но неприводим в $\mathbb{R}$. А полином

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

приводим в $\mathbb{R}$, но неприводим в $\mathbb{Q}$.

• Неприводимы в $\mathbb{C}$ только многочлены первой степени. Любой многочлен степени $n > 2$ приводим в $\mathbb{R}$, поскольку в разложение (9.2) комплексные корни входят сопряженными парами[4], а $(x - \alpha)(x - \overline{\alpha})$ — есть квадратный многочлен с действительными коэффициентами. Роль «простых чисел» в $\mathbb{R}[x]$ играют, таким образом, многочлены первой и второй степени.

• Приводимость многочлена, вообще говоря, не связана с существованием корней. Многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим в поле рациональных чисел, но не имеет в $\mathbb{Q}$ ни одного корня.

Более удивителен пример

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2),$$

поскольку многочлен $x^4 + 4$ «выглядит» неприводимым.

---

[4] $f_n(\alpha) = 0 \Rightarrow f_n(\overline{\alpha}) = 0$.

Многочлен $f_n(x)$ с рациональными коэффициентами неприводим над $\mathbb{Q}$ в **томм** случае, когда над $\mathbb{Q}$ неприводим многочлен с целыми коэффициентами, полученный умножением $f_n(x)$ на НОК знаменателей всех его коэффициентов.

9.3.1. *Многочлен*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \tag{9.7}$$

*с целыми коэффициентами неприводим над $\mathbb{Q}$ в **томм** случае, когда он не раскладывается в произведение двух многочленов ненулевой степени с коэффициентами из $\mathbb{Z}$.* (*?*)

Утверждение 9.3.1 без особого труда доказывается, и в принципе — сводит решение вопроса о *приводимости/неприводимости* к целочисленному перебору. На практике широко используются различные достаточные условия неприводимости.

9.3.2. Критерий Эйзенштейна. *Многочлен* (9.7), *все коэффициенты которого — кроме a_0 — делятся на некоторое простое число p, но a_n не делится на p^2, — неприводим над полем рациональных чисел.*

Известно множество других признаков неприводимости, но критерий 9.3.2 наиболее популярен, и его обычно «хватает», ибо потребность, как правило, заключается в указании примера неприводимого многочлена.

- Критерию 9.3.2 удовлетворяет, например, многочлен

$$3x^5 + 8x^4 - 4x^2 + 6x - 2,$$

для которого подходит число $p = 2$.

- *Многочлен*

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

*где p — **простое число**, неприводим над $\mathbb{Q}$.*

◄ В предположении противного был бы приводи́м многочлен

$$f(x+1) = x^{p-1} + C_p^1x^{p-2} + C_p^2x^{p-3} + \ldots + p,$$

что невозможно по *критерию Эйзенштейна.* ►

Многочлен с целыми коэффициентами называют *примитивным*, если НОД его коэффициентов равен 1. Любой многочлен

с коэффициентами из $\mathbb{Q}$ можно рассматривать как примитивный, умноженный на числовую дробь. Для этого коэффициенты надо привести к общему знаменателю, последний вынести за скобки, а также вынести за скобки НОД числителей. Это позволяет о неприводимых многочленах над $\mathbb{Q}$ говорить как о *примитивных* (с точностью до умножения на рациональную константу), что удобно с точки зрения стандартизации.

Произведение примитивных многочленов дает примитивный многочлен (лемма Гаусса). (?) Доказательство совсем просто, но изначально результат выглядит неожиданным.

9.4. Существование корней

Проблема разрешимости уравнения $f_n(x) = 0$ обычно ассоциируется с *основной теоремой алгебры* о существовании корня у любого полинома $f_n(x)$ в комплексной плоскости $\mathbb{C}$. Однако интересно — и важно (!), если думать не только о синице в руках, — начать с общего результата сугубо алгебраического характера.

9.4.1. Теорема. *По любому многочлену $f(x)$ над P всегда можно указать расширение поля $P' \supset P$, в котором $f(x)$ имеет корень.*

◀ Достаточно рассмотреть неприводимый многочлен $f(x)$ некоторой степени $n > 1$. В качестве P' возьмем фактор-кольцо $P[x]/I$, где $P[x]$ кольцо полиномов над P, а идеал $I = f(x)P[x]$ состоит из полиномов, делящихся на $f(x)$.

Таким образом, элементами P' являются *классы вычетов по модулю идеала*[5]. Сумма и произведение в P' определяются как остатки от деления на $f(x)$ обычной суммы и обычного произведения полиномов[6]. Необходимые свойства операций (ассоциативность, дистрибутивность) легко проверяются. Не совсем тривиально лишь существование в P' обратного элемента по умножению. Поскольку теорема 8.3 была оставлена без доказательства, остановимся на соответствующем обосновании более подробно.

Пусть степень $g(x)$ меньше степени $f(x)$. Поскольку полином $f(x)$ неразложи́м, то НОД f и g равен единице. Но тогда по теореме 9.2.1 существуют такие полиномы u и v, что

$$u(x)g(x) + v(x)f(x) = 1,$$

[5] Принадлежность $g(x)$, $h(x)$ одному и тому же классу $r(x)+I$ записывается как $g(x) = h(x) \pmod I$, что равносильно $g(x) - h(x) = I$, т. е. разность эквивалентных полиномов делится на $f(x)$.

[6] Представителей классов вычетов.

откуда $u(x)g(x) - 1$ делится на $f(x)$, — поэтому $u(x) * g(x) = 1'$, где звездочка означает умножение в P', следовательно $u(x) = g^{-1}(x)$.

Таким образом, фактор-кольцо $P[x]/I$ — есть поле, нулем которого служит сам идеал I, являющийся корнем полинома f (поскольку f делится сам на себя без остатка)[7]. ►

9.4.2. Следствие. *Для любого многочлена $f(x) \in P[x]$ существует расширение $P' \supset P$, над которым $f(x)$ раскладывается на линейные множители вида* (9.2).

Уместно заметить, что для многочленов от нескольких переменных это не так. Существуют *абсолютно неприводимые многочлены* $f(x_1, \ldots, x_n)$, неприводимые при любом расширении поля [15].

Поначалу теорема 9.4.1 и ее доказательство выглядят бесполезным фокусом. Возникает впечатление, что корнем объявлено нечто взятое с потолка. Но это не так. Построено вполне определенное расширение $P' \supset P$ исходного поля P, и в этом расширении указан корень полинома. Другое дело, если имеется желание «пощупать» P', но это уже вопрос изоморфизма полей с ориентацией на выбор удобных интерпретаций.

Рассмотрим, для примера, расширение поля действительных чисел $\mathbb{R}$ присоединением к $\mathbb{R}$ корня уравнения

$$x^2 + 1 = 0.$$

Начинать в самом деле можно «с потолка», объявив корнем некое i, — благо обозначение в нашей власти. Но далее мы оказываемся связанными «правилами игры». Расширение $\mathbb{R}' \supset \mathbb{R}$ обязано быть полем, включая в себя элементы

$$z = a + bi, \quad a, b \in \mathbb{R}. \tag{9.8}$$

Запись (9.8) однозначна, иначе из

$$z = a + bi = c + di, \quad b \neq d,$$

следовало бы $i = \dfrac{c-a}{d-b} \in \mathbb{R}$. Требования из определения поля приводят затем к свойствам, которые принято характеризовать как

[7] В [15] доказательство расписано подробнее (на 5 страницах).

правила обращения с комплексными числами. Следующий результат в данном контексте вполне очевиден.

9.4.3. Теорема. *Все расширения поля действительных чисел* $\mathbb{R}$, *полученные присоединением к* $\mathbb{R}$ *корня уравнения*

$$x^2 + 1 = 0,$$

изоморфны между собой.

Матрицы вида $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ образуют поле, изоморфное полю комплексных чисел $a + bi$. Сохранение операций и соответствия

$$1 \leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i \leftrightarrow \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

легко проверяются.

Реконструируя историю, можно представить, что вместо i была бы введена матрица $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ в качестве решения уравнения $x^2 + 1 = 0$, и стали бы рассматривать «числа» $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Возможно, для «аборигенов Сахалина» это было бы чересчур, но в целом — результат был бы иной. Мистических охов поубавилось бы. Дело в том, что использование матриц вместо чисел, как ни странно выглядит, имеет «материальную природу». Механизм оголен, все на виду, почвы для фантазии не остается. Когда же речь заходит о мнимой единице, появляется возможность домысливать, что уводит в потусторонних направлениях.

9.5. Производная многочлена

Производной многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

называется многочлен

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + a_{n-1}. \qquad (9.9)$$

Если $f(x)$ — многочлен над $\mathbb{R}$ или $\mathbb{C}$ и переменная x принимает значения в том же поле, то (9.9) — есть не что иное как обычная производная функции $f(x)$. Но определение (9.9) успешно работает и в общем случае многочлена над произвольным полем.

При этом сохраняются обычные свойства дифференцирования:

$$(\lambda f + \mu g)' = \lambda f' + \mu g',$$
$$(fg)' = f'g + fg'.$$

Вплоть до разложения в *ряд Тэйлора*:

$$f(x) = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n. \qquad (9.10)$$

Из (9.10) сразу следует

9.5.1. Теорема. *Многочлен $f \in P[x]$ над произвольным полем P имеет кратный корень $x = c$ в томм случае, когда*

$$f(c) = f'(c) = 0.$$

Более точная и полезная формулировка такова: *многочлен $f \in P[x]$ над P имеет кратный корень $x = c \in S$, где $S \supset P$ — произвольное расширение поля P, в томм случае, когда $f(c) = f'(c) = 0$.*

9.6. Дробно-рациональные функции

Дробно-рациональной функцией называется выражение вида $\dfrac{f(x)}{g(x)}$, где $f(x)$ и $g(x) \neq 0$ — многочлены над некоторым полем. Совокупность дробно-рациональных функций над любым полем — является полем. Отношение $\dfrac{f(x)}{g(x)}$ называют также просто *рациональной дробью*. Дробь $\dfrac{f(x)}{g(x)}$ считается *несократимой*, если многочлены $f(x)$ и $g(x)$ взаимно просты; и — *правильной*, если степень числителя меньше степени знаменателя. Всякая рациональная дробь единственным образом представляется в виде суммы многочлена и правильной дроби.

Правильная дробь $\dfrac{f(x)}{g(x)}$ называется *простейшей*, если $g(x)$ является степенью неприводимого многочлена $p(x)$, а степень $f(x)$ меньше степени $p(x)$.

9.6.1. Теорема. *Всякая правильная дробь единственным образом разлагается в сумму простейших.*

Рецепт соответствующего разложения состоит в следующем. Знаменатель $g(x)$ разлагается в произведение неприводимых многочленов,

$$g(x) = p_1^{s_1}(x) \dots p_m^{s_m}(x),$$

после чего дробь $\dfrac{f(x)}{g(x)}$ представляется в виде суммы дробей

$$\frac{q_j^k(x)}{p_k^{s_k-j+1}(x)}, \quad k = 1, \dots, m, \quad j = 1, \dots, s_k,$$

где $q_j^k(x)$ — многочлен степени, меньшей степени многочлена $p_j(x)$, взятый с неопределенными коэффициентами. Затем все дроби соответствующей суммы приводятся к общему знаменателю $g(x)$, складываются, и получаемый в числителе многочлен приравнивается $f(x)$, что дает необходимые уравнения для определения неизвестных коэффициентов.

Пример

В случае $\dfrac{f(x)}{g(x)} = \dfrac{x^2+2}{(x-1)^3}$ полагаем

$$\frac{f(x)}{g(x)} = \frac{a}{(x-1)^3} + \frac{b}{(x-1)^2} + \frac{c}{x-1}.$$

Действуя по указанному рецепту, получаем

$$x^2 + 2 = a + b(x-1) + c(x-1)^2,$$

что приводит к

$$\frac{x^2+2}{(x-1)^3} = \frac{3}{(x-1)^3} + \frac{2}{(x-1)^2} + \frac{1}{x-1}.$$

9.7. Симметрические многочлены

Многочленом $f(x_1, \dots, x_n)$ *от* n *неизвестных* $x_1, \dots, x_n$ *над полем* P называется сумма конечного числа произведений вида

$$x_1^{k_1} \dots x_n^{k_n}, \quad \text{где все} \quad k_j \geqslant 0,$$

с коэффициентами из P. При обычном определении суммы и произведения многочленов — их совокупность превращается в *коммутативное кольцо* $P[x_1, \ldots, x_n]$.

Рациональные дроби

$$\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)}, \quad p, q \in \mathbb{Q}[x_1, \ldots, x_n],$$

называют также *рациональными функциями.*

Функция $\varphi(x_1, \ldots, x_n)$ — в частности многочлен — называется *симметрической*, если она не меняется при любой перестановке $\sigma \in \mathbf{S_n}$ неизвестных,

$$\varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varphi(x_1, \ldots, x_n). \tag{9.11}$$

Эталонную роль играют *элементарные симметрические многочлены*:

$$\begin{aligned} s_1 &= x_1 + \ldots + x_n, \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_n &= x_1 \ldots x_n. \end{aligned}$$

9.7.1. Теорема[8]. *Всякий симметрический многочлен* $f(x_1, \ldots, x_n)$ *над полем* P *является многочленом над* P *от элементарных симметрических многочленов,*

$$f(x_1, \ldots, x_n) = \varphi(s_1, \ldots, s_n).$$

9.7.2. Следствие. *Всякий симметрический многочлен от корней уравнения*

$$x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \tag{9.12}$$

есть многочлен от коэффициентов $a_1, \ldots, a_n$.

[8] Это так называемая *основная теорема о симметрических многочленах*. Несложное доказательство имеет рутинный характер и может быть найдено практически в любом курсе общей алгебры.

Симметрия многочлена может быть «частичной». Например, несимметрический многочлен

$$x_1^5x_2x_3x_4 + x_1x_2x_3^5x_4 - x_1 - x_3 + 2$$

под действием подстановок

$$(x_1, x_3) \to (x_3, x_1), \quad (x_2, x_4) \to (x_4, x_2)$$

не меняется. А полином

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

не меняется под действием любой четной подстановки.

Многочлен

$$(x_1 + x_2)^2 + (x_3 + x_4)^2$$

инвариантен к заменам индексов $1 \leftrightarrow 2$, $3 \leftrightarrow 4$, а также к замене пар $(1, 2) \leftrightarrow (3, 4)$. Но для рациональной функции

$$\frac{(x_1 + x_2)^2}{(x_3 + x_4)^2}$$

замена пар $(1, 2) \leftrightarrow (3, 4)$ уже не годится.

9.8. Групповая инвариантность

Если рациональная функция $\varphi(x_1, \ldots, x_n)$ не меняется под действием перестановок индексов (переменных), то она не меняется и под действием композиции этих перестановок[9]. Поэтому совокупность всех подстановок $\sigma \in \mathbf{S_n}$, оставляющих функцию $\varphi(x_1, \ldots, x_n)$ инвариантной, всегда составляет группу, которую будем называть *группой инерции функции* φ и обозначать G_φ.

9.8.1. Теорема. *Пусть* $G_\varphi \subset G_\psi$. *Тогда*

$$\psi(x_1, \ldots, x_n) = \frac{f[\varphi(x_1, \ldots, x_n)]}{g[\varphi(x_1, \ldots, x_n)]}, \tag{9.13}$$

[9] Потому что в данном случае при перестановках существенна не нумерация самих переменных, а нумерация мест, на которых они стоят.

где коэффициенты полиномов f, g являются симметрическими функциями от $x_1, \ldots, x_n$.

◄ Разобьем группу G_ψ на смежные классы по подгруппе G_φ:

$$g_1 G_\varphi,\ g_2 G_\varphi,\ \ldots,\ g_p G_\varphi,$$

где для единообразия положено $g_1 = 1$.

Под действием любой подстановки $\sigma \in G_\varphi$ функция $\varphi = \varphi_1$ не меняется. Под действием любой подстановки $\sigma \in g_j G_\varphi$ функция φ преобразуется в φ_j, причем все $\varphi_1, \ldots, \varphi_p$ различны. Аналогично, подстановки $\sigma \in g_j G_\varphi$ преобразуют ψ в ψ_j, но некоторые из $\psi_1, \ldots, \psi_p$ могут совпадать.

Рассматривая равенства

$$\sum_j \varphi_j^k \psi_j = \omega_k, \quad k = 0, \ldots, p-1,$$

как систему уравнений относительно $\psi_1, \ldots, \psi_p$, имеем

$$\psi = \psi_1 = \begin{vmatrix} 1 & \ldots & 1 \\ \varphi_1 & \ldots & \varphi_p \\ \vdots & \ddots & \vdots \\ \varphi_1^{p-1} & \ldots & \varphi_p^{p-1} \end{vmatrix} : \begin{vmatrix} \omega_0 & 1 & \ldots & 1 \\ \omega_1 & \varphi_2 & \ldots & \varphi_p \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{p-1} & \varphi_2^{p-1} & \ldots & \varphi_p^{p-1} \end{vmatrix}. \tag{9.14}$$

Несложный анализ [10] показывает, что (9.14) дает необходимое (9.13). ►

Теорема 9.8.1 фактически принадлежит *Лагранжу*, который в знаменитом мемуаре «Рассуждения об алгебраическом решении уравнений» (1771) пришел к следующему выводу. Решение в радикалах удается получить в тех случаях, когда существуют некоторые функции $\varphi(x_1, \ldots, x_n)$ от корней $x_1, \ldots, x_n$, которые удовлетворяют уравнениям более низкой степени, решаемым в радикалах. В свою очередь, подобное свойство $\varphi(x_1, \ldots, x_n)$ оказывается связанным с инвариантностью функций φ к некоторым перестановкам корней. Тем самым *Лагранж* подошел к месту, где «горячо». Неразрешимость в радикалах уравнений 5-й степени была установлена *Руффини* (1799) и окончательно (аккуратно) *Абелем* (1826). Глубинный механизм был вскрыт *Галуа* (1811–1832).

Вернемся, однако, к теореме 9.8.1, которая лежит не так уж глубоко, но в теоретико-групповой идеологии играет важную роль. Вот ее принципиальные следствия:

[10] См., например, [24].

- *В случае $G_\varphi = G_\psi$ функции φ и ψ рационально выражаются друг через друга* [11].
- *Если многочлен $f(x_1, \ldots, x_n)$ при всевозможных подстановках переменных принимает два возможных значения, то*

$$f = \theta_1 + \theta_2 \prod_{i<j} (x_i - x_j),$$

где θ_1 и θ_2 — симметрические функции.

9.9. Как реагировать на ассоциации

Помещение разнородных объектов под одну крышу будит ассоциации и порождает иллюзии. Принадлежность, скажем, кольцевой структуре не гарантирует алгебраической идентичности, но соблазн переноса свойств — возникает. Рассмотрим, для примера, следующий простой, но весьма продуктивный результат [12].

9.9.1. Теорема Мэйсона—Стотерса. *Пусть многочлены $f(x)$, $g(x)$, $h(x)$ ненулевой степени взаимно просты и $f + g = h$. Тогда степень любого из этих полиномов не превосходит $n_0(fgh) - 1$, где $n_0(p)$ обозначает количество различных корней полинома p.*

О силе теоремы 9.9.1 говорит, например, элементарное следствие (*теорема Ферма для многочленов*):

9.9.2. *Для взаимно простых многочленов $x_1(t)$, $x_2(t)$, $x_3(t)$ ненулевой степени равенство*

$$x_1^n(t) + x_2^n(t) = x_3^n(t)$$

при $n > 2$ — невозможно.

Доказательство получается «в две строчки».

---

[11] Под рациональной выразимостью подразумевается связь вида (9.13), где коэффициенты полиномов f, g над полем нулевой характеристики являются симметрическими функциями от $x_1, \ldots, x_n$.

[12] *Mason R. C.* Diophantine Equations over Function Fields. Cambridge University Press, 1984 (London Math. Soc. Lecture Note Series. **96**); *Stothers W.* // Quart. Math. Oxford. 1981. **32** (2). P. 349–370.

◄ Согласно теореме 9.9.1, с учетом $n_0(p^n) = n_0(p)$,

$$\deg x_i^n = n \deg x_i \leqslant \deg x_1 + \deg x_2 + \deg x_3 - 1.$$

Суммируя по i, получаем

$$n(\deg x_1 + \deg x_2 + \deg x_3) \leqslant 3(\deg x_1 + \deg x_2 + \deg x_3 - 1),$$

откуда $n < 3$. ►

Хотя *теорема Ферма* для целых чисел уже доказана, простота, с которой устанавливается ее аналог 9.9.2, действует интригующе и побуждает задуматься о поиске новых инструментов в $\mathbb{Z}$. Однако прямолинейные попытки ничего не дают, потому что доказательство стержневого результата 9.9.1 опирается на дифференцирование полиномов [13], т. е. на использование специфики за пределами кольцевой аксиоматики. Не говоря о том, что даже формулировка аналога теоремы 9.9.1 в $\mathbb{Z}$ вызывает затруднения.

Тем не менее весьма отдаленные параллели иногда подсказывают удачные повороты теории [14]. В данном случае имеется гипотеза, которая в некотором роде может служить аналогом теоремы *Мэйсона—Стотерса* в $\mathbb{Z}$.

9.9.3. Гипотеза abc (Masser, Oesterle) [15]. *По любому $\varepsilon > 0$ можно указать такую константу $K(\varepsilon)$, что для всех взаимно простых целых чисел $a, b, c > 0$, таких что $a + b = c$, верно неравенство*

$$\max\{a, b, c\} \leqslant K(\varepsilon)[N_0(abc)]^{1+\varepsilon},$$

где

$$N_0(m) = p_1 \dots p_r,$$

если разложением целого m на простые множители является

$$m = p_1^{\nu_1} \dots p_r^{\nu_r}.$$

Из 9.9 теорема Ферма в $\mathbb{Z}$ следует так же легко как 9.9.2 из 9.9.1. Точнее говоря, справедливость 9.9 влечет за собой невозможность

[13] См. *Lang S.* // Bull. AMS. 1990. **23**. P. 37–75; или [24].

[14] Например, *производная многочлена* (9.9) — успешно работает в общем случае многочлена над произвольным полем, где обычное понятие производной не имеет смысла.

[15] *Stewart C. L., Tijdeman R.* On the Oesterle—Masser conjecture // Monatshefte Math. 1986. **102**. P. 251–257.

$x^n + y^n = z^n$ при достаточно больших n. И если гипотеза окажется верной, идея наличия глубинных связей между объектами разной природы получит еще одно подтверждение [16)].

Так или иначе, разговор к тому, что самые нелепые на первый взгляд предположения, вытекающие из кажущегося родства явлений, приносят иногда плоды. Нередко — тем фундаментальнее, чем смехотворнее догадка.

[16)] Конечно, скрытые механизмы со временем обнажаются, и удивительное становится банальным.

Глава 10

Алгебраические числа

Теория алгебраических чисел с различной степенью полноты излагается во многих источниках — см., например, [2, 5, 17, 22], — и в данном случае оказывается в поле зрения той частью, которая соприкасается с *теорией Галуа*. Стержневые результаты сопровождаются доказательствами, сопутствующие — упоминаются вскользь.

10.1. Расширения полей

Поле F по отношению к любому своему подполю P называется ***расширением*** P. Как правило, далее речь идет о ситуациях $F \subset \mathbb{R}$ либо $F \subset \mathbb{C}$. По крайней мере, подразумевается, если не оговорено противное, что P имеет *нулевую характеристику*.

Наименьшее по включению поле

$$F = P(S),$$

содержащее подполе P и множество S, — называется *расширением поля* P на S. В случае, когда S состоит из одного элемента θ, о $P(\theta)$ говорят как о ***простом расширении***[1] поля P.

10.1.1. *Корни ненулевых многочленов*

$$f(x) \in P[x]$$

называются ***алгебраическими числами*** (*элементами*) ***над полем*** P.

Любое число, алгебраическое над полем P, алгебраично и над любым расширением $F \supset P$ (но не наоборот).

10.1.2. ***Минимальным многочленом числа*** α ***над*** P *называют тот из ненулевых многочленов* $f(x) \in P[x]$, $f(\alpha) = 0$, — *который имеет наименьшую степень* (***степень*** α ***над*** P) *и старший коэффициент* 1.

[1] Понятно, что $P(\theta)$ — поле отношений кольца многочленов $P[\theta]$.

Корни минимального[2)] многочлена α над P называют числами, ***сопряженными*** с α. Частным случаем этого определения является обычное понятие *комплексно сопряженного числа.*

10.1.3. *Минимальный (неприводимый) многочлен не может иметь кратных корней.*

◄ Иначе вместе с $f(\alpha)=0$ было бы необходимо $f'(\alpha)=0$ (теорема 9.5.1), что противоречило бы минимальности f. ►

• Минимальные многочлены чисел -3, $\sqrt[n]{2}$, i равны:

$$x+3, \quad x^n-2, \quad x^2+1.$$

• В главе 8 (по сути), что простое расширение $\mathbb{Q}(\sqrt{2})$ *кольца* $\mathbb{Q}$, полученного присоединением числа $\sqrt{2}$, состоит из чисел вида $a+b\sqrt{2}$; а в случае присоединения $\sqrt[3]{2}$ — простым расширением $\mathbb{Q}$ оказывается кольцо чисел $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где $a,b,c\in\mathbb{Q}$.

Если говорить о расширениях кольца $\mathbb{Q}$, рассматриваемого как *поле*, то $\mathbb{Q}(\sqrt{2})$ состоит из элементов

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}, \quad a,b,c,d\in\mathbb{Q},$$

а $\mathbb{Q}(\sqrt[3]{2})$ — из элементов

$$\frac{a+b\sqrt[3]{2}+c\sqrt[3]{4}}{a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4}}, \quad a,b,c,a_1,b_1,c_1\in\mathbb{Q},$$

однако в том и другом случае избавление от иррациональности в знаменателе позволяет считать, что расширения $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt[3]{2})$ *поля* $\mathbb{Q}$ состоят, как и прежде, из элементов $a+b\sqrt{2}$ и $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, соответственно.

Аналогичная ситуация имеет место и в общем случае, что фиксируется следующей — до некоторой степени «неожиданной» — теоремой.

10.1.4. Теорема. *Пусть алгебраический элемент α над P имеет степень n. Тогда расширение $P(\alpha)$ является n-мерным линейным пространством с базисом $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$, т. е. любой элемент $\beta\in P(\alpha)$ единственным образом представим в виде*

$$\beta=p_0+p_1\alpha+\ldots+p_{n-1}\alpha^{n-1}, \quad \textit{все} \quad p_j\in P. \tag{10.1}$$

[2)] А значит, и неприводимого.

◄ Каждый элемент $\beta \in P(\alpha)$ представим в виде $\beta = \dfrac{g(\alpha)}{h(\alpha)}$, где полиномы $g(x), h(x)$ из кольца $P[x]$. Минимальный многочлен $f(x)$ числа α над P — взаимно прост с $h(x)$ (иначе $h(\alpha) = 0$). Поэтому (теорема 9.2.1) существуют такие многочлены $u(x), v(x) \in P[x]$, что $u(x)f(x) + v(x)h(x) = 1$, а поскольку $f(\alpha) = 0$, то

$$v(\alpha)h(\alpha) = 1 \quad \Rightarrow \quad \beta = g(\alpha)v(\alpha). \tag{10.2}$$

Подставляя теперь $x = \alpha$ в разложение

$$g(x)v(x) = q(x)f(x) + r(x),$$

где $r(x)$ обозначает остаток

$$r(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1},$$

и учитывая (10.2), получаем (10.1)[3].

Линейная независимость элементов $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ вытекает из определения минимального многочлена $f(x)$. ►

В случае произвольного расширения $F \supset P$ поле F также рассматривается как векторное пространство над P. Его размерность, обозначаемая $[F : P]$, называется ***степенью расширения*** F над P. В случае трансцендентного элемента $\theta \in F$ степень расширения $[P(\theta) : P] = \infty$.

В цепочке расширений[4] $R \supset Q \supset P$ *степень* $[R : P]$ *конечна в томм случае, когда конечны степени* $[R : Q]$ *и* $[Q : P]$, *— при этом*

$$[R : P] = [R : Q] \cdot [Q : P].$$

• Поле комплексных чисел $\mathbb{C}$ является простым расширением поля $\mathbb{R}$, полученного присоединением к $\mathbb{R}$ мнимой единицы, $\mathbb{C} = \mathbb{R}(i)$.

10.2. Алгебраические расширения

О расширении $P(\alpha_1, \ldots, \alpha_m)$ с алгебраическими над P элементами α_j — обычно говорят как о ***конечном расширении*** поля P. Точнее, *расширение* $F \supset P$ *конечно*, если F — конечномерное линейное пространство над P.

---

[3] Проведенная манипуляция есть не что иное как рецепт избавления от иррациональности в знаменателе, который упоминался в разделе 9.2.

[4] Такие цепочки принято называть ***башнями расширений***.

Люфт определения непринципиален, поскольку: *расширение $F \supset P$ конечно в том случае, когда существуют алгебраические над P элементы $\alpha_1, \ldots, \alpha_m$, такие что $F = P(\alpha_1, \ldots, \alpha_m)$.*

Любое конечное расширение $F \supset P$ *алгебраично*[5]. *Последовательность алгебраических расширений является алгебраическим расширением.* Поле P считается *алгебраически замкнутым*, если все корни любого полинома $f(x) \in P[x]$ лежат в P, т. е. всякое алгебраическое расширение P совпадает с P.

Каждое из следующих условий равносильно алгебраической замкнутости поля P:

- *неприводимыми над P являются только линейные многочлены;*
- *любой полином из $P[x]$ имеет корень в P.*

Для любого многочлена $f(x) \in P[x]$ существует (см. теорему 9.4.1 *и следствие* 9.4.2*) расширение $F \supset P$, над которым $f(x)$ раскладывается в произведение линейных множителей*

$$f(x) = a_0(x - x_1)(x - x_2)\ldots(x - x_n).$$

Полем разложения неприводимого многочлена $f(x)$ считается наименьшее расширение поля P, содержащее **все** корни $f(x)$.

Например, $\mathbb{Q}(\sqrt[3]{2}, e^{(2\pi/3)i})$ — поле разложения многочлена $f(x) = x^3 - 2$.

Остановимся, наконец, на *алгебраичности алгебраических расширений*, что само по себе не вполне очевидно.

Пусть α и β — корни неприводимых многочленов, соответственно, f и g, причем $a_1 = \alpha, \ldots, \alpha_n$ — корни f; $b_1 = \beta, \ldots, \beta_m$ — корни g. Многочлен

$$h(x) = \prod_{i,j}[x - \alpha_i - \beta_j]$$

симметричен по $a_1, \ldots, \alpha_n$ и по $b_1, \ldots, \beta_m$. Поэтому его коэффициенты будут многочленами от коэффициентов[6] $f(x)$ и $g(x)$. При этом $h(\alpha + \beta) = 0$. Следовательно, сумма алгебраических чисел α и β — алгебраическое число. Аналогично

[5] Расширение $F \supset P$ считается алгебраичным, если любой элемент из F алгебраичен над P. Обоснование см. далее.

[6] См. например [15], где речь идет о многочленах, симметрических по двум системам переменных.

устанавливается алгебраичность чисел $\alpha - \beta$ и $\alpha\beta$. Далее, если α — корень многочлена

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

то α^{-1} — корень многочлена

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,$$

что позволяет утверждать алгебраичность отношения β/α.

10.3. Нормальные расширения

Расширение F поля P называется ***нормальным***[7], если всякий неприводимый над P многочлен, имеющий корень в F, разлагается над F на линейные множители. Можно сказать иначе.

*Расширение $F \supset P$ **нормально**, если любое α входит в F со своими сопряженными числами.*

Расширение $\mathbb{Q}(\sqrt[3]{2})$ *не нормально*, поскольку не содержит комплексных корней минимального многочлена $x^3 - 2$. Нормальным расширением будет $\mathbb{Q}(\sqrt[3]{2}, e^{(2\pi/3)i})$.

10.3.1. Теорема. *Расширение F поля P нормально в томм случае, когда*

$$F = P(\alpha_1, \ldots, \alpha_n),$$

*где $\alpha_1, \ldots, \alpha_n$ — **все** корни некоторого многочлена f над P.*

◀ Любой элемент $\omega \in F$ представим в виде

$$\omega = \varphi(\alpha_1, \ldots, \alpha_n), \quad \varphi \in P[x_1, \ldots, x_n].$$

Многочлен

$$g(x) = \prod_{\sigma \in S_n} \left(x - \varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)})\right)$$

симметричен по $x_1, \ldots, x_n$, — поэтому его коэффициенты выражаются через коэффициенты $f(x)$. Следовательно, $g(x)$ — многочлен над P, и ω — его корень. Таким образом, минимальный многочлен $h(x)$ числа ω имеет с $g(x)$ общий корень ω и потому делит $g(x)$, а значит, все корни $h(x)$ лежат в F.

В обратную сторону теорема очевидна. ▶

[7] Нормальные расширения $F \supset P$ называют также ***нормальными полями***.

Теорема 10.3.1 утверждает по сути, что нормальные расширения $F \supset P$ совпадают с полями разложения многочленов над P. Здесь, правда, остается некоторый зазор для уточнений. Во-первых, необходимо напомнить, что речь идет о полях P нулевой характеристики[8]. Во-вторых, мы оставляем за кадром оговорки типа «с точностью до изоморфизма», каковые в принципе важны, но сильно утяжеляют изложение скучными рассуждениями.

• Если F — нормальное расширение поля P, а L — промежуточное поле, $F \supset L \supset P$, то F — нормальное расширение поля L. (?)

• *Композитом полей* P_1 и P_2 называется минимальное (по включению) поле $P = P_1 \cdot P_2$, содержащее оба поля P_1 и P_2. *Расширение* $P(\alpha_1, \alpha_2)$ — *есть композит расширений* $P(\alpha_1)$ *и* $P(\alpha_2)$. (?)

• Если K и L — расширения поля P, причем $K = P(\alpha_1, \ldots, \alpha_m)$, то *композит*

$$K \cdot L = L(\alpha_1, \ldots, \alpha_m). \quad (?)$$

• Композит и пересечение нормальных расширений — нормальны. (?)

10.4. Теорема о примитивном элементе

Поле $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ образуют числа вида

$$\xi = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q},$$

каковые в то же время исчерпываются линейными комбинациями

$$\xi = \alpha + \beta\theta + \gamma\theta^2 + \delta\theta^3, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Q}, \quad \theta = \sqrt{2} + \sqrt{3},$$

поскольку

$$\sqrt{2} = \frac{1}{2}(\theta^3 - 9 \cdot \theta), \quad \sqrt{3} = \frac{1}{2}(11 \cdot \theta - \theta^3), \quad \sqrt{6} = \frac{1}{2}(\theta^2 - 5 \cdot \theta).$$

Таким образом, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, т. е. расширение $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ равносильно простому расширению $\mathbb{Q}$ с помощью одного элемента $\theta = \sqrt{2} + \sqrt{3}$, — что может показаться исключением, но это общее правило.

10.4.1. Теорема о примитивном элементе. *Любое алгебраическое расширение F поля P нулевой характеристики может быть порож-*

[8] Иначе приходится еще говорить о *сепарабельных* расширениях [5, 14].

дено одним ***примитивным элементом*** θ, *т. е.*[9]

$$\boxed{F = P(\alpha_1, \ldots, \alpha_m) = P(\theta).}$$

◀ Расширение $F = P(\alpha_1, \ldots, \alpha_m)$ можно представить как последовательность простых расширений

$$P \subset P(\alpha_1) \subset P(\alpha_1)(\alpha_2) \subset \ldots P(\alpha_1, \ldots, \alpha_{m-1})(\alpha_m) = F.$$

Поэтому достаточно ограничиться случаем двух элементов $F = P(\alpha, \beta)$.

Поскольку расширение алгебраично, — существуют неприводимые над P многочлены $f(x)$ и $g(x)$, имеющие, соответственно, корни

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r \quad \text{и} \quad \beta = \beta_1, \beta_2, \ldots, \beta_s.$$

Выберем далее $\zeta \in P$ так, чтобы[10] $\alpha_i + \zeta\beta_j \neq \alpha + \zeta\beta$ для всех пар $(i, j) \neq (1, 1)$, и положим $\theta = \alpha + \zeta\beta$.

В силу

$$f(\theta - \zeta\beta) = f(\alpha) = 0,$$

β является общим корнем многочленов $h(x) = f(\theta - \zeta x)$ и $g(x)$, причем единственным[11]. Поэтому НОД $h(x)$ и $g(x)$ равен[12] $x - \beta$, — откуда $\beta \in P(\theta)$. Но тогда и $\alpha = \theta - \zeta\beta \in P(\theta)$. Следовательно, $P(\alpha, \beta) \subset P(\theta)$, а поскольку обратное включение $P(\theta) \subset P(\alpha, \beta)$ очевидно, то $P(\theta) = P(\alpha, \beta)$. ▶

Из теоремы 10.4.1 и ее доказательства легко усматриваются следующие утверждения.

10.4.2. *Примитивный элемент поля* $P(\alpha_1, \ldots, \alpha_m)$ *может быть выбран в виде линейной комбинации*

$$\theta = s_1\alpha_1 + \ldots + s_m\alpha_m, \quad \textit{все} \quad s_j \in P.$$

10.4.3. *Все корни* $x_1, \ldots, x_n$ *любого многочлена* $f(x)$ *с коэффициентами из* P *рационально выражаются через «одну иррациональность»* θ,

$$x_j = s_{0j} + s_{1j} \cdot \theta + \ldots + s_{(n-1)j} \cdot \theta^{n-1}, \quad \textit{все} \quad s_{kj} \in P.$$

---

[9] Можно было бы сказать, что $P(\theta)$ есть *фактор-кольцо* $P[x]/g(x)$, где $g(x)$ — минимальный многочлен элемента θ.

[10] В случае конечного поля P ненулевой характеристики обеспечить условие $\alpha_i + \zeta\beta_j \neq \alpha + \zeta\beta$ не всегда удается. Но теорема остается верной, доказательство проводится другим способом.

[11] Если допустить $h(\beta_j) = 0$ $(j \neq 1)$, то $\theta - \zeta\beta_j = \alpha_i$ при некотором i, что противоречит выбору θ.

[12] Неприводимые многочлены над полем нулевой характеристики кратных корней не имеют.

При этом n равно размерности $P(\alpha_1, \ldots, \alpha_m)$, т. е. степени расширения [13] $[F : P]$.

10.5. Круговые поля

Корнями многочлена $x^n - 1$ в $\mathbb{C}$, как хорошо известно, служат

$$\sqrt[n]{1} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0, \ldots, n-1,$$

или по-другому:

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}, \quad \text{где} \quad \zeta = e^{i(2\pi/n)} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}. \qquad (10.3)$$

Легко видеть, что числа (10.3), делящие единичную окружность в $\mathbb{C}$ на n равных частей, являются *циклической группой* относительно умножения с образующей ζ.

Число ζ представляет собой один из *примитивных корней* $\varepsilon_1, \ldots, \varepsilon_r$, каковые определяются условиями

$$\boxed{\varepsilon_j^n = 1, \quad \text{но} \quad \varepsilon_j^k \neq 1 \quad \text{при} \quad k < n.}$$

При этом ряд $1, \varepsilon_j, \varepsilon_j^2, \ldots, \varepsilon_j^{n-1}$ (при любом j) исчерпывает все корни (10.3). Поэтому *циклическая группа всех корней порождается любым примитивным корнем ε_j*.

Разумеется, если n простое, все корни (10.3) примитивные. Но в случае составного n ситуация не такая уж простая. Даже вопрос подсчета числа примитивных корней требует определенных усилий — это число оказывается равным значению *функции Эйлера* [14] $\varphi(n)$.

При изучении расширений полей с ориентацией на проблему разрешимости уравнений в радикалах — важную роль играют ***круговые многочлены***

$$\Phi_n(x) = (x - \varepsilon_1) \ldots (x - \varepsilon_r), \quad r = \varphi(n),$$

[13] Речь идет о полях нулевой характеристики.

[14] Значение $\varphi(n)$ определяется равным количеству натуральных $k < n$, взаимно простых с n; $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$, $\varphi(5) = 4$.

корнями которых служат исключительно *примитивные корни* из единицы (при заданном n) [15].

В случае простого n

$$\Phi_n(x) = x^{n-1} + \ldots + x + 1.$$

В общем случае для вычисления $\Phi_n(x)$ приходится вникать в теоретико-числовую специфику [14, 24]. Начало ряда выглядит так:

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1,$$

$$\Phi_6(x) = x^2 - x + 1, \quad \Phi_8(x) = x^4 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Создается впечатление, что коэффициентами $\Phi_n(x)$ могут быть лишь ± 1. Такая закономерность прослеживается довольно далеко. Но, например, один из коэффициентов $\Phi_{210}(x)$ уже оказывается равным 2, а далее — *коэффициенты $\Phi_n(x)$ могут быть любыми целыми числами* [24]. Удивительной может показаться сама целочисленность коэффициентов $\Phi_n(x)$, но от удивления легко избавиться с помощью *леммы Гаусса* [16].

Некоторая «таинственность» вокруг многочленов $\Phi_n(x)$ ликвидируется легко обнаруживаемой формулой [17]

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{10.4}$$

дающей индуктивное правило вычисления круговых многочленов. Например, в силу (10.4)

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.$$

10.5.1. *Многочлены $\Phi_n(x)$ неприводимы над $\mathbb{Q}$.*

◄ Для малых n факт проверяется. Далее работает индукция. Однако скоро сказка сказывается. За техническими подробностями можно обратиться к одной из книг [5, 14, 24]. ►

---

[15] Уравнение $\Phi_n(x) = 0$ называется ***уравнением деления круга***, а поле корней (10.3) — ***круговым полем***.

[16] О примитивности произведения примитивных многочленов.

[17] Символ «$d|n$» означает «d делит n», т. е. d является делителем n. Произведение в (10.4), таким образом, идет по всем делителям d числа n.

Глава 11

Теория Галуа

Математика состоит из задач, иерархически объединяемых в схемы. «Хождение по этажам» иногда вдохновляет на преобразование действительности, что толкает, как думают одни, в пропасть, другие, — к спасению. Но так или иначе, сами задачи прямого влияния на реальность не оказывают. Влияние опосредованное. В чем-то аналогичное воздействию разрешимости уравнений в радикалах на судьбу Галактики.

11.1. Предварительные замечания

Как уже отмечалось, *Руффини* и *Абель* показали, что алгебраические уравнения 5-й степени и выше в радикалах, вообще говоря, не решаются. Закономерно встал вопрос об условиях, позволяющих отделить разрешимые ситуации от неразрешимых. Ответ был получен *Галуа* (1832) на основе идей, которые в головы современников никак не укладывались. Потенциал неприятия, конечно, постепенно ослаб, но теория Галуа до сих пор считается весьма нетривиальной и труднодоступной для понимания.

Самое удивительное при этом, что там нет каких-либо особо сложных доказательств. Точнее говоря, в рассуждениях нет технически сложных трюков, но используются идеологические конструкции, непривычные для подсознания и с трудом укладывающиеся в голове, — что в некотором роде характерно для теории групп вообще. В дополнение к главным «неприятностям» сценарий сопровождается массой второстепенных мелких понятий и терминов, в результате чего без освоения нового языка и новых категорий мышления браться за дело нелегко.

Но основная трудность все же — в скрытом характере изучаемых явлений. Пояснить это можно на постороннем примере векторного анализа, который большей частью изучает поверхностные явления, в достаточной мере наглядные для геометрической интуиции. Но есть следующий пласт, где фигурирует, скажем,

ковариантное и *контравариантное дифференцирование*, что уже не так хорошо укладывается в голове, — потому что голова задумывалась Создателем для других дел.

Кроме того, теория Галуа приводит в движение сразу несколько механизмов из разных областей, которыми необходимо владеть, чтобы следить за «взаимодействием», не отвлекаясь на изматывающее перелистывание книг в поисках нужных определений и фактов. Минимальные исходные требования заключаются в предварительном освоении элементов *теории групп* и *алгебраических чисел*, не говоря о мелочах типа многочленов и полей.

В связи с отмеченными обстоятельствами теория Галуа рассматривается далее в упрощенном варианте, основанном на рассмотрении числовых полей — имеющих *характеристику* 0 — и освобожденном от второстепенных деталей.

Одно из минимальных требований для дальнейшего чтения — прочное владение понятиями, связанными с расширениями полей (глава 10). Вот главные опорные точки. *Расширением* F поля P называется любое поле F, содержащее P в качестве подполя [1]. Всякое расширение можно рассматривать как *линейное пространство над* P, размерность которого называют *степенью расширения* и обозначают $[F : P]$. Элемент $\alpha \in F$ называют *алгебраическим над* P, если он является корнем некоторого полинома $f(x)$ с коэффициентами из P. Наименьшее расширение P, содержащее α, обозначают $\boxed{P(\alpha)}$. *Полем разложения* неприводимого многочлена $f(x)$ считается наименьшее расширение поля P, содержащее все корни $f(x)$.

11.2. Группа Галуа

Напомним: взаимнооднозначное отображение $\mathcal{A} : G \to G$ группы на себя, сохраняющее групповую операцию, называется *автоморфизмом*. *Группа автоморфизмов* обозначается $\mathrm{Aut}\, G$. ***Автоморфизмы полей*** $\mathcal{A} : P \to P$ определяются аналогично, с тем уточнением, что

[1] В качестве образца P можно иметь в виду поле рациональных чисел.

взаимнооднозначное отображение $\mathcal{A}$ поля на себя обязано сохранять обе операции,

$$\mathcal{A}(x+y)=\mathcal{A}(x)+\mathcal{A}(y), \quad \mathcal{A}(xy)=\mathcal{A}(x)\mathcal{A}(y),$$

что чаще записывают в виде

$$(x+y)^{\mathcal{A}}=x^{\mathcal{A}}+y^{\mathcal{A}}, \quad (xy)^{\mathcal{A}}=x^{\mathcal{A}}y^{\mathcal{A}},$$

пользуясь обозначением $\mathcal{A}(x)=x^{\mathcal{A}}$.

Пусть теперь $F \supset P$ — *нормальное расширение*[2] поля P. В группе автоморфизмов $\operatorname{Aut} F$ выделим подгруппу $\operatorname{Aut} F/P$ тех автоморфизмов $\mathcal{A}: F \to F$, которые поле P оставляют на месте, т. е. $\mathcal{A}(x)=x$, если $x \in P$.

11.2.1. *Группу* $\operatorname{Aut} F/P$ *называют* ***группой Галуа*** *нормального расширения* $F \supset P$ *и обозначают* $\mathrm{G}(F/P)$.

Наравне с $\mathrm{G}(F/P)$ используется также обозначение G_f, где f — многочлен, не имеющий кратных корней, полем разложения которого является расширение F. При этом говорят о *группе Галуа* как *многочлена*, так и соответствующего *расширения*.

С самого начала важно разобраться, что из себя представляет *группа Галуа*. Хотя исчерпать вопрос не так просто, кое-что лежит на поверхности.

Поскольку $F=P(\alpha_1,\ldots,\alpha_n)$, где $\alpha_1,\ldots,\alpha_n$ — корни полинома $f(x)$, то[3]

$$\boxed{\mathcal{A}f(\alpha_j)=f(\mathcal{A}(\alpha_j))=0,} \tag{11.1}$$

откуда следует, что $\mathcal{A}(\alpha_j)$ — также корень $f(x)$, т. е.

$$\mathcal{A}(\alpha_j)=\alpha_i.$$

---

[2] Нормальные расширения рассматриваемых здесь полей нулевой характеристики — совпадают с полями разложения (см. теорему 10.3.1) полиномов f, не имеющих кратных корней.

[3] $\mathcal{A}f(x)=f(\mathcal{A}(x))$ — потому что $\mathcal{A}$, по определению, не меняет коэффициентов $f(x)$, так как оставляет элементы поля P на месте. Например,

$$\mathcal{A}(3x^2-5)=\mathcal{A}(3)[\mathcal{A}(x^2)]-\mathcal{A}(5)=3[\mathcal{A}(x)]^2-5.$$

Поэтому группа автоморфизмов $\operatorname{Aut} F/P$ характеризуется лишь тем, как автоморфизмы переставляют корни, и потому $\mathrm{G}(F/P)$ — *есть некоторая* ***подгруппа*** *подстановок*. При этом порядок группы $\mathrm{G}(F/P)$ равен степени расширения $[F : P]$ (см. п. 10.4.3).

Действие $\mathcal{A}$ на остальные элементы поля F полностью определяется действием $\mathcal{A}$ на корнях $\alpha_1, \ldots, \alpha_n$, поскольку F конечномерное векторное пространство с базисом, зависящим только от $\{1, \alpha_1, \ldots, \alpha_n\}$. Более того, действие $\mathcal{A}$ может быть полностью определено значением $\mathcal{A}(\theta)$ на единственном *примитивном элементе* θ, который, в свою очередь, определяется через $\{\alpha_1, \ldots, \alpha_n\}$ (см. пп. 10.4.2, 10.4.3).

11.3. Общая картина

Дальнейший путь состоит примерно в следующем. Каждой *подгруппе* $H \subset \mathrm{G}(F/P)$ отвечает *подполе*

$$L \subset F,$$

состоящее из элементов F, неподвижных под действием автоморфизмов из H. И наоборот, каждому $L \subset F$ отвечает подгруппа H автоморфизмов, оставляющих элементы L на месте. В результате изучение всех подполей поля F сводится к изучению всех подгрупп группы $G = \mathrm{G}(F/P)$, что является существенно более простой задачей. При этом каждой *башне* (цепочке вложенных) *полей*

$$P = L_0 \subset L_1 \subset \ldots \subset L_r = F,$$

отвечает *нормальный ряд* вложенных (в противоположном направлении) групп

$$\mathrm{G}(F/P) = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r = \{1\},$$

и наоборот (*соответствие Галуа*).

С задачей решения алгебраических уравнений вся эта кухня сопрягается через механизм *радикальных расширений* (раздел 11.5)[4)].

[4)] Расширение $F \supset P$ *радикально*, если существует цепочка промежуточных полей $P = L_0 \subset L_1 \subset \ldots \subset L_r = F$, где каждое P_j является *простым радикальным расширением* L_{j-1}, т. е. полем разложения многочлена $x^k - \xi$ над L_{j-1}.

Поскольку разрешимость алгебраического уравнения $f(x) = 0$ в радикалах сводится к возможности последовательного решения уравнений вида $z^m - a = 0$, — на языке расширений суть дела заключается в возможности последовательного расширения исходного поля с помощью присоединения на каждом шаге элементов вида $\sqrt[r]{a}$ — с целью получить в итоге расширение, содержащее все корни рассматриваемого уравнения. Критерием существования радикального расширения оказывается *разрешимость группы Галуа* рассматриваемого многочлена.

11.4. Соответствие Галуа

Стержнем теории Галуа является соответствие между структурой расширения полей и структурой подгрупп автоморфизмов. Упаковав детали такого соответствия в одну теорему можно «отделаться одним махом», что удобно для «писателей», но убийственно для читателей. Поэтому здесь лучше двигаться поэтапно, тем более что все шаги достаточно прозрачны.

Первым делом полезно присмотреться к свойствам автоморфизмов из группы $\mathrm{Aut}\, F/P = \mathrm{G}_f$. Как уже отмечалось — см. (11.1) — любое отображение $\mathcal{A} \in \mathrm{Aut}\, F/P$ характеризуется тем, что переставляет корни многочлена f, *полем разложения* которого служит F. Но то же самое автоморфизмы $\mathcal{A} \in \mathrm{Aut}\, F/P$ делают и с корнями любого другого многочлена $h(x)$,

$$h(\gamma) = 0, \quad \gamma \in F \quad \Rightarrow \quad h(\gamma^{\mathcal{A}}) = \mathcal{A}h(\gamma) = 0,$$

т. е. корень γ любого многочлена под действием автоморфизма заменяется некоторым другим корнем $\gamma^{\mathcal{A}}$ того же многочлена. Иначе говоря, *автоморфизм $\mathcal{A} \in \mathrm{G}_f$ переводит любое число $\gamma \in F$ в сопряженное $\gamma^{\mathcal{A}}$*.

Если $g(x)$ — *минимальный многочлен примитивного элемента* θ, то $g(\theta) = 0$ влечет за собой $\mathcal{A}g(\theta) = g(\theta^{\mathcal{A}}) = 0$. Поэтому корни $\theta^{\mathcal{A}} = \mathcal{A}(\theta)$ минимального многочлена $g(x)$ могут быть поставлены во взаимно однозначное соответствие с автоморфизмами из $\mathrm{G}(F/P)$, что еще раз доказывает $|\mathrm{G}(F/P)| = [F : P]$.

11.4.1. *Нормальное расширение $F \supset P$ над любым промежуточным полем L в цепочке $F \supset L \supset P$ — нормально.*

◄ Если $f(x)$ — многочлен над P, корнем которого является *примитивный элемент* θ расширения $F \supset P$, то $f(x)$ тем более можно рассматривать как многочлен над L. При этом $F = L(\theta)$. ►

11.4.2. *Всякому промежуточному полю L в цепочке $F \supset L \supset P$ соответствует подгруппа $H = \mathrm{G}(F/L) \subset \mathrm{G}(F/P)$ автоморфизмов, оставляющих на месте все элементы из L. Соответствие взаимно однозначно.*

◄ Утверждение в принципе тривиально. Совокупность автоморфизмов из группы $\mathrm{Aut}\, F/P$, оставляющих на месте элементы некоторого, неважно какого, множества, — является подгруппой [5].

Обратно. Если группа (подгруппа) $H \subset \mathrm{G}(F/P)$ оставляет неподвижным некоторое множество L, в смысле $x^{\mathcal{A}} = x$ для $x \in L$, $\mathcal{A} \in H$, то L — поле, потому что для $x, y \in L$

$$(x+y)^{\mathcal{A}} = x^{\mathcal{A}} + y^{\mathcal{A}} = x + y, \quad (xy)^{\mathcal{A}} = x^{\mathcal{A}} y^{\mathcal{A}} = xy.$$

При этом, очевидно, $L \supset P$.

Остается вопрос о взаимной однозначности, для решения которого достаточно установить, что H является группой Галуа $\mathrm{G}(F/L)$, о которой можно говорить [6] в силу п. 11.4.1. Автоморфизмы из $\mathrm{G}(F/L)$ по определению оставляют на месте элементы L — поэтому $H \subset \mathrm{G}(F/L)$. Если бы группа Галуа $\mathrm{G}(F/L)$ содержала больше элементов, чем H, то степень $[F : L]$ была бы больше порядка $|H|$. Но $[F : L]$ равна степени *примитивного элемента* θ расширения F над L. И если $H = \{\mathcal{A}_1, \ldots, \mathcal{A}_r\}$, то θ — корень уравнения r-й степени

$$(x - \theta^{\mathcal{A}_1}) \ldots (x - \theta^{\mathcal{A}_r}) = 0,$$

коэффициенты которого инвариантны под действием автоморфизмов из H, — и потому принадлежат L. Поэтому степень элемента θ не больше r, откуда $[F : L] = |H|$, а значит $H = \mathrm{G}(F/L)$. ►

11.4.3. *Если промежуточным полям L_1, L_2 в цепочке*

$$F \supset L_1 \supset L_2 \supset P$$

соответствуют подгруппы $H_1, H_2 \subset \mathrm{G}(F/P)$,

$$H_1 = \mathrm{G}(F/L_1), \quad H_2 = \mathrm{G}(F/L_2),$$

то $H_1 \subset H_2$.

---

[5] Потому что композиция таких автоморфизмов обладает тем же свойством. Другое дело, существует ли такое нетривиальное (не совпадающее ни с P, ни с F) неподвижное множество L.

[6] О группах Галуа допустимо говорить лишь в случае нормальных расширений.

◄ «Противоход» включений $L_1 \supset L_2 \Leftrightarrow H_1 \subset H_2$ очевиден (разумеется, если пребывать в контексте). ►

11.4.4. *Пусть ξ — некоторый элемент из расширения $F \supset P$ и подгруппа $H \subset \mathrm{G}(F/P)$ состоит из автоморфизмов, оставляющих элемент ξ неподвижным. Тогда автоморфизмы из $\mathrm{G}(F/P)$, переводящие ξ в сопряженные элементы образуют смежные классы по подгруппе H.*

◄ Пусть $\mathcal{A}, \mathcal{B} \in \mathrm{G}(F/P)$ и $\xi^{\mathcal{A}} = \xi^{\mathcal{B}}$, т. е. $\mathcal{A}(\xi) = \mathcal{B}(\xi)$. Тогда

$$\mathcal{B}^{-1}\mathcal{A}(\xi) = \mathcal{B}^{-1}\mathcal{B}(\xi) = \xi,$$

что означает $\mathcal{B}^{-1}\mathcal{A} \in H$, и поэтому $\mathcal{A}$ и $\mathcal{B}$ принадлежат одному и тому же смежному классу $\mathcal{B}H$.

Обратно, $\mathcal{B}^{-1}\mathcal{A} \in H \Rightarrow \mathcal{A}(\xi) = \mathcal{B}(\xi)$. ►

Пункт 11.4.4 раскрывает природу следующего принципиального результата.

11.4.5. *Промежуточное поле L в цепочке $F \supset L \supset P$ нормально в томм случае, когда подгруппа $H \subset \mathrm{G}(F/P)$ автоморфизмов, оставляющих элементы L неподвижными, — нормальна.*

◄ Пусть нормальному полю L отвечает группа H, т. е. $\mathcal{B}(\xi) = \xi$ для $\xi \in L$, $\mathcal{B} \in H$. Нормальное поле содержит все элементы вместе с сопряженными, поэтому

$$\forall\, \mathcal{A} \in \mathrm{G}(F/P) : \mathcal{A}(\xi) \in L \Rightarrow \forall\, \mathcal{B} \in H : \mathcal{B}\mathcal{A}(\xi) = \mathcal{A}(\xi).$$

Последнее означает $\mathcal{A}^{-1}\mathcal{B}\mathcal{A} \in H$ для $\mathcal{B} \in H$ и всех $\mathcal{A} \in \mathrm{G}(F/P)$. Но это и есть условие нормальности группы H.

Обратное устанавливается аналогично. ►

11.5. Простое радикальное расширение

Вопрос представимости корней через коэффициенты уравнений с помощью рациональных операций и радикалов после определенных уточнений [5] сводится к возможности записи корней в виде [7)]

$$\sqrt[k]{\ldots + \sqrt[l]{\ldots + \sqrt[m]{\ldots}}}, \tag{11.2}$$

[7)] С учетом возможности избавляться от иррациональности в знаменателе.

что имеет люфт интерпретации, но при соблюдении определенных предосторожностей [8] дает адекватный инструмент для решения проблемы, см. [5].

Если говорить точнее, разрешимость в радикалах алгебраического уравнения $f(x) = 0$ сводится к возможности последовательного решения уравнений вида $z^m - a = 0$. Например, если $f(x)$ преобразуется в

$$f(x) = [(x^{n_1} - a)^{n_2} - b]^{n_3} - c, \tag{11.3}$$

то решением $f(x) = 0$ будет

$$\sqrt[n_1]{a + \sqrt[n_2]{b + \sqrt[n_3]{c}}}.$$

Поэтому суть дела сводится к возможности преобразования полинома $f(x)$ к виду типа (11.3), где числа типа a, b, c «радикально» выражаются через коэффициенты исходного полинома $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$.

Эквивалентная точка зрения заключается в последовательном расширении исходного поля, например $\mathbb{Q}$, с помощью присоединения на каждом шаге элементов вида $\sqrt[r]{a}$, — где a принадлежит расширению, возникшему на предыдущем шаге, — с целью получить в итоге расширение, содержащее все корни рассматриваемого уравнения. Это как раз будет означать разрешимость в радикалах.

Адекватность такого подхода решаемой проблеме, конечно, заслуживает осмысления, чему в книгах обычно уделяется определенное внимание. Нередко с отрицательным результатом — потому что здесь требуется лишь оживить в памяти определения о расширениях полей и привести их (определения) в соприкосновение. А это работа, которую в любом случае необходимо проделать самостоятельно.

Исходным элементом рассматриваемой идеологии служит *поле разложения* многочлена $x^n - a$, $a \in P$, — называемое ***простым радикальным расширением*** поля P.

При условии существования последовательности промежуточных полей

$$P = L_0 \subset L_1 \subset \ldots \subset L_r = F, \tag{11.4}$$

[8] Если радикал $\sqrt[r]{a}$, многозначный по своей природе, входит в (11.2) несколько раз, то ему при вычислении каждого корня уравнения придается одно и то же значение. В то же время при любом выборе значений входящих радикалов формула (11.2) обязана давать корень изучаемого уравнения.

где каждое L_j является *простым радикальным расширением* L_{j-1}, — расширение $F \supset P$ называют ***радикальным.***

Простое радикальное расширение $P(\zeta, \zeta^2, \ldots, \zeta^{n-1}) \supset P$, содержащее все корни n-й степени из единицы, есть *поле разложения* кругового полинома[9] $\Phi_n(x)$. *Уравнение деления круга*

$$\Phi_n(x) = 0$$

имеет корнями только примитивные корни $\sqrt[n]{1}$, но их достаточно для требуемого расширения P.

В то же время ясно, что простое расширение $P(\zeta)$ с помощью любого *примитивного корня* ζ порождает то же самое расширение[10] $P(\zeta, \zeta^2, \ldots, \zeta^{n-1})$. А поскольку любой *примитивный корень* ζ порождает циклическую группу всех корней $\sqrt[n]{1}$, то *группа Галуа* $\mathrm{G}(P(\zeta)/P)$ также будет циклической[11].

При этом, разумеется, в случае простого n, порядок $|\mathrm{G}(P(\zeta)/P)| = n$, т. е. *степень расширения* $[P(\zeta) : P] = n$. Если же n составное, то степень расширения и порядок группы Галуа равны

$$[P(\zeta) : P] = |\mathrm{G}(P(\zeta)/P)| = \varphi(n) + 1,$$

где $\varphi(n)$ — *функция Эйлера* (раздел 10.5).

При переходе от ситуации $x^n - 1$ к более общей $x^n - a$ — возникают новые обстоятельства. Если θ — произвольный корень уравнения $x^n - a = 0$, т. е. $\theta^n = a$, а ζ — примитивный корень $\sqrt[n]{1}$, то корнями уравнения $x^n - a = 0$ служат

$$\theta, \theta\zeta, \ldots, \theta\zeta^{n-1} \tag{11.5}$$

и $P(\theta, \zeta)$ дает искомое *простое радикальное расширение* поля P. Но каково фактическое расширение и каковы соответствующие группы Галуа?

---

[9] См. раздел 10.5.

[10] Поскольку ряд $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, где ζ — любой *примитивный корень*, исчерпывает все корни $\sqrt[n]{1}$.

[11] Ибо автоморфизмам из $\mathrm{G}(P(\zeta)/P)$ очевидным образом ставится в соответствие возведение примитивных корней в ту или иную степень. Если $\zeta \in P$, то фактического расширения не происходит, группа Галуа тривиальна.

11.5.1. Теорема. *Группа Галуа* $\mathrm{G}(P(\theta,\zeta)/P)$ *простого радикального расширения — разрешима.*

◀ Есть три возможности:

(i) $\theta \in P$, $\zeta \notin P$ — ситуация ничем не отличается от рассмотренной выше (с присоединением к полю корней из единицы).

(ii) $\theta \notin P$, $\zeta \in P$ — тогда автоморфизмы $\mathcal{A}$ из группы Галуа имеют вид $\theta \mapsto \theta\zeta^{\lambda}$, поэтому каждому $\mathcal{A}$ соответствует определенный корень ζ^{λ}, и группа Галуа опять-таки циклична.

(iii) Общий случай $\theta \notin P$, $\zeta \notin P$ — исчерпывается последовательным расширением. Сначала к P подсоединяется ζ, затем θ. Но почему группа Галуа разрешима — сразу не ясно.

Любой автоморфизм $\mathcal{A}$ из $\mathrm{G}(P(\theta,\zeta)/P)$ переводит корень ζ многочлена $x^n - 1$ в сопряженный (см. раздел 11.4), т. е.

$$\boxed{\zeta^{\mathcal{A}} = \zeta^a.}$$

При этом ζ^a не может быть корнем многочлена $x^m - 1$ меньшей степени $m < n$, потому что ζ — примитивный корень $x^n - 1$. Поэтому a взаимно просто с n.

Корень θ автоморфизм $\mathcal{A}$ переводит в один из корней (11.5) уравнения $x^n - a = 1$. Поэтому

$$\boxed{\theta^{\mathcal{A}} = \zeta^b\theta}$$

при некотором b. В итоге каждый автоморфизм $\mathcal{A}$ однозначно характеризуется двумя числами a и b.

При этом, как легко проверить, если $\mathcal{A}_1$ характеризуется парой $[a,b]$, а $\mathcal{A}_2$ — парой $[c,d]$, то композиции $\mathcal{A}_1\mathcal{A}_2$ отвечает пара $[ac, bc+d]$. Таким образом, группа Галуа $\mathrm{G}(P(\theta,\zeta)/P)$ изоморфна группе $\{[a,b]\}$, разрешимость которой была установлена в разделе 6.4. ►

11.6. Циклические расширения

При доказательстве теоремы 11.5.1 — пункт **(ii)** — отмечалось, что в случае $\theta \notin P$, $\zeta \in P$ — группа Галуа циклична. Верно также обратное.

11.6.1. *Если поле* P *содержит примитивный корень* $\zeta = \sqrt[n]{1}$, *то любое его циклическое расширение*[12] $\widetilde{P} \supset P$ *степени* n *— образуется присоединением к* P *корня неприводимого над* P *многочлена* $x^n - a$.

[12] *Циклическим расширением поля* называют расширение, группа Галуа которого циклична.

◄ Пусть автоморфизм $\mathcal{A}$ из $\mathrm{G}(\widetilde{P}/P)$ порождающий, т. е. $\mathcal{A}^n = 1$. В *резольвенте Лагранжа*

$$(\zeta, \omega) = \omega + \zeta\mathcal{A}\omega + \ldots + \zeta^{n-1}\mathcal{A}^{-1}\omega, \quad \omega \in \widetilde{P}, \tag{11.6}$$

элемент ω выберем так, чтобы [13] $(\zeta, \omega) \neq 0$.

Применяя $\mathcal{A}$ к (11.6), имеем $\mathcal{A}(\zeta, \omega) = \zeta^{-1}(\zeta, \omega)$. Повторение процесса дает $\mathcal{A}^k(\zeta, \omega) = \zeta^{-k}(\zeta, \omega)$ для $k = 1, \ldots, n-1$. Единственный автоморфизм, не двигающий (ζ, ω), — тождественный. Поэтому $\nu = (\zeta, \omega)$ порождает все поле $\widetilde{P} = P(\nu)$. ►

11.7. Главный результат

Перед «заключительным аккордом» надо было бы провести еще некоторые приготовления, но аудитория из-за рутины часто теряет терпение. Поэтому перейдем к главному.

11.7.1. Теорема Галуа. *Неразложимое в P уравнение $f(x) = 0$ разрешимо в радикалах в томм случае, когда группа Галуа многочлена f — разрешима.*

◄ «Мотором» обоснования является *соответствие Галуа* (раздел 11.4), благодаря которому из наличия башни полей

$$P = L_0 \subset L_1 \subset \ldots \subset L_r = F \tag{11.7}$$

следует существование нормального ряда групп

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}, \tag{11.8}$$

и наоборот.

Если уравнение $f(x) = 0$ разрешимо в радикалах, и (11.7) — соответствующая цепочка *простых радикальных расширений* $L_i \subset L_{i+1}$, то все факторы G_{i-1}/G_i абелевы (теорема 11.5.1), и для разрешимости группы Галуа $\mathrm{G}_f = \mathrm{G}(F/P)$ не хватает одного: гарантии нормальности расширения [14] F. Удобный выход из положения дает элементарный факт: «*всякое радикальное расширение содержится в нормальном радикальном расширении*» (см. ниже), — на основании которого доказательство завершается просто и коротко [14]. Но интуитивно предпочтительнее, пожалуй, рассуждение у Ван дер Вардена [5], которое более расплывчато, но зато дает представление о причинах возможных затруднений и опирается на элементарное

[13] Это можно сделать в силу линейной независимости $1, \mathcal{A}, \ldots, \mathcal{A}^{n-1}$, которая несложно устанавливается [24].

[14] Потому что последовательность нормальных расширений не обязана давать нормальное расширение.

изменение порядка расширений. В силу $\sqrt[rs]{a} = \sqrt[r]{\sqrt[s]{a}}$ используется возможность последовательного присоединения к полю P корней из единицы (и корней из чисел a) *простых степеней*, входящих в разложения всех показателей корней, участвующих в (11.2). В результате получается серия *циклических нормальных расширений*, каковые нормальны *в силу простоты степеней*. Далее остается лишь утрясти порядок таких расширений и некоторые мелкие детали [5]. Группа G_f получается разрешимой.

Пусть теперь, наоборот, группа G_f разрешима. Тогда G_f имеет нормальный ряд вида (11.8) с абелевыми факторами, который можно уплотнить до композиционного ряда уже с *циклическими факторами* простых порядков. Соответствие Галуа в этом случае гарантирует существование цепочки (11.7), в которой последовательные расширения $L_i \subset L_{i+1}$ цикличны, простых степеней. Далее, чтобы воспользоваться результатом п. 11.6.1, присоединим к P примитивный корень ζ из единицы степени $n = |G_f|$, и тогда (11.7) перейдет в цепочку

$$P \subset P(\zeta) \subset L_1(\zeta) \subset \ldots \subset F(\zeta),$$

в которой, в силу п. 11.6.1, $F(\zeta)$ оказывается радикальным расширением поля P, содержащим все корни уравнения $f(x) = 0$. ►

Вот упомянутый выше факт, дополнительно характеризующий радикальные расширения.

• *Любое радикальное расширение содержится в некотором нормальном радикальном расширении.*

◄ Для радикального расширения (11.4), т. е.

$$P = L_0 \subset L_1 \subset \ldots \subset L_r = F,$$

в случае $r = 1$ нормальность $F = P(\theta, \zeta)$ фактически была установлена при доказательстве теоремы 11.5.1.

Далее используем индукцию. Допустим, L_{r-1} содержится в нормальном радикальном расширении $\widetilde{L}_{r-1} \supset P$ и $F = L_{r-1}(\nu)$, $\nu^n = a \in L_{r-1}$. Пусть $f(x)$ — минимальный многочлен элемента a над P, и L — поле разложения полинома $f(x^n)$. Тогда *композит* $\widetilde{L}_{r-1} \cdot L$ — искомое нормальное радикальное расширение. ►

11.8. Неразрешимые уравнения

Главная роль теоремы 11.7.1 — принципиальная. Но результат можно использовать и утилитарно, для анализа конкретных уравнений, — что требует умения вычислять группы Галуа и уводит исследование в новую плоскость. Для указания частных случаев неразрешимых уравнений годится путь полумер.

11.8.1. *Неприводимость многочлена $f(x)$ равносильна транзитивности его группы Галуа* $\mathrm{G}_f = \mathrm{G}(F/P)$.

◀ Пусть ν — произвольный корень f. Нормальность расширения $F \supset P$ означает, что все сопряженные ν числа принадлежат F. В том числе:

$$\nu^{\mathcal{A}_1}, \ldots, \nu^{\mathcal{A}_n}, \tag{11.9}$$

где $\mathcal{A}_1, \ldots, \mathcal{A}_n$ — все автоморфизмы группы $\mathrm{G}(F/P)$.

Любое $\nu^{\mathcal{A}_j}$ является (раздел 11.2) корнем f, и f для $\nu^{\mathcal{A}_j}$ — минимальный полином. Но тогда все числа (11.9) обязаны быть различны (что есть транзитивность группы G_f), иначе произведение

$$\prod(x - \nu^{\mathcal{A}_j})$$

по различным $\nu^{\mathcal{A}_j}$ давало бы полином, «меньший» минимального. ▶

В случае простого n транзитивная группа G_f, содержащая хотя бы одну транспозицию, совпадает с $\mathbf{S}_n$ (упражнение в конце раздела 2.2). Если $f(x)$ имеет *ровно два комплексных корня*, автоморфизм комплексного сопряжения $z \mapsto \bar{z}$, переставляющий комплексные корни и не трогающий вещественные, дает нужную транспозицию в G_f. Транзитивность G_f обеспечивает неприводимость полинома f над P.

Полином $f(x) = x^5 + 3x + 3$ имеет ровно два комплексных корня и *неприводим* над $\mathbb{Q}$ (по *критерию Эйзенштейна*). Поэтому его группа Галуа совпадает с $\mathbf{S}_5$, которая содержит простую (теорема 6.3.3) группу $\mathbf{A}_5$, — и потому неразрешима. Соответственно, уравнение

$$x^5 + 3x + 3 = 0$$

неразрешимо в радикалах.

Понятно, что уравнение

$$x^k(x^5 + 3x + 3) = 0, \quad k > 0,$$

также неразрешимо в радикалах. Это объясняет, почему теория ориентируется на неприводимые многочлены.

Группа Галуа уравнения n-й степени, коэффициенты которого взяты более-менее наугад, есть $\mathbf{S}_n$, и потому при $n \geqslant 5$ — неразрешима. Таким образом, уравнения высоких степеней, разрешимые в радикалах, являются исключением.

11.9. Построения циркулем и линейкой

Если исходить из заданного поля $P \subset \mathbb{C}$, то с помощью циркуля и линейки можно построить любое комплексное число c, квадрат которого [15] $c^2 \in P$. Аналитическая геометрия присовокупляет сюда некоторые элементарные соображения, в итоге возможности циркуля и линейки описываются последовательным расширением исходного поля:

$$P \subset P(c_1) \subset \ldots \subset P(c_1, \ldots, c_r) = F,$$

где

$$c_1^2 \in P, \quad c_2^2 \in P(c_1), \quad \ldots, \quad c_r^2 \in P(c_1, \ldots, c_{r-1}).$$

Иначе говоря, возможность построения сводится к разрешимости некоторого алгебраического уравнения (для каждой задачи — своего) в *квадратных* радикалах.

Степень каждого квадратичного расширения равна 2. Поэтому $[F : P] = 2^r$, и в случае $[\mathbb{Q}(z) : \mathbb{Q}] \neq 2^r$ при любом $r > 0$, — число z невозможно построить, отправляясь от отрезков рациональной длины.

Невозможность *удвоения куба* сразу следует из неприводимости многочлена $x^3 - 2$, влекущей за собой $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^r$.

Построение правильного p-угольника (p простое) равносильно построению числа

$$z = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}, \quad z^{p-1} + \ldots + z + 1 = 0,$$

откуда ясно

$$[\mathbb{Q}(z) : \mathbb{Q}] = p - 1.$$

Следовательно, необходимо

$$p = 2^r + 1$$

при некотором r. Такие p называют *простыми числами Ферма*: 3, 5, 17, 257, 65 537.

[15] Что базируется на возможности по двум отрезкам a и b построить гипотенузу $c = \sqrt{a^2 + b^2}$.

11.10. Дополнение

• Алгоритмы вычисления групп Галуа мы оставляем за кадром. Идея вычисления опирается на два обстоятельства. Во-первых, G_f изоморфна группе перестановок корней, не меняющих алгебраические зависимости между корнями. Во-вторых, о таких перестановках можно судить косвенно по коэффициентам многочлена из-за наличия взаимосвязей (формул Виета).

• Хотя игровой площадкой в главе были числовые поля нулевой характеристики, результаты после внесения определенных поправок остаются справедливыми в более широком диапазоне, в том числе — для конечных полей. В то же время ограничение горизонтов комплексной плоскостью $\mathbb{C}$ позволяет взглянуть на ситуацию с позиций ТФКП.

Корни многочлена

$$f(z) = z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n$$

есть нули функции $z(w)$, определяемой равенством $w = f(z)$. Аналитическая функция $z(w)$, разумеется, многозначна. При движении по кривой C (проходящей только через регулярные точки) из точки w_0 в точку w_1 значение функции меняется с $z(w_0)$ на $z(w_1)$. При этом значение $z(w_1)$ зависит не только от «конечного пункта» w_1, но и от пути C.

В случае движения по *замкнутой* ориентированной кривой C (не проходящей через точки ветвления решений), которая начинается и заканчивается в w_0, решение z_j уравнения $w_0 = f(z)$ перейдет в некоторое другое решение z_k того же уравнения. В результате на множестве решений $z_1, \ldots, z_n$ уравнения $w_0 = f(z)$ возникает *группа подстановок*, которая и является *группой Галуа*[16] многочлена $h(z) = f(z) - w_0$.

Вопрос о разрешимости уравнения $f(z) - w_0 = 0$ в радикалах сводится к принадлежности $z(w)$ классу $\mathcal{R}$ функций, которые могут быть получены из $I(w) \equiv w$ и констант (функций $g(w) \equiv c$) с помощью *сложения*, *вычитания*, *умножения*, *деления*, *а также возведения в целые степени и извлечения корней*. Класс $\mathcal{R}$, как оказывается, характеризуется разрешимостью групп Галуа — групп подстановок, определяемых функциями $z(w)$.

• Рассмотрение проблематики с точки зрения ТФКП позволяет добавить к классу $\mathcal{R}$ однозначные аналитические функции без изменения выводов о разрешимости уравнений — теперь уже с возможностью дополнительных операций. К $\mathcal{R}$ можно добавить и многозначные функции типа логарифма, но тогда группы Галуа перестанут быть конечными, что не мешает им в принципе быть разрешимыми или неразрешимыми с аналогичными последствиями.

---

[16] Называемая в теории аналитических (алгебраических) функций *группой монодромии*. Индивидуальные подстановки отвечают классам эквивалентных кривых C.

Глава 12

Группы Ли

Со времени открытия *Софусом Ли* (1842–1899) непрерывных групп [1] уровень недоступности теории был существенно поднят усилиями других математиков [2]. В результате современные руководства по *группам Ли* [9, 18, 19, 27] достигают цели лишь в очень узкой аудитории, а «рецептура» теряет связь с приложениями. Но такова диалектика. Слишком много «хвостов» оставляют упрощенные подходы. С другой стороны, наведение порядка уводит так далеко, что кругом «никого нет». Поэтому, как бы там ни было, пора возвращаться обратно. Жертвуя строгостью и рекордными достижениями. Конечно, путь аскетизма и замалчивания трудностей, избранный в главе, чреват иллюзиями обманчивой простоты, но с этого можно начинать.

12.1. Параметрические группы

Пусть $x \in \mathbb{R}^n$, $a \in \mathbb{R}^r$, и $\{G_a\}$ — семейство непрерывных функций $G_a(x) = G(x, a)$, преобразующих (при заданном параметре a) точки x в точки x' того же пространства $\mathbb{R}^n$. Чтобы семейство преобразований (*штрих не обозначает дифференцирования*)

$$x' = G(x, a) \tag{12.1}$$

составляло группу (с композицией в качестве умножения), должны выполняться обычные групповые аксиомы.

В частности, групповая операция не должна выводить из $\{G_a\}$, т. е.

$$\boxed{x' = G(x, a), \quad x'' = G(x', b) \quad \Rightarrow \quad x'' = G(x, c)} \tag{12.2}$$

при некотором $c = \varphi(a, b)$. Иными словами, последовательное выполнение двух преобразований типа (12.1) равносильно преобразованию того же вида,

$$G_b G_a = G_{\varphi(a,b)}.$$

---

[1] Итоговая монография (*Lie S.* Vorlesungen über continuierliche Gruppen. Leipzig: Teubner, 1893) — содержит более 800 страниц.

[2] Как говорил *Эйнштейн*, «с тех пор как за теорию относительности принялись математики, я ее уже сам больше не понимаю».

Ассоциативность очевидна. Далее, необходимо $\boxed{G(x,e)\equiv x}$ при некотором значении параметра $a=e$, что гарантирует существование единичного элемента группы. Для простоты обычно полагается $e=0$, т. е. $G(x,0)\equiv x$. Наконец, уравнения (12.1) обязаны иметь решение $x=\psi(x',a)$, причем функция $\psi(x',a)$ после подходящей перепараметризации должна попадать в то же семейство, т. е.

$$\psi(x',a)=G(x',b),\quad b=b(a).$$

Это обеспечивает существование обратных элементов, $G_a^{-1}=G_{b(a)}$.

Чтобы получить определение *группы Ли*, дополнительно надо предположить, что функции $b(a)$ и $\varphi(a,b)$ «достаточное» число раз непрерывно дифференцируемы [3)].

Обратим внимание, что все, кроме дифференцируемости, укладывается в обычные определения группы и сопутствующих понятий. Семейство функций $\{G(x,a)\}$ можно интерпретировать как *действие* (глава 3) группы $\mathbf{G}=\{G_a\}$ на элементах x. А множество

$$\mathrm{Orb}(x)=\{G_a x : G_a\in\mathbf{G}\}$$

представляет собой *орбиту* элемента x.

Однопараметрические группы ($r=1$) дают простейший путь к пониманию общей идеологии *групп Ли*, но одновременно вводят в заблуждение. Суть дела, как выясняется, близка к тому, что и так хорошо известно (интегралы движения, производные по направлению векторного поля). В результате возникает впечатление о безосновательном переиначивании привычных понятий.

12.1.1. *В случае однопараметрической группы с помощью перепараметризации (замены параметра) всегда можно добиться, чтобы* $\varphi(a,b)\equiv a+b$, $b(a)=-a$. *Иначе говоря,*

$$G_bG_a=G_{a+b},\quad G_a^{-1}=G_{-a}. \tag{12.3}$$

Это совсем простой, но принципиальный факт. Разъяснения будут даны позже. Пока же остановимся на более важном, хотя и тривиальном утверждении.

[3)] Это упрощенное определение. Менее понятные варианты можно найти в указанных выше источниках. О причинах возникающих сложностей будет сказано далее.

12.1.2. *Если параметризация группы Ли* $G = \{G_a\}$ *такова, что выполняется* (12.3), *то* $G(x, a)$ *может быть получено как решение задачи Коши*:

$$\boxed{\frac{\partial G}{\partial a} = \xi(f), \quad G\big|_{a=0} = x,} \tag{12.4}$$

где

$$\xi(x) = \left.\frac{\partial G(x, a)}{\partial a}\right|_{a=0}. \tag{12.5}$$

◄ Пусть $G(x, 0) \equiv x$. Тогда

$$G(x, a + \Delta a) = G(x, a) + \frac{\partial G(x, a)}{\partial a}\Delta a + o(\Delta a), \tag{12.6}$$

$$G(G(x, a), \Delta a) = \underbrace{G(G(x, a), 0)}_{G(x,a)} + \underbrace{\frac{\partial G(G(x, a), 0)}{\partial \Delta a}}_{\xi(G(x,a))}\Delta a + o(\Delta a). \tag{12.7}$$

В предположении (12.3) левые части (12.6) и (12.7) — равны. Поэтому равны и правые. Откуда

$$\boxed{\frac{\partial G(x, a)}{\partial a} = \xi[G(x, a)].} \quad ► \tag{12.8}$$

Из п. 12.1.2 следует, что *вся группа* $\{G(x, a)\}$ *определяется производными в нуле* (12.5).

(!) Последнее имеет место и в многопараметрическом случае. *Группу Ли определяет сколь угодно малая окрестность единичного элемента.* Все семейство $\{G(x, a)\}$ определяется его поведением в окрестности тождественного преобразования $G(x, 0) \equiv x$. Это удивительно, потому что причина заключается не в линейности. Напрашиваются, конечно, другие аналогии. Например, задание аналитической функции в окрестности любой точки определяет функцию целиком. В группах Ли возникает нечто подобное.

Необходимо подчеркнуть, что запись (12.4) маскирует банальный факт. *Задача Коши*

$$\frac{dz}{dt} = \xi(z), \quad z(0) = x, \tag{12.9}$$

имеет решение $z(x,t)$, что с точностью до обозначений и есть $G(x,a)=z(x,a)$. Таким образом, *однопараметрические группы Ли* исчерпываются —(!) в предположении (12.3) — *операторами сдвига*[4)]

$$z = G(x,a) = G_a x$$

по траекториям систем диф-уравнений вида (12.9).

• Поскольку система (12.9) автономна, оператор сдвига G_a удовлетворяет *полугрупповому свойству* $G_s G_t = G_{s+t}$, откуда следует $G_a = (G_{\Delta a})^N$ при условии $N\Delta a = a$ и любом N. Поэтому G_a определяется сдвигом $G_{\Delta a}$ за сколь угодно малое «время» Δa, что и было выше предметом обсуждения.

• Если семейство $\{G(x,a)\}$ не удовлетворяет аксиомам группы, то семейство операторов сдвига $\{U_a\}$ по траекториям (12.9) не совпадает с $\{G_a\}$.

Посмотрим, что получается без предположения (12.3). В случае $x' = G(x,a)$, $c = \varphi(a,b)$ имеем, в силу $G(x',b) = G(x,\varphi(a,b))$, тождество

$$\frac{\partial G(x',b)}{\partial b} = \frac{\partial G(x,c)}{\partial c}\frac{\partial \varphi(a,b)}{\partial b},$$

переходящее при $b=0$ в

$$\frac{\partial G(x',0)}{\partial b} = \frac{\partial G(x,a)}{\partial a}\left.\frac{\partial \varphi(a,b)}{\partial b}\right|_{b=0},$$

что можно записать в виде

$$\omega(a)\frac{dx'}{da} = \xi(x'), \tag{12.10}$$

где

$$\xi(x) = \frac{\partial G(x,0)}{\partial a}, \quad \omega(a) = \left.\frac{\partial \varphi(a,b)}{\partial b}\right|_{b=0}.$$

При переходе к новому «времени»

$$\widetilde{a} = \int_0^a \frac{da}{\omega(a)}$$

[4)] Если a считать временем. Более привычно выглядит $U_t x$ вместо $G_a x$.

дифференциальное уравнение (12.10) приобретает форму

$$\frac{dx'}{da'} = \xi(x'), \tag{12.11}$$

т. е. укладывается в формат (12.9), равносильный (12.4), — что *доказывает утверждение* п. 12.1.1, ибо в новом «времени» a' группу задает автономный дифур (12.11), оператор сдвига по траекториям которого обладает *полугрупповым свойством*.

Таким образом, *однопараметрические группы Ли* — необязательно удовлетворяющие (12.3) — исчерпываются *операторами сдвига* по траекториям систем диф-уравнений вида [5)]

$$\frac{dz}{dt} = \sigma(t)\xi(z), \tag{12.12}$$

фазовые траектории которых совпадают с траекториями автономных дифференциальных уравнений (12.9). Отличие — в скорости движения по этим траекториям.

В случае однопараметрической группы

$$x' = ax, \quad y' = \frac{1}{a}y \tag{12.13}$$

единичному элементу отвечает значение параметра $a = 1$. Уравнение (12.4) (с поправкой на «$a = 0$» $\Rightarrow$ «$a = 1$») имеет вид

$$\frac{dG_1}{dt} = G_1, \quad \frac{dG_2}{dt} = -G_2, \qquad G_1(1) = x, \quad G_2(1) = y.$$

Решение $G(x,t) = \begin{bmatrix} xe^t \\ ye^{-t} \end{bmatrix}$ автоматически получается аддитивным по параметру и с описанием группы (12.13) не совпадает. Чтобы вернуться к исходной параметризации надо сделать замену $a = e^t$. Подобного рода «помехи на вторичном уровне» характерны не только для математики.

12.2. Инварианты и первые интегралы

Инвариантами однопараметрических групп служат *первые интегралы*. Напомним основные сведения [4, т. 2].

[5)] Переходящие в автономные — при замене «времени».

Производная по времени скалярной функции $u(x)$ вдоль траекторий $x(t)$ автономного уравнения $\boxed{\dot{x} = \xi(x)}$ равна

$$\dot{u} = \sum_i \frac{\partial u}{\partial x_i}\xi_i(x) = \nabla u \cdot \xi(x),$$

т. е. скалярному произведению градиента $u(x)$ на вектор $\xi(x)$.

Величину $\nabla u \cdot \xi(x)$ называют *производной Ли*, либо *производной $u(x)$ по направлению (вдоль) векторного поля $\xi(x)$*.

Если производная $\dot{u}(x)$ вдоль $\xi(x)$ равна нулю, то траектории $x(t)$ целиком располагаются на поверхностях постоянного уровня $u(x) = \text{const}$. В этом случае говорят, что $u(x)$ является *первым интегралом* системы $\dot{x} = \xi(x)$. Другими словами, любое нетривиальное решение *линейного уравнения с частными производными* $\nabla u \cdot \xi(x) = 0$, т. е.

$$\sum_i \xi_i(x)\frac{\partial u}{\partial x_i} = 0, \tag{12.14}$$

является *первым интегралом* уравнения $\dot{x} = \xi(x)$, — последнее называют *уравнением характеристик*, а его траектории *характеристиками* уравнения (12.14).

Наличие первых интегралов у автономной системы, вообще говоря, редкость. Соответственно, линейное уравнение (12.14) имеет нетривиальные решения лишь в исключительных случаях. Но в достаточно малых окрестностях неособых точек фазового пространства — первые интегралы существуют «всегда» [4, т. 2]. Точнее говоря, в невырожденных точках векторного поля $\xi(x)$ гарантировано локальное существование $n - 1$ первых интегралов. Причина заключается в том, что в малой окрестности неособой точки траектории $\dot{x} = \xi(x)$ почти параллельны, и их можно локальной заменой переменных (диффеоморфизмом) «выпрямить» и перевести в систему

$$\dot{y}_1 = 1, \quad \dot{y}_2 = 0, \quad \ldots, \quad \dot{y}_n = 0, \tag{12.15}$$

имеющую $n - 1$ интегралов движения: $y_2 = c_2, \ldots, y_n = c_n$.

Каждый первый интеграл позволяет понизить порядок изучаемой системы на единицу. Скажем, если $u(x)$ — первый интеграл системы $\dot{x} = \xi(x)$, то выражая, например, x_n из уравнения $u(x) = c$ (при надлежащем выборе константы c), получим $x_n = \varphi(x_1, \ldots, x_{n-1})$, после чего остается решить систему

$$\dot{x}_i = \xi_i(x_1, \ldots, x_{n-1}, \varphi(x_1, \ldots, x_{n-1})) \quad (i = 1, \ldots, n-1),$$

что отражает суть идеи.

Другая ситуация, имеющая непосредственное отношение к группам Ли, возникает в связи с рассмотрением в $\mathbb{R}^n$ *неавтономных систем* $\dot{x} = f(x, t)$ и *первых интегралов* $u(x, t)$, *зависящих от времени*, — каковыми называют функции $u(x, t)$, являющиеся первыми интегралами *расширенной автономной системы*:

$$\begin{cases} \dot{x} = f(x, t), \\ \dot{t} = 1. \end{cases}$$

Сведéние к предыдущему случаю создает впечатление, что говорить, собственно, не о чем. Но ситуация другая. В естественных предположениях[6] — *всегда существует* n *функционально независимых первых интегралов*

$$u_1(x, t) = c_1, \quad \ldots, \quad u_n(x, t) = c_n. \tag{12.16}$$

Остальные первые интегралы функционально зависят от (12.16).

◀ Если $x = x(x_0, t)$ — решение системы $\dot{x} = f(x, t)$, то разрешение $x = x(c, t)$ относительно вектора c дает n первых интегралов $c_i = \psi_i(x, t)$. ▶

Инфинитезимальные операторы. Равенство (12.14) можно записать в виде $\boxed{X(u) = 0}$ с помощью оператора

$$X = \sum_i \xi_i(x) \frac{\partial}{\partial x_i}, \tag{12.17}$$

где $\partial/\partial x_i$ обозначает частное дифференцирование, под знак которого автоматически попадает функция $u(x)$ при воздействии на нее оператором X.

В случае (12.5) $\xi_i(x) = \left.\dfrac{\partial G_i(x, a)}{\partial a}\right|_{a=0}$, — (12.17) называется *инфинитезимальным оператором* группы $\{G(x, a)\}$ с *касательным* в нуле векторным полем $\xi(x)$.

(!) Если единичным элементом группы является $G(x, a_0)$, то формула для $\xi_i(x)$ меняется на

$$\xi_i(x) = \left.\frac{\partial G_i(x, a)}{\partial a}\right|_{a=a_0}.$$

[6] Локальная единственность плюс нелокальная продолжимость всех решений системы $\dot{x} = f(x, t)$.

Примеры

• В случае $x' = ax$, $y' = \dfrac{1}{a}y$ единичному элементу группы отвечает значение $a = 1$. Поэтому

$$\left.\frac{\partial ax}{\partial a}\right|_{a=1} = x, \quad \left.\frac{\partial y/a}{\partial a}\right|_{a=1} = -y.$$

В результате

$$X = x\frac{\partial}{\partial x} - y\frac{\partial}{\partial y}.$$

• Для *группы вращений*

$$\begin{cases} x' = x\cos\varphi - y\sin\varphi, \\ y' = x\sin\varphi + y\cos\varphi \end{cases} \tag{12.18}$$

имеем

$$\left.\frac{\partial x'}{\partial \varphi}\right|_{\varphi=0} = -y, \quad \left.\frac{\partial y'}{\partial \varphi}\right|_{\varphi=0} = x.$$

Инфинитезимальный оператор:

$$X = -y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}.$$

Идея *касательного поля* в теории групп Ли — один из краеугольных камней. Для однопараметрических групп она, по сути, хорошо известна и достаточно наглядна. Семейство *нелинейных* функций $G(x, a)$ (операторов сдвига) однозначно определяется линейным по a движением вдоль касательных векторов

$$\xi(x) = \left.\frac{\partial G(x, a)}{\partial a}\right|_{a=0}.$$

Если функция $u(x)$ инвариантна под действием группы $\{G(x, a)\}$, т. е.

$$\boxed{u[G(x, a)] \equiv u(x),} \tag{12.19}$$

то (12.19) равносильно тому, что вектор $\xi(x)$ в любой точке x касателен к поверхности $u(x) = \text{const}$ — иначе говоря, $X(u) = 0$, т. е. $\xi(x)\nabla u = 0$.

Переход на язык инфинитезимальных операторов — вместо разговоров о дифференциальных уравнениях вида (12.4) — избавляет от неуклюжести в связи с требованием (12.3), в зависимости от чего приходится рассматривать то ли уравнение (12.4), то ли — (12.12), в то время как подобная дилемма принципиального значения обычно не имеет. Как правило, важны касательные направления и сами траектории, а не абсолютные скорости движения.

Функцию $u(x)$, удовлетворяющую условию $X(u) = 0$, называют *инвариантом группы* $\{G(x, a)\}$. Иначе говоря,

$$u\,(G(x, a)) \equiv u(x),$$

что выражает отмеченное выше свойство первого интеграла: содержать траектории целиком на поверхностях постоянного уровня $u(x) = \text{const}$.

Сценарий, конечно, выглядит плагиатом. Новизна — в названиях, аудитория — в недоумении. Может быть, поэтому традиционные изложения групп Ли начинаются с другого конца. Прямо с инфинитезимальных операторов и инвариантов группы, в результате чего о первых интегралах в подоплеке многие так и не догадываются. Тем не менее первоначальное движение по знакомым местам заводит постепенно в джунгли.

Сколько у группы инвариантов? Выше отмечалось, что в автономном случае, о котором вроде бы речь, гарантировано существование лишь локальных инвариантов. На самом деле:

12.2.1. *Однопараметрическая группа имеет $n - 1$ глобальных функционально независимых инвариантов.*

В утверждении 12.2.1 опущено, для краткости формулировки, предположение о глобальной и однозначной разрешимости уравнения $x' = G(x, a)$ относительно x, что здесь подразумевается, и обычно называется *регулярностью действия* группы. Именно это требование позволяет локальные инварианты (см. выше) срастить в глобальные. Понять результат удобнее, видимо, опираясь на следующий принципиальный сам по себе факт:

12.2.2. *Однопараметрическая группа*[7] *невырожденной заменой переменных $y_i = y_i(x)$ может быть приведена к группе переносов вдоль y_1.*

[7] Опять-таки регулярная.

◀ В силу

$$\sum_i \xi_i(x)\frac{\partial}{\partial x_i} = \sum_i \xi_i(x)\frac{\partial y_i}{\partial x_i}\frac{\partial}{\partial y_i},$$

оператор

$$X = \sum_i \xi_i(x)\frac{\partial}{\partial x_i}$$

переходит в

$$\widetilde{X} = \sum_i X(y_i)\frac{\partial}{\partial y_i}.$$

В малой окрестности любой точки векторное поле $\xi(x)$ можно выпрямить, обеспечивая (12.15) в новых координатах y_i, что приводит (локально) к

$$\widetilde{X} = \frac{\partial}{\partial y_1} + 0\cdot\frac{\partial}{\partial y_2} + \ldots + 0\cdot\frac{\partial}{\partial y_n}. \tag{12.20}$$

В силу регулярности действия группы *локальные карты*[8] сращиваются воедино, и тогда (12.20) выполняется глобально. Это означает, что в новых координатах действие группы сводится к сдвигу по координате y_1. ▶

Таким образом, в координатах y_i имеется $n-1$ первых интегралов $y_2(y_1), \ldots, y_n(y_1)$, переходящих при возврате к исходным переменным в $n-1$ интегралов движения $J_1(x), \ldots, J_{n-1}(x)$.

Пример

Инварианты группы растяжений с инфинитезимальным оператором

$$X = 2x\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} + z\frac{\partial}{\partial z}$$

определяет уравнение

$$2x\frac{\partial u}{\partial x} + y\frac{\partial u}{\partial y} + z\frac{\partial u}{\partial z} = 0,$$

стандартно решаемое с помощью уравнения характеристик $\dfrac{dx}{2x} = \dfrac{dy}{y} = \dfrac{dz}{z}$.

В итоге получается два первых интеграла: $y^2/x = C_1$ и $z/y = C_2$. Условие $X(t) = 2x\dfrac{\partial t}{\partial x} = 1$ приводит к $t = \ln\sqrt{x}$. В переменных[9]

$$u_1 = \frac{y^2}{x}, \quad u_2 = \frac{z}{y}, \quad t = \ln\sqrt{x}$$

---

[8] *Локальной картой* называют гомеоморфизм, который осуществляет локальную замену координат.

[9] Замена $t = \ln\sqrt{x}$ выгоднее «тренировочно». Проще положить $t = z$.

группа с инфинитезимальным оператором X — есть группа переносов по t, а любое диф-уравнение, инвариантное по отношению к этой группе, становится «автономным», т. е. его порядок понижается на единицу.

12.3. Инвариантные функции и множества

Как уже отмечалось, функция $u(x)$, инвариантная к действию группы $\{G_a\}$, характеризуется тождеством

$$u(G_a x) \equiv u(x),$$

либо условием $\xi(x)\nabla u = 0$, и точки x под действием элементов группы остаются на «своих» поверхностях постоянного уровня $u(x) = \text{const}$. В том числе сохраняется нулевой уровень. Но иногда важна инвариантность только нулевого уровня. В этом случае нет необходимости, чтобы $u(x)$ была инвариантна.

12.3.1. *Пусть G — группа Ли с инфинитезимальным оператором X и $\nabla u(x) \neq 0$, если $u(x) = 0$. Тогда множество решений уравнения* $\boxed{u(x) = 0}$ *инвариантно относительно G в том случае, когда*

$$X(u) = 0 \quad \textit{при условии} \quad u(x) = 0.$$

Пример [19]

Множество решений уравнения

$$u(x, y) = x^4 + x^2y^2 + y^2 - 1 = 0$$

инвариантно относительно группы вращения $\left(X = -y\dfrac{\partial}{\partial x} + x\dfrac{\partial}{\partial y}\right)$. Действительно,

$$X(u) = -4x^3y - 2xy^3 + 2x^3y + 2xy = -2xy(x^2 + 1)^{-1}u(x, y),$$

и поэтому $X(u) = 0$, если $u(x, y) = 0$. Градиент u вырожден только в нулевой точке ($x = y = 0$), но $u(0, 0) \neq 0$.

«Секрет» раскрывает представление

$$u(x, y) = (x^2 + 1)(x^2 + y^2 - 1),$$

откуда ясно: $u(x, y) = 0 \Leftrightarrow x^2 + y^2 = 1$.

Надо иметь в виду, что инвариантность диф-уравнений подразумевает нечто подобное. Уравнение $\dot{x} + \alpha x^2 = \beta t^{-2}$ инвариантно

к группе преобразований $t = kt'$, $x = (1/k)x'$ не потому, что не меняет формы, а потому что при подстановке $t \mapsto kt$, $x \mapsto (1/k)x$ переходит в эквивалентное уравнение

$$\frac{1}{k^2}(\dot{x} + \alpha x^2 - \beta t^{-2}) = 0 \quad (k > 0).$$

Разумеется, встречаются более запутанные варианты.

При концентрации внимания на корнях уравнения действие группы можно сузить на множество решений $u(x) = 0$ — в результате возникает новая группа и в какой-то мере новая ситуация.

Рассмотрим, например, алгебраическое уравнение $P(x) = x^2 + x + 1 = 0$, корни которого выдерживают преобразования $x' = x^k$ при любом $k \in \mathbb{Z}$, не кратном 3. (?) Скажем, для $x' = x^{-1}$ получается $P(x') = P(x)/x^2$, а в случае $x' = x^2$:

$$P(x') = x^4 + x^2 + 1 = (x^2 - x + 1)P(x).$$

Поэтому $P(x) = 0 \Rightarrow P(x') = 0$. Полином, таким образом, преображается, но корни остаются корнями, хотя под действием элементов группы могут меняться местами. В результате образуется фактор-группа перестановок корней. На этом пути и возникают, собственно, *группы Галуа*.

Левые части *рациональных отношений*

$$\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n} = 0$$

между корнями $x_1, \dots, x_n$ алгебраического уравнения, где все $a_{i_1,\dots,i_n}$ — рациональны, перестановка корней σ переводит в выражения

$$\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n},$$

в результате чего равенство нулю может нарушаться. Подгруппа перестановок, сохраняющих все рациональные отношения между корнями, является *группой Галуа*.

Пример в обрамлении *групп Ли* выглядит белой вороной, но это не совсем так. Идеологии дискретных и непрерывных групп во многом пересекаются, и поэтому барьер между ними лучше не ставить. Более того, в приложениях часто имеет смысл рассматривать комбинации дискретных и непрерывных групп. Дифференциальные уравнения, которые представляются вотчиной *групп Ли*, — благодатный объект с точки зрения нечувствительности и к дискретным преобразованиям. Например, инвариантность диф-уравнения $\sum_j a_j x^{(j)} = 0$ к обращению времени — влечет за собой равенство нулю всех коэффициентов a_j с нечетными номерами.

12.4. О разделении переменных

Вернемся к вопросам о методе разделения переменных, которые в разделе 1.3 повисли без ответов.

В одном из примеров рассматривалось уравнение

$$\frac{dx}{dt} + x - 3t = 0, \tag{12.21}$$

нечувствительное к действию преобразований

$$t' = t + a, \quad x' = x + 3a. \tag{12.22}$$

Инвариант группы (12.22) — функция $z = x - 3t$. Замена $x \mapsto z + 3t$ приводила к уравнению с разделяющимися переменными $\dfrac{dz}{z+3} = -dt$, интегрирование которого в итоге давало решение

$$x(t) = 3t + Ce^{-t} - 3.$$

Обратим внимание, что инвариант группы $z = x - 3t$ не обязан быть и не является инвариантом (первым интегралом) решаемого дифура.

Причина происшедшего разделения переменных связана не столько с уравнением (12.21), сколько с наличием инвариантной группы (12.22), которая после замены $t \mapsto t$, $x \mapsto z + 3t$ становится в переменных (z, t) группой переносов вдоль оси t:

$$t' = t + a, \quad z' = z.$$

Общий же вид уравнения $\dot{z} = f(z, t)$, неважно какого, но инвариантного по отношению к такой группе [10], есть

$$\frac{dz}{dt} = f(z) \quad \Rightarrow \quad \frac{dz}{f(z)} = dt.$$

В любом диф-уравнении, инвариантном к (12.22), переменные разделяются *заочно* той же самой заменой.

Таким образом, в случае двух переменных работает единый рецепт. Одной новой переменной назначается инвариант группы, другая переменная выбирается так, чтобы по ней происходил сдвиг (перенос). Например, для группы

$$x' = ax, \quad t' = a^2 t \tag{12.23}$$

[10] В силу $f(z, t + a) \equiv f(z, t)$.

инвариантом служит $z = x^2/t$. Замена $z = x^2/t$, $\tau = \tau(t)$ переводит оператор

$$X = x\frac{\partial}{\partial x} + 2t\frac{\partial}{\partial t}$$

в

$$\widetilde{X} = X(z)\frac{\partial}{\partial z} + X(\tau)\frac{\partial}{\partial \tau} = X(\tau)\frac{\partial}{\partial \tau}.$$

Выбор $X(\tau) = 2t\dfrac{\partial \tau}{\partial t} = 1$ приводит к $\tau = \ln\sqrt{t}$. В переменных (z, τ) действие группы сводится к переносу по τ. Соответствующая замена развязывает переменные в любом диф-уравнении, инвариантном относительно группы (12.23).

Вообще говоря, выбор второй переменной так, чтобы по ней получался чистый сдвиг, не всегда обязателен. Вместо $\dot{z} = f(z)$ может получиться уравнение $\dot{z} = \omega(t)f(z)$ тоже с разделяющимися переменными. Но в принципе вторая переменная требует заботы. Скажем

$$\frac{dy}{dx} = \frac{y + xf(x^2 + y^2)}{x - yf(x^2 + y^2)} \tag{12.24}$$

с произвольной (до разумных пределов) функцией f — описывает класс дифференциальных уравнений, инвариантных относительно группы вращений [11] (12.18). Переход к полярным координатам в любом из уравнений вида (12.24) разделяет переменные. Но если ограничиться лишь заменой $z = x^2 + y^2$, оставив в качестве второй переменной x, — ничего не получится.

При большей размерности описанная технология требует определения всех $n - 1$ инвариантов — см. раздел 12.2. В силу п. 12.2.2 любое уравнение

$$\frac{dx}{dx_1} = f(x), \quad x \in \mathbb{R}^n,$$

инвариантное относительно однопараметрической группы, заменой переменных $y(x)$ может быть преобразовано в фактически «автономную» систему

$$\frac{dy_i}{dy_1} = \widetilde{f}_i(y_1, \ldots, y_n)$$

$(n - 1)$-го порядка, поскольку $\widetilde{f}_1 \equiv 1$, а остальные $\widetilde{f}_i$ не зависят от y_1, поскольку группа сведена к группе переносов вдоль y_1.

[11] Описание классов диф-уравнений, инвариантных относительно той или иной группы, — стандартная задача, которая привлекает внимание определенной части исследователей.

12.5. Многопараметрический сценарий

В случае многопараметрических групп ситуация идеологически остается вроде бы прежней, но декорации меняются. Функция $u(x)$ под действием преобразования

$$G_i(x_1, \ldots, x_n; \delta a_1, \ldots, \delta a_r), \quad i = 1, \ldots, n$$

получает приращение [12)]

$$\Delta u = \sum_{j=1}^{r} \delta a_j \left(\sum_{i=1}^{n} \xi_{ij}(x) \frac{\partial u}{\partial x_i} \right) + o(\|\delta a\|) =$$

$$= \sum_{j=1}^{r} \delta a_j X_j u + o(\|\delta a\|), \tag{12.25}$$

где

$$X_j = \sum_{i=1}^{n} \xi_{ij}(x) \frac{\partial}{\partial x_i}, \quad j = 1, \ldots, r, \tag{12.26}$$

— *инфинитезимальные операторы* группы, которых теперь r штук вместо одного, а «касательные поля» определяются элементами

$$\xi_{ij}(x) = \left. \frac{\partial G_i(x, a)}{\partial a_j} \right|_{a=0}. \tag{12.27}$$

Справедливость (12.25) опирается на следующие выкладки.

◀ Точка $z = G(x, a)$ под действием возмущения $G_{\delta a}$ переходит в

$$z + \Delta z = G(z, \delta a) = G(z, 0) + f'_a(z, 0)\delta a + o(\|\delta a\|).$$

При этом [13)]

$$\varphi(a, \delta a) = \varphi(a, 0) + \varphi'(a, 0)\delta a + o(\|\delta a\|),$$

откуда

$$\delta a = \sigma(a)\Delta a + o(\| \ldots \|), \quad \Delta a = \varphi(a, \delta a) - \varphi(a, 0),$$

где $\sigma(a)$ — обратная матрица к $\varphi'(a, 0)$.

[12)] Мы избегаем делить индексы на верхние и нижние, что при более детальном анализе позволяет различать *ковариантные* и *контравариантные* переменные. Но тут ситуация та же, что и с десятипальцевой системой печати, которая хороша при наборе объемных текстов.

[13)] Подразумевается дифференцирование φ' по второму аргументу.

Учитывая $f'_a(z,0)=\xi(z)$, окончательно имеем

$$\Delta z=\xi(z)\sigma(a)\Delta a+o(\ldots). \quad \blacktriangleright \tag{12.28}$$

Разумеется, соблюдая формальности, надо было бы кое-что оговорить. Например, невырожденность матрицы $\varphi'(a,0)$. Но мы часть рутины оставляем за бортом.

Итак, для инвариантности $u(x)$ относительно группы преобразований $\{G(x,a)\}$ теперь требуется больше, чем прежде. Равенство нулю приращения Δu в первом приближении — влечет за собой необходимость обращения в нуль r скалярных произведений градиента ∇u на r касательных векторов:

$$\xi_1(x)=\begin{pmatrix}\xi_{11}\\ \vdots\\ \xi_{n1}\end{pmatrix}, \quad \ldots, \quad \xi_r(x)=\begin{pmatrix}\xi_{1r}\\ \vdots\\ \xi_{nr}\end{pmatrix}, \tag{12.29}$$

т. е.

$$X_j(u)=0, \quad j=1,\ldots,r. \tag{12.30}$$

Зато если интеграл движения $u(x)$ удовлетворяет условиям (12.30), то порядок системы дифференциальных уравнений можно (*иногда*) понизить сразу на r единиц [14)].

Аналогом (12.12) в данном случае является, в силу (12.28), задача Коши для системы дифференциальных уравнений в частных производных вида

$$\frac{\partial z_i}{\partial a_j}=\sum_{k=1}^{r}\xi_{ik}(z)\sigma_{kj}(a), \quad z(0)=x, \tag{12.31}$$

решения которой $z=G(x,a)$ исчерпывают группу $\{G(x,a)\}$.

(!) Формула (12.27) предполагает, что единичным элементом группы является $G(x,0)$. Если единичный элемент группы $G(x,a_0)$,

[14)] В отличие от однопараметрической ситуации, не всегда ясно, как и когда это можно сделать. Положительное решение вопроса зависит от *разрешимости* индуцируемой *алгебры Ли*.

то (12.27) меняется на

$$\xi_{ij}(x) = \left.\frac{\partial G_i(x,a)}{\partial a_j}\right|_{a=a_0}. \tag{12.32}$$

12.5.1. *При чтении литературы надо иметь в виду разнобой в терминологии, удобный с точки зрения свободы маневра. Инфинитезимальными операторами, помимо* (12.26), *называют также*: **(i)** ***линейные комбинации*** (12.26) *и даже* **(ii)** ***любые преобразования*** $G(x,a)$ *из достаточно малой окрестности единичного элемента группы. Кроме того, инфинитезимальные операторы физики называют* ***генераторами группы.***

Примеры

- Группа невырожденных преобразований

$$x' = Ax = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} x$$

имеет единичный элемент при $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. С учетом (12.32) инфинитезимальные операторы, по формуле (12.26):

$$X_1 = x_1\frac{\partial}{\partial x_1}, \quad X_2 = x_2\frac{\partial}{\partial x_1}, \quad X_3 = x_1\frac{\partial}{\partial x_2}, \quad X_4 = x_2\frac{\partial}{\partial x_2}.$$

- При вращении твердого тела вокруг оси x_1 с единичной скоростью точка $x = \{x_1, x_2, x_3\}$ имеет скорость $v = \{0, -x_3, x_2\}$. Скорость изменения любой функции $u(x)$ в этой точке равна

$$-x_3\frac{\partial u}{\partial x_2} + x_2\frac{\partial u}{\partial x_3}.$$

Поэтому инфинитезимальные операторы вращения в $\mathbb{R}^3$:

$$X_1 = x_2\frac{\partial}{\partial x_3} - x_3\frac{\partial}{\partial x_2}, \quad X_2 = x_3\frac{\partial}{\partial x_1} - x_1\frac{\partial}{\partial x_3}, \quad X_3 = x_1\frac{\partial}{\partial x_2} - x_2\frac{\partial}{\partial x_1}, \tag{12.33}$$

что характеризует вращение твердого тела, закрепленного в точке. При освобождении поступательных степеней свободы к (12.33) надо добавить еще три оператора:

$$X_4 = \frac{\partial}{\partial x_1}, \quad X_5 = \frac{\partial}{\partial x_2}, \quad X_6 = \frac{\partial}{\partial x_3}.$$

Соответствующие касательные поля скоростей:

$$\xi_1(x) = (0, -x_3, x_2), \quad \xi_2(x) = (x_3, 0, -x_1), \quad \xi_3(x) = (-x_2, x_1, 0),$$
$$\xi_4(x) = (1, 0, 0), \quad \xi_5(x) = (0, 1, 0), \quad \xi_6(x) = (0, 0, 1).$$

Заметим, аналогом утверждения 12.3.1 является следующее.

12.5.2. *Пусть G — r-параметрическая группа Ли с инфинитезимальными операторами $X_1, \ldots, X_r$ и система уравнений*

$$f_1(x) = 0, \quad \ldots, \quad f_m(x) = 0, \quad x \in \mathbb{R}^n, \quad m \leqslant n, \tag{12.34}$$

такова, что матрица Якоби $\left[\dfrac{\partial f_i}{\partial x_j}\right]$ *имеет ранг m в любом решении системы. Тогда множество решений системы* (12.34) *инвариантно относительно G в том случае, когда*

$$\forall\, i, j:\ X_j(f_i) = 0$$

в любой точке x, удовлетворяющей (12.34).

Вопрос о числе инвариантов r-параметрических групп решается в принципе следующим образом.

12.5.3. *Если группа действует в $\mathbb{R}^n$ и ее орбиты r-мерны, то она имеет $n - r$ глобальных функционально независимых инвариантов* [15].

12.6. Локальные группы

Поскольку переход к рассмотрению инфинитезимальных операторов сохраняет информацию о группе в целом, фокус внимания при обсуждении $\{G(x, a)\}$ можно сузить до малой окрестности единичного элемента $G(x, 0)$, что дает возможность говорить о *локальных группах*.

Такой переход на самом деле принципиален. Дело в том, что есть довольно много практически интересных однопараметрических групп типа

$$x' = \frac{x}{1 - \varepsilon x}, \quad y' = \frac{y}{1 - \varepsilon x}, \tag{12.35}$$

которые могут быть определены лишь локально. Но этого достаточно, чтобы обсуждать инварианты группы.

[15] Для «глобальности» необходимы оговорки, аналогичные тем, которые делались по поводу утверждения 12.2.1.

Локальная группа (12.35) не может быть определена при всех $\varepsilon \in \mathbb{R}$ из-за обращения знаменателей в нуль. Но если $\varepsilon_1, \varepsilon_2$ достаточно малы, то последовательность двух преобразований (12.35) с этими параметрами точку (x, y) переводит в

$$\left(\frac{x}{1-(\varepsilon_1+\varepsilon_2)x}, \frac{y}{1-(\varepsilon_1+\varepsilon_2)x}\right),$$

и на пути анализа не возникает препятствий — при рассмотрении касательного поля (x^2, xy) и *генератора*

$$X = x^2\frac{\partial}{\partial x} + xy\frac{\partial}{\partial y}.$$

Препятствия возникают при рассмотрении диф-уравнения (12.4), имеющего в данном случае вид системы

$$\frac{dx}{d\varepsilon} = x^2, \quad \frac{dy}{d\varepsilon} = xy,$$

решения которой *нелокально непродолжимы* [4, т. 2], что и является причиной обращения в нуль знаменателей (12.35).

Таким образом, локальный характер определения группы не касается «инфинитезимального анализа». Но это только «до поры до времени», пока не возникают «глобальные вопросы», приводящие к необходимости продолжения локальной группы, — и здесь картина и трудности едва ли не идентичны *продолжению аналитических функций* [4, т. 1]. В данном контексте соответствующие подробности остаются за кадром — см. [19, 21].

12.7. Алгебры Ли

Комплект инфинитезимальных операторов в многопараметрическом случае образует, как неожиданно выясняется, так называемую *алгебру Ли*, представляющую собой «инфинитезимальное ядро», несущее на себе всю информацию о группе. Нелинейные условия инвариантности, например, заменяются линейными «инфинитезимальными уравнениями». Но это лежит на поверхности. Обнаруживаются более глубокие механизмы, позволяющие решать неприступные с виду задачи, такие как перечисление и классификация инвариантных групп и диф-уравнений, не говоря об интегрируемости в квадратурах.

Построение алгебры инфинитезимальных операторов начинается с простого наблюдения. Произведение (композиция) дифференциальных операторов

$$X_1 = \sum_{i=1}^{n} \xi_i(x)\frac{\partial}{\partial x_i}, \quad X_2 = \sum_{i=1}^{n} \eta_i(x)\frac{\partial}{\partial x_i} \tag{12.36}$$

является дифференциальным оператором второго порядка, потому что

$$\xi_j(x)\frac{\partial}{\partial x_j}\eta_i(x)\frac{\partial}{\partial x_i} = \xi_j(x)\frac{\partial \eta_i(x)}{\partial x_j}\frac{\partial}{\partial x_i} + \eta_i(x)\xi_j(x)\frac{\partial^2}{\partial x_j \partial x_i}.$$

Но *коммутатор*

$$[X_1, X_2] = X_1X_2 - X_2X_1, \tag{12.37}$$

называемый *скобкой Ли*, будет дифференциальным оператором *первого порядка*, поскольку слагаемые со вторыми производными взаимно уничтожатся [16].

Скобка Ли в результате:

$$[X_1, X_2] = \sum_{i,j=1}^{n} \left[\xi_j \frac{\partial \eta_i}{\partial x_j} - \eta_j \frac{\partial \xi_i}{\partial x_j}\right]\frac{\partial}{\partial x_i}.$$

Соответственно, *коммутатор векторных полей* $\xi(x)$, $\eta(x)$ полагается равным

$$[\xi, \eta] = \left\{\sum_{i}^{n}\left[\xi_1 \frac{\partial \eta_i}{\partial x_1} - \eta_1 \frac{\partial \xi_i}{\partial x_1}\right], \ldots, \sum_{i}^{n}\left[\xi_n \frac{\partial \eta_i}{\partial x_n} - \eta_n \frac{\partial \xi_i}{\partial x_n}\right]\right\}.$$

Коммутатор (12.37) далее служит *билинейной операцией*, лежащей в основе определения *алгебры Ли*, каковой называют векторное пространство L с билинейной операцией умножения $[\cdot, \cdot]$, удовлетворяющей следующим аксиомам:

- *Билинейность*:

$$\alpha[X_1, X_2] = [\alpha X_1, X_2] = [X_1, \alpha X_2], \quad \alpha \in \mathbb{R},$$
$$[X_1, X_2 + X_3] = [X_1, X_2] + [X_1, X_3],$$
$$[X_1 + X_2, X_3] = [X_1, X_3] + [X_2, X_3].$$

[16] Ибо в гладком случае смешанные производные не зависят от порядка дифференцирования [4, т. 1].

- *Антисимметричность*:

$$[X_1, X_2] = -[X_2, X_1].$$

- *Тождество Якоби*:

$$[X_1, [X_2, X_3]] + [X_2, [X_3, X_1]] + [X_3, [X_1, X_2]] = 0. \tag{12.38}$$

Если функции $\xi_j(x)$ гладкие, то множество операторов (12.36) с умножением (12.37) — образует алгебру Ли. Это малоинтересный факт. Интересно другое. Набор инфинитезимальных операторов (12.26) составляет базис *конечномерной* алгебры Ли L_r. При этом любой оператор $X \subset L_r$ раскладывается по базису, и поэтому:

$$[X_\lambda, X_\mu] = \sum_{\nu=1}^{r} c_{\lambda\mu}^{\nu} X_\nu, \quad \lambda, \mu = 1, \ldots, r, \tag{12.39}$$

где $c_{\lambda\mu}^{\nu} \in \mathbb{R}$ — *структурные константы* алгебры L_r.

Результат (12.39) является в некотором роде сюрпризом. Если $[X_\lambda, X_\mu]$ — дифференциальный оператор первого порядка, то почему он обязан представлять собой линейную комбинацию ряда $X_1, \ldots, X_r$ — сразу не ясно. Тем не менее сообразить несложно, и это хорошее упражнение, если мыслить геометрически. Контуры рассуждения примерно такие. С одной стороны, нет особой разницы, говорить об инфинитезимальных операторах, как о преобразованиях $G(x, a)$, близких к единичному оператору группы (см. п. 12.5.1), либо о касательных векторах (12.29), задающих натянутое на них касательное подпространство, аппроксимирующее группу в окрестности единицы. С другой — линейная часть последовательного применения $X_\lambda X_\mu$ обязана (в силу групповых свойств) лежать в том же «натянутом пространстве», и потому будет выражаться как линейная комбинация $X_1, \ldots, X_r$. Формальный эквивалент рассуждения в виде цепочки дифференцирований можно найти у *Хамермеша* [26].

Подстановка (12.39) в *тождество Якоби* (12.38) приводит к соотношениям

$$c_{\lambda\mu}^{\nu} c_{\nu\tau}^{\theta} + c_{\mu\tau}^{\nu} c_{\nu\rho}^{\theta} + c_{\tau\rho}^{\nu} c_{\nu\mu}^{\theta} = 0, \tag{12.40}$$

которые обязаны выполняться наряду с

$$c^{\nu}_{\lambda\mu} = -c^{\nu}_{\mu\lambda}, \tag{12.41}$$

что вытекает из антисимметричности скобки Ли.

Ли показал, что путь к уравнениям (12.40), (12.41) можно пройти в обратном направлении, определяя тем самым по структурным константам *алгебру Ли*, а значит, и *группу Ли*. Иначе говоря, любому решению системы (12.40), (12.41) — отвечает группа Ли, что сводит труднообозримую проблему классификации групп Ли к изучению системы алгебраических уравнений — достаточно сложной, но идеологически прозрачной [17].

На вещественной прямой $\mathbb{R}$ генераторами группы $G(x, a)$ могут быть операторы $\xi_i(x)\dfrac{\partial}{\partial x}$ с линейно независимыми функциями $\xi_i(x)$ — и их линейные комбинации. Разложение функций $\xi(x)$ в ряд по $\{1, x, \ldots, x^n, \ldots\}$ и поиск конечной алгебры с базисом

$$X_1 = \frac{\partial}{\partial x}, \quad X_2 = x\frac{\partial}{\partial x}, \quad \ldots, \quad X_{r+1} = x^r\frac{\partial}{\partial x}$$

показывает, что r не может быть больше двух. Действительно,

$$[X_r, X_{r+1}] = x^{2r-2}\frac{\partial}{\partial x} = X_{2r-1},$$

что противоречит требованию (12.39) в случае $r > 2$.

Таким образом, на вещественной прямой $\mathbb{R}$ возможны лишь три конечномерные алгебры Ли (с точностью до диффеоморфизма):

(i) алгебра с единственным инфинитезимальным оператором $\partial/\partial x$, порождающая группу сдвигов $G(x, a) = x + a$;

(ii) алгебра с двумя генераторами,

$$X_1 = \frac{\partial}{\partial x}, \quad X_2 = x\frac{\partial}{\partial x},$$

порождающая двухпараметрическую группу $G(x, a) = a_1 x + a_2$;

(iii) алгебра с тремя генераторами,

$$X_1 = \frac{\partial}{\partial x}, \quad X_2 = x\frac{\partial}{\partial x}, \quad X_3 = x^2\frac{\partial}{\partial x},$$

[17] Конечно, это слишком сильно сказано. Система (12.40), (12.41) не только сложна, ее надо еще изучать с учетом эквивалентности решений — потому что структурные константы меняются при замене переменных.

порождающая трехпараметрическую группу, эквивалентную проективной группе

$$G(x, a) = \frac{a_1 x + a_2}{a_3 x + 1}.$$

Рассуждение, конечно, содержит пробелы, но результат именно таков. На вещественной прямой возможны, максимум, *трехпараметрические* группы Ли, причем их всего три (с точностью до эквивалентности). *Ли* в анализе продвинулся дальше, но уже на плоскости технические детали настолько громоздки, что книги, в которых воспроизводятся соответствующие результаты, можно пересчитать на пальцах. Возможных групп оказалось более 30 типов, среди них примитивные, максимум, восьмипараметрические, импримитивные — любой размерности.

12.8. Дифференциальные уравнения

Приложения групп Ли к дифференциальным уравнениям связаны в основном с простым соображением. Если дифур инвариантен к некоторой группе преобразований, то интегралы движения надо искать в классе функций, инвариантных относительно той же группы. «Соображение» просто выглядит, конечно, пока не доходит до дела, потому что в конкретных задачах возникают неясности, о чем можно судить хотя бы по примерам из главы 1.

> Однако именно «примитивный подход» лежит в основе большинства практических успехов, и это полезно было бы признать, не прикрываясь разговорами о роли высокой науки. Роль последней несомненна, но *путь к решению* всегда обнаруживается «на пальцах». Потом на обоснование иногда уходит вся жизнь, но это второй этап. Открытия любого калибра избегают «причесанных методов». Хорошая находка — всегда результат озарения, игнорирующего строгие правила.

Весь этот разговор к тому, что для успешного применения групповой идеологии к диф-уравнениям — совсем необязательно начинать с изучения теории групп Ли, особенно в современном изложении [21]. Более того, наивный подход (глава 1) даже лучше, ибо раскрепощает и вдохновляет. Систематический взгляд потребуется на этапе доработки, и то не факт. Однако заранее полезно иметь *общее представление* о сфере поисков, возможных трудностях и простейших инструментах.

• Вот внешне простая ситуация. Дифференциальное уравнение

$$t\frac{dx}{dt} = x + \sqrt{x^2 + t^2}, \tag{12.42}$$

как легко убедиться, имеет частное решение

$$x = \frac{1}{2}(t^2 - 1), \tag{12.43}$$

инвариантно относительно группы растяжений $\{Cx, Ct\}$, и подстановка в (12.43) $\{Cx, Ct\}$ вместо $\{x, t\}$ приводит к общему решению (12.42):

$$x = \frac{1}{2}\left(Ct^2 - \frac{1}{C}\right).$$

• Трюк довольно симпатичный. Из одного решения получаются сразу все. Но идея размножения решений с помощью группового воздействия не всегда работает. Скажем, уравнение Риккати

$$\dot{x} + x^2 = \frac{2}{t^2}, \tag{12.44}$$

инвариантное относительно группы растяжений

$$\left\{Cx, \frac{1}{C}t\right\}, \tag{12.45}$$

имеет общее решение

$$x = \frac{3t^2}{t^3 + C} - \frac{1}{t}, \tag{12.46}$$

которое не может быть получено групповым воздействием ни из частного решения $x = -1/t$, ни из $x = 2/t$. Однако (12.46) получается из решения

$$x = \frac{3t^2}{t^3 + 1} - \frac{1}{t}$$

подстановкой $x \mapsto Cx$, $t \mapsto \frac{1}{C}t$ с последующей заменой константы $C^3 \mapsto C$.

Причина вскрывается при рассмотрении первых интегралов. Инвариантами группы (12.45) служат кривые $xt = k$, среди которых лишь две,

$$xt = 2, \quad xt = -1,$$

переводятся группой (12.45) сами в себя [18]. Именно они и не подходят для целей «размножения». В любом другом частном решении действие группы $x \mapsto Cx$, $t \mapsto \frac{1}{C}t$ сдвигает константу, и механизм работает.

[18] Что проверяется подстановкой $xt = k$ в (12.44).

Предыдущие примеры указывают путь, но он далеко не всегда ведет к цели. Общее решение вообще не обязано получаться из конечного числа — частных.

Считается, что система дифференциальных уравнений

$$\dot{x} = \Phi(x, t), \quad x \in \mathbb{R}^n, \tag{12.47}$$

имеет *фундаментальную систему решений*, если общее решение функционально выражается через конечное число m произвольно выбранных частных решений и n произвольных констант. За пределами линейного случая, в котором фундаментальная система решений существует всегда [4, т. 2], вопрос не так прост.

12.8.1. Теорема (Ли). *Система* (12.47) *имеет фундаментальную систему решений, если она представима в виде*

$$\dot{x}_i = \nu_1(t)\xi_{i1}(x) + \ldots + \nu_r(t)\xi_{ir}(x), \quad i = 1, \ldots, n,$$

и операторы

$$X_j = \sum_{i=1}^{n} \xi_{ij}(x)\frac{\partial}{\partial x_i}, \quad j = 1, \ldots, r,$$

образуют алгебру Ли. При этом $m \geqslant r/n$.

Стандартный пример нелинейного уравнения с фундаментальной системой решений — *уравнение Риккати*:

$$\dot{x} = \alpha(t) + \beta(t)x + \gamma(t)x^2,$$

для которого алгебру Ли образуют операторы

$$X_1 = \frac{d}{dx}, \quad X_2 = x\frac{d}{dx}, \quad X_3 = x^2\frac{d}{dx}.$$

Теорема 12.8.1, конечно, — флаг. Практически — результат малополезный, но «философски» — крайне важный. Математика вообще держится на опорных столбах, которые чисто утилитарного значения почти не имеют. Но как фундамент, обозначение горизонтов, демонстрация перспектив, — эти столбы опосредованно влияют на все остальное.

Что касается непосредственно практики, внимание традиционно концентрируется на интегрировании конкретных дифференциальных уравнений. И хотя оное ремесло — далеко не ядро теории (см. [4, т. 2]), им полезно владеть.

К примерам и приемам из главы 1 здесь полезно добавить некоторые общие соображения, которые отчасти развязывают глаза. Это не всегда превращает поиск вслепую в более эффективное занятие, но в целом — дает понимание, которое часто оказывается дороже отдельно решенной задачи.

В первую очередь надо сказать о целесообразности использования *инфинитезимальных операторов*. Если функция $u(x, y)$ инвариантна относительно группы преобразований

$$x' = ax, \quad y' = \frac{1}{a}y,$$

то использование *генератора группы*

$$X = x\frac{\partial}{\partial x} - y\frac{\partial}{\partial y}$$

особых выгод обычно не сулит.

Если же $u(x, y)$ инвариантна относительно *группы вращений*

$$\begin{cases} x' = x\cos\varphi - y\sin\varphi, \\ y' = x\sin\varphi + y\cos\varphi, \end{cases}$$

то сама проверка инвариантности с помощью инфинитезимального оператора

$$X = -y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}$$

бывает намного проще.

Интегрирующий множитель. Дифференциальные уравнения на плоскости

$$\frac{dy}{dx} = f(x, y)$$

часто записывают в форме $dy - f(x, y)\,dx = 0$. Рассматривают также более общий случай

$$P(x, y)\,dx + Q(x, y)\,dy = 0, \tag{12.48}$$

равносильный уравнению в частных производных [19)]

$$Q\frac{\partial u}{\partial x} - P\frac{\partial u}{\partial y} = 0. \tag{12.49}$$

[19)] См. раздел 12.2 о *первых интегралах*.

Если левая часть (12.48) представляет собой дифференциал некоторой функции (потенциала) $u(x, y)$, т. е. $du = P\,dx + Q\,dy$, что означает

$$\frac{\partial u}{\partial x} = P(x, y), \quad \frac{\partial u}{\partial y} = Q(x, y), \tag{12.50}$$

то это сразу дает первый интеграл $u(x, y) = c$, и тем самым решает исходное уравнение.

Из равенства перекрестных производных $u(x, y)$ вытекает, в силу (12.50),

$$\frac{\partial P(x, y)}{\partial y} = \frac{\partial Q(x, y)}{\partial x}, \tag{12.51}$$

что служит достаточным условием существования потенциала $u(x, y)$.

Поскольку умножение (12.48) на ненулевой множитель $\mu(x, y)$ не меняет уравнения по сути, — потенциал u существует и в том случае, когда условию типа (12.51) удовлетворяет уравнение

$$\mu(x, y)P(x, y)\,dx + \mu(x, y)Q(x, y)\,dy = 0.$$

Тогда $\mu(x, y)$ называют *интегрирующим множителем*, и u определяют, интегрируя $du = \mu P\,dx + \mu Q\,dy$, а μ предварительно находят, решая уравнение с частными производными

$$\frac{\partial \mu P}{\partial y} = \frac{\partial \mu Q}{\partial x},$$

что в общем случае не менее сложно, чем решение исходного уравнения.

Но если уравнение (12.48) *допускает* группу преобразований [20] с инфинитезимальным оператором

$$X = \xi(x, y)\frac{\partial}{\partial x} + \eta(x, y)\frac{\partial}{\partial y},$$

то любой интеграл $u(x, y) = C$ уравнения (12.48) под действием группы остается интегралом. Поэтому любое решение (12.49) $u(x, y)$ дает другое решение $X(u)$ того же уравнения. Но решение у (12.49), с точностью до функциональной зависимости, может быть только одно. Следовательно, $X(u) = \varphi(u)$, т. е.

$$\xi\frac{\partial u}{\partial x} + \eta\frac{\partial u}{\partial y} = \varphi(u), \tag{12.52}$$

где φ — некоторая функция.

Решая систему (12.49), (12.52) относительно производных, получаем

$$\frac{\partial u}{\partial x} = \frac{\varphi P}{\xi P + \eta Q}, \quad \frac{\partial u}{\partial y} = \frac{\varphi Q}{\xi P + \eta Q}.$$

[20] Уравнение *допускает* группу преобразований, если оно инвариантно относительно этой группы.

В итоге

$$\frac{du}{\varphi(u)} = \frac{Pdx + Qdy}{\xi P + \eta Q},$$

откуда вытекает[21], что искомый *интегрирующий множитель*:

$$\mu = \frac{1}{\xi P + \eta Q}.$$

12.9. Инфинитезимальные продолжения

При изучении дифференциальных уравнений $f(\dot{x}, x, t) = 0$ (либо более высокого порядка) с точки зрения инвариантности — часто имеет смысл на первичном этапе исследования рассматривать дифур $f(\dot{x}, x, t) = 0$ как сугубо статическое уравнение, забыв на время, что $\dot{x}$ производная. Взаимосвязь задач сохраняется иначе: *продолжением* действия изучаемой группы G на переменные $\dot{x}$.

Делается это следующим образом. Пусть элементы группы $G = \{G_a\}$ действуют по правилу

$$y = \Phi(x, t, a), \quad \tau = \Psi(x, t, a). \tag{12.53}$$

Тогда

$$\dot{y} = \frac{dy}{d\tau} = \frac{\Phi_t + \dot{x}\Phi_x}{\Psi_t + \dot{x}\Psi_x} = \Theta(\dot{x}, x, t), \tag{12.54}$$

что в совокупности с (12.53) дает описание *продолженной группы* G^{*1}, действующей в расширенном пространстве переменных $\{\dot{x}, x, t\}$.

При необходимости группу можно продолжать на производные более высоких порядков. Например,

$$\ddot{y} = \frac{d\dot{y}}{d\tau} = \frac{\Theta_t + \dot{x}\Theta_x + \ddot{x}\Theta_{\dot{x}}}{\Psi_t + \dot{x}\Psi_x}, \tag{12.55}$$

что, будучи добавлено к (12.53) и (12.54), дает *продолженную группу* G^{*2}, действующую в пространстве переменных $\{\ddot{x}, \dot{x}, x, t\}$.

Все это, конечно, выглядит упражнением на дифференцирование, и трудно поверить, что где-то может дать выигрыш. Но ситуация кардинально меняется при переходе к инфинитезимальным

[21] Ибо $\dfrac{du}{\varphi(u)}$ — полный дифференциал.

операторам. Ничего существенно нового, вообще говоря, не появляется, но итоговые формулы еще дальше отдаляются от исходного описания группы, и «удобства» становятся принципиальны.

Если

$$X = \xi\frac{\partial}{\partial t} + \eta\frac{\partial}{\partial x},$$

то каков инфинитезимальный оператор продолженной группы? Идеологически ответ прост, но технически громоздок, и выкладки проделываются в общем виде один раз, чтобы не возиться с каждой задачей отдельно. При этом уравнения (12.53) надо заменить на $y = x + a\eta + o(a)$, $\tau = t + a\xi + o(a)$ и перейти к формулам типа (12.54), (12.55) с точностью до о-малых, получая в результате

$$\dot{y} = \dot{x} + a\omega_1, \quad \ddot{y} = \ddot{x} + a\omega_2,$$

где

$$\omega_1 = D(\eta) - \dot{x}D(\xi), \quad \omega_2 = D(\omega_1) - \ddot{x}D(\xi),$$

что записано с помощью так называемого *оператора полного дифференцирования*

$$D = \frac{\partial}{\partial t} + \dot{x}\frac{\partial}{\partial x} + \ddot{x}\frac{\partial}{\partial \dot{x}} \dots .$$

В результате *инфинитезимальный оператор первого продолжения*

$$X^{*1} = X + \omega_1\frac{\partial}{\partial \dot{x}} = \xi\frac{\partial}{\partial t} + \eta\frac{\partial}{\partial x} + \omega_1\frac{\partial}{\partial \dot{x}},$$

второго продолжения

$$X^{*2} = X^{*1} + \omega_2\frac{\partial}{\partial \dot{x}}.$$

Пример

Для оператора $X = -y\dfrac{\partial}{\partial x} + x\dfrac{\partial}{\partial y}$ группы вращений:

$$X^{*1} = -y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y} + (1 + y_x^2)\frac{\partial}{\partial y_x}.$$

12.10. Поиск допускаемых групп

Под «*допускаемыми группами*» здесь подразумеваются группы, относительно которых инвариантны изучаемые уравнения.

Указанию допускаемой группы способствует обычно понимание содержательной стороны задачи. Физические соображения,

равноправие переменных, та или иная «геометрическая» симметрия — именно такого сорта факторы чаще всего помогают обнаружить искомую группу. Более логичная задача «по уравнению найти группу формальными средствами» — вызывает обычно меньше энтузиазма из-за технических препятствий, но принципиально она решаема.

Если изучается уравнение

$$f(\dot{x}, x, t) = 0, \tag{12.56}$$

то для инвариантности (12.56) относительно группы с инфинитезимальным оператором X требуется (необходимо и достаточно):

$$X^{*1} f = 0 \quad \text{при условии} \quad f(y, x, t) = 0, \tag{12.57}$$

где y стоит вместо производной $\dot{x}$. При этом (12.57) называют *определяющим уравнением* для допускаемой группы уравнения (12.56).

Если бы речь шла об уравнении второго порядка $f(\ddot{x}, x, t) = 0$, то вместо (12.57) требовалось бы

$$X^{*2} f = 0 \quad \text{при условии} \quad f(z, x, t) = 0.$$

И так далее — для уравнений более высокого порядка.

Определяющие уравнения типа (12.57) оказываются в итоге системами уравнений в частных производных, решение которых (позволяющее указать допускаемую группу), как правило, сложнее исходного дифура. Поэтому овчинка не стоит выделки, если задача упирается только в решение дифференциального уравнения. Однако знание инвариантной группы обычно дает больше, позволяя судить о различных свойствах изучаемого объекта, что гораздо важнее стерильного решения. Такого рода соображения подталкивают к анализу определяющих уравнений и приводят (иногда) к конструктивным результатам [18, 19].

12.11. ЧП-уравнения

Продолжение *групп Ли* в расчете на изучение уравнений в частных производных находится в том же идеологическом русле. Переменные делятся на зависимые $u = \{u_1, \ldots, u_m\}$ и независимые

$x = \{x_1, \ldots, x_n\}$. Описание группы внешне прежнее:

$$u = \Phi(u, x, a), \quad x = \Psi(u, x, a),$$

где x теперь играет роль «многомерного времени». Группы продолжаются на переменные

$$p_{ij} = \frac{\partial u_i}{\partial x_j}, \quad p_{ijk} = \frac{\partial^2 u_i}{\partial x_j \partial x_k} \quad \text{и т. д.}$$

При определенных соглашениях относительно обозначений формулы (продолженных операторов и определяющих уравнений) совпадают с предыдущими.

Тут, конечно, хорошо было бы привести примеры, но регламент поджимает. К тому же ситуация аналогична «алкоголю за рулем». Много пить нельзя, мало — неинтересно. Поэтому здесь лучше обратиться к обстоятельным источникам [18, 19]. В элементарном изложении примеры есть в [10].

12.12. Комментарии

• **Откуда берутся сложности.** О трудностях систематического изучения *групп Ли* нетрудно догадаться. Источников «неприятностей» довольно много. Серьезную головную боль доставляют вопросы продолжения локальных групп. Как уже отмечалось, картина здесь напоминает *теорию аналитических функций*. Во многих практически интересных случаях продолжение локальной группы оказывается многозначным (типа продолжения логарифма на комплексной плоскости). В ТФКП положение спасают римановы поверхности, на которых многозначные функции становятся однозначными, — но инструмент не из простых. Подобную технику приходится вводить и здесь, что в рядовых ситуациях приводит к стрельбе из пушек по воробьям. Конечно, можно дать упрощенный вариант теории, но его приходится то и дело расширять и подстраивать. Общий же подход рождает монстров. Простые исходные понятия постепенно рассыпаются, и неожиданно выясняется, что изучается-то по сути симбиоз теории групп с теорией гладких многообразий. При этом не скажешь, что хуже: алгебраические головоломки или топологические ловушки.

• Центральным мотивом деятельности *Ли* и образцом для подражания служила *теория Галуа* алгебраических уравнений. Аналогом «разрешимости в радикалах» была интегрируемость дифференциальных уравнений в квадратурах. Успех, вообще говоря, не был достигнут, и через некоторое время тематика была оставлена

в покое, хотя результатов было получено много (*Ли* и его ближайшими последователями). В частности, было выяснено, что *система дифференциальных уравнений n-го порядка с транзитивной группой Ли и разрешимой алгеброй Ли — интегрируема в квадратурах, а если множества транзитивности m-мерны, то порядок системы квадратурами может быть снижен до $(n-m)$-го.* Но это еще не теория Галуа. Система может оказаться интегрируемой, даже если она не инвариантна относительно хоть какой-нибудь группы Ли [22].

• Векторное поле $\xi(x)$ в $\mathbb{R}^n$ (либо на многообразии $M \subset \mathbb{R}^n$) в естественных предположениях для любой точки определяет кривую (траекторию), проходящую через эту точку и всюду касающуюся поля $\xi(x)$. В случае системы векторных полей

$$\xi_j(x) = \{\xi_{1j}(x), \ldots, \xi_{nj}(x)\}, \quad j = 1, \ldots, r,$$

вместо траекторий говорят об *интегральных многообразиях* полей $\{\xi_1, \ldots, \xi_r\}$, касательные пространства которых в каждой точке x порождаются векторами $\{\xi_1(x), \ldots, \xi_r(x)\}$. При этом система $\{\xi_1(x), \ldots, \xi_r(x)\}$ считается *интегрируемой*, если через каждую точку x проходит интегральное многообразие.

О системе $\{\xi_1(x), \ldots, \xi_r(x)\}$ говорят как о *находящейся в инволюции*, если существуют гладкие функции $c^{\nu}_{\lambda\mu}(x)$, такие что

$$[\xi_\lambda, \xi_\mu] = \sum_{\nu=1}^{r} c^{\nu}_{\lambda\mu}(x)\xi_\nu, \quad \lambda, \mu = 1, \ldots, r,$$

см. (12.39).

Теорема Фробениуса. *Система гладких векторных полей*

$$\{\xi_1(x), \ldots, \xi_r(x)\}$$

интегрируема в томм случае, если она находится в инволюции [23].

• Определенный интерес представляет взаимосвязь коммутатора (*скобки Ли*)

$$[A, B] = AB - BA,$$

где под A, B можно понимать матрицы, с *групповым коммутатором*

$$[A, B]^* = ABA^{-1}B^{-1}.$$

Взаимосвязь определяется равенством

$$[A, B] = \frac{\partial^2}{\partial s \partial t}\left[e^{As}, e^{Bt}\right]^*\Big|_{s=t=0},$$

которое проверяется простым дифференцированием.

---

[22] Современный вариант теории Галуа для дифференциальных уравнений см. в книге: *Pommaret J. F.* Differential Galois Theory. New York, 1983.

[23] Исторические и технические подробности см. в [19].

Сокращения и обозначения

◄ и ► — начало и конец рассуждения, темы, доказательства.

(?) — предлагает проверить или доказать утверждение в качестве упражнения, либо довести рассуждение до «логической точки», — но не является вопросом «правильно или неправильно?»

(!) — предлагает обратить внимание

«в томм случае» — «в том и только том случае»

НОД — наибольший общий делитель

НОК — наименьшее общее кратное

ЧП-уравнение — уравнение с частными производными

$A \Rightarrow B$ — из A следует B

$x \in X$ — x принадлежит X

$X \cup Y$, $X \cap Y$, $X \setminus Y$ — объединение, пересечение и разность множеств

$X \subset Y$ — X подмножество Y, в том числе имеется в виду возможность $X \subseteq Y$, т. е. между $X \subset Y$ и $X \subseteq Y$ различия не делается

$\mathbb{N}$ — множество натуральных чисел $\{1, 2, \ldots\}$

$\mathbb{Z}$ — множество целых чисел $\{\ldots, -1, 0, 1, \ldots\}$

$\mathbb{Q}$ — множество рациональных чисел

$\mathbb{R} = (-\infty, \infty)$ — вещественная прямая

$\mathbb{C}$ — комплексная плоскость

$x = a \pmod{p}$ — «x при делении на p дает в остатке a»

$\mathrm{Aut}\, G$ — группа автоморфизмов группы G

C_n — группа поворотов на углы $\dfrac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$

D_n — группа диэдра, изоморфна *группе самосовмещений* правильного n-угольника

$\mathbf{S}_n$ — симметрическая группа подстановок n-й степени

$\mathbf{A}_n$ — знакопеременная группа подстановок

$a \mapsto b$ — отображение, сопоставляющее элементам a элементы b

$\langle a_1, \ldots, a_n \rangle$ — группа с образующими $a_1, \ldots, a_n$

$\langle x, y \rangle$ — скалярное произведение векторов x, y; различие с предыдущим обозначением определяется контекстом

$\langle S \rangle$ — группа порожденная множеством S

$*$, $\otimes$, $\circ$ — знаки для обозначения групповой операции (группового умножения)

$\ker \varphi$ — ядро гомоморфизма φ

$k(\alpha)$ — наименьшее расширение поля k, содержащее элемент α

$[F : P]$ — степень расширения F над полем P

$|G : H|$ — индекс подгруппы H в группе G

Литература

1. *Биркгоф Г.* Гидродинамика. М.: ИЛ, 1963.
2. *Боревич З. И., Шафаревич И. Р.* Теория чисел. М.: Наука, 1972.
3. *Босс В.* Интуиция и математика. М.: Айрис-Пресс, 2003. 2-е изд. М.: КомКнига/URSS, 2007.
4. *Босс В.* Лекции по математике. Т. 1. Анализ; Т. 2. Дифференциальные уравнения; Т. 3. Линейная алгебра; Т. 4. Вероятность, информация, статистика; Т. 5. Функциональный анализ; Т. 6. От Диофанта до Тьюринга; Т. 7. Оптимизация. М.: URSS, 2004–2006.
5. *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1979.
6. *Вейль Г.* Симметрия. М.: УРСС, 2002.
7. *Винберг Э. Б.* Линейные представления групп. М.: Наука, 1985.
8. *Журавлев Ю. И., Флеров Ю. А., Вялый М. Н.* Дискретный анализ. Основы высшей алгебры. М.: МЗ-Пресс, 2006.
9. *Ибрагимов Н. Х.* Группы преобразований в математической физике. М.: Наука, 1983.
10. *Ибрагимов Н. Х.* Азбука группового анализа. М.: Знание, 1989.
11. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1972.
12. *Картан Э.* Теория конечных непрерывных групп и дифференциальная геометрия, изложенные методом подвижного репера. М.: МГУ, 1963.
13. *Коксетер Г. С. М., Мозер У. О. Дж.* Порождающие элементы и определяющие соотношения. М.: Наука, 1980.
14. *Кострикин А. И.* Введение в алгебру. Ч. III. Основные структуры. М.: Физматлит, 2001.
15. *Курош А. Г.* Курс высшей алгебры. М.: Лань, 2004.
16. *Курош А. Г.* Теория групп. М.: Лань, 2005.
17. *Ленг С.* Алгебра. М.: Мир, 1968.
18. *Овсянников Л. В.* Групповой анализ дифференциальных уравнений. М.: Наука, 1993.
19. *Олвер П.* Приложения групп Ли к дифференциальным уравнениям. М.: Мир, 1989.
20. *Ольшанский А. Ю.* Геометрия определяющих соотношений в группах. М.: Наука, 1989.

21. *Понтрягин Л. С.* Непрерывные группы. М.: УРСС, 2004.
22. *Постников М. М.* Введение в теорию алгебраических чисел. М.: Наука, 1982.
23. *Постников М. М.* Основы теории Галуа. М.: Наука, 1960.
24. *Прасолов В. В.* Многочлены. М.: МЦНМО, 2000.
25. *Седов Л. И.* Методы подобия и размерности в механике. М.: Наука, 1967.
26. *Хамермеш М.* Теория групп и ее применение к физическим проблемам. М.: УРСС, 2002.
27. *Шевалле К.* Теория групп Ли. М.: ИЛ, 1948.
28. *Яглом И. М.* Геометрические преобразования. Т. 1, 2. М.: Гостехиздат, 1955, 1956.

Предметный указатель

В проекте издания «Лекций по математике» В. Босса вышли тома:

1. Анализ. 2. Дифференциальные уравнения. 3. Линейная алгебра. 4. Вероятность, информация, статистика. 5. Функциональный анализ. 6. От Диофанта до Тьюринга. 7. Оптимизация. 8. Теория групп.

Готовятся к изданию:

9. ТФКП. 10. Труднорешаемые задачи.

В условиях информационного наводнения инструменты вчерашнего дня перестают работать.
Поэтому учить надо как-то иначе.
«Лекции» дают пример.
Плохой ли, хороший – покажет время.
Но в любом случае, это продукт нового поколения.
Те же «колеса», тот же «руль», та же математическая суть, – но по-другому.

В. Босс

Из отзывов читателей:

Чтобы усвоить предмет, надо освободить его от деталей, обнажить центральные конструкции, понять, как до теорем можно было додуматься. Это тяжелая работа, на которую не всегда хватает сил и времени. В «Лекциях» такая работа проделывается автором.

Популярность книг В. Босса легко объяснима. Дается то, чего недостает: общая картина, мотивация, взаимосвязи. И самое главное — легкость вхождения в любую тему.

Содержание продумано и хорошо увязано. Громоздкие доказательства ужаты до нескольких строчек. Виртуозное владение языком.

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА

E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (495) 135–42–16
URSS Тел./факс: 7 (495) 135–42–46

4673 ID 50795

9 785484 009411 >

Отзывы о настоящем издании, а также обнаруженные опечатки присылайте по адресу **URSS@URSS.ru**. Ваши замечания и предложения будут учтены и отражены на web-странице этой книги в нашем интернет-магазине **http://URSS.ru**