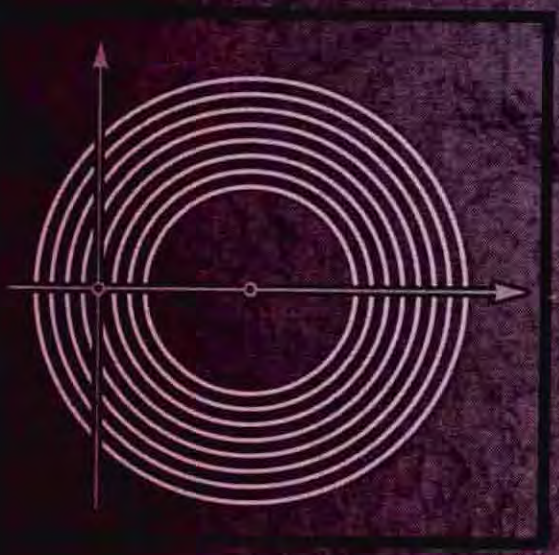
Л. С. Понтрягин

ОБОБЩЕНИЯ ЧИСЕЛ



УРСС

Л. С. Понтрягин

ОБОБЩЕНИЯ ЧИСЕЛ

Издание второе, исправленное

Москва • 2003

УРСС

Понтрягин Лев Семенович

Обобщения чисел. Изд. 2-е, испр. — М.: Едиториал УРСС, 2003. — 224 с.

ISBN 5-354-00259-1

В книге представлен популярный рассказ о возможных обобщениях понятия числа. Сначала подробно рассмотрены обобщения действительных чисел, именно комплексные числа и кватернионы. Доказано, что других логически возможных величин, аналогичных действительным и комплексным числам и пригодных к употреблению в математике в роли чисел, кроме действительных и комплексных чисел, не существует. Затем рассматриваются другие обобщения понятия числа, уже не содержащие действительных чисел.

Издательство «Едиториал УРСС». 117312, г. Москва, пр-т 60-летия Октября, 9.
Лицензия ИД № 05175 от 25.06.2001 г. Подписано к печати 23.06.2003 г.
Формат 60×90/16. Тираж 2000 экз. Печ. л. 14. Зак. № 3-988/214.

Отпечатано в типографии ООО «Рохос». 117312, г. Москва, пр-т 60-летия Октября, 9.

ИЗДАТЕЛЬСТВО УРСС
НАУЧНОЙ И УЧЕБНОЙ ЛИТЕРАТУРЫ
E-mail: URSS@URSS.ru
Каталог изданий
в *Internet*: http://URSS.ru
Тел./факс: 7 (095) 135-44-23
Тел./факс: 7 (095) 135-42-46

ISBN 5-354-00259-1

Оглавление

Предисловие 5

Глава 1. Комплексные числа 9

§ 1. Историческая справка 11

§ 2. Определение комплексных чисел 13

§ 3. Геометрическое изображение комплексных чисел . 16

Глава 2. Основная теорема алгебры 25

§ 4. Пути в плоскости комплексного переменного 28

§ 5. Комплексные функции комплексного переменного . 37

Глава 3. Алгоритм Евклида 43

§ 6. Деление многочленов 45

§ 7. Разложение многочлена на множители 49

§ 8. Общий наибольший делитель двух многочленов . . . 55

§ 9. Устранение кратных корней 59

§ 10. Подсчет числа действительных корней многочлена на заданном отрезке 63

Глава 4. Кватернионы **69**

§ 11. Векторные пространства 71

§ 12. Евклидово векторное пространство 85

§ 13. Кватернионы 99

§ 14. Геометрические применения кватернионов 106

Глава 5. Другие обобщения чисел **127**

§ 15. Алгебраические тела и поля 129

§ 16. Поле вычетов по простому модулю p 137

§ 17. Теорема Фробениуса 145

Глава 6. Тополого-алгебраические тела **159**

§ 18. Топологическое тело 164

§ 19. Топологические понятия в топологическом теле L . 173

§ 20. Теорема единственности 183

§ 21. p-адические числа 187

§ 22. Некоторые топологические свойства поля K_0^p p-адических чисел 203

§ 23. Поле рядов над полем вычетов 209

§ 24. О структуре несвязных локально компактных топологических тел 218

Об авторе **221**

Предисловие

Понятие числа складывалось в математике постепенно в результате длительного развития, которое шло под воздействием практики и внутренних потребностей математики. Так, в конце концов, сформировалось понятие действительного числа, которое в данной книге предполагается известным.

На этом, однако, развитие понятия числа не остановилось. Внутренние потребности математики привели к комплексным числам. Возникшая на их основе теория функций комплексного переменного имеет теперь большие практические применения. Комплексным числам в книге отведено много места. Доказана основная теорема алгебры о том, что многочлен имеет хотя бы один действительный или комплексный корень. Возникающее из этой теоремы разложение многочлена на линейные множители тщательно изучено. При этом в качестве вспомогательного аппарата в книге используется деление многочленов друг на друга и алгоритм Евклида.

Поскольку комплексные числа оказались очень важными и полезными в математике, возникла чисто обобщательская попытка развивать понятие числа в том же направлении. Так возникли кватернионы, но лишь в результате отказа от коммутативности умножения. Благодаря отсутствию коммутативности

умножения оказалось невозможным построить теорию функций кватернионного переменного. Таким образом, применение кватернионов в математике оказалось очень незначительным. При помощи кватернионов хорошо описываются вращения трехмерного и четырехмерного евклидовых пространств. Конечно, это по своему значению не может идти ни в какое сравнение с применением комплексных чисел. В книге дается описание кватернионов и их применения их к изучению вращений трехмерного и четырехмерного евклидовых пространств. Этот раздел книги завершается доказательством теоремы Фробениуса, утверждающей, что дальнейшее развитие понятия числа в направлении кватернионов невозможно.

Переход от рациональных чисел к действительным числам вызван скорее внутренней логикой развития математики, чем практическими потребностями, так как при помощи рациональных чисел с любой точностью можно осуществить любое измерение. К действительным числам привело математическое открытие, возникающее из теоремы Пифагора и состоящее в том, что длина диагонали квадрата со стороной, равной единице, не может быть измерена точно рациональным числом. Действительные числа как бы заполняют промежутки между рациональными числами и приводят к тому, что условие сходимости Коши является не только необходимым, но и достаточным условием сходимости. Этот факт чрезвычайно важен в математике. Действительные числа представляют собой ту непрерывную среду, в которую помещены рациональные числа. Здесь становится совершенно ясным, что для чисел характерно не только наличие действий сложения, вычитания, умножения и деления, но также и понятие предельного перехода, т. е. известно, что означает последовательность чисел, сходящаяся к данному числу.

Совокупность величин, в которой имеются алгебраические операции сложения, вычитания, умножения и деления, а также определен предельный переход, является естественным логически возможным обобщением понятия числа. Оказывается, что таких обобщений вовсе не очень много. Именно их описанию в основном посвящена эта книга.

Переход от рациональных чисел к действительным опирается на представление о том, что́ такое малое рациональное число. Оказывается, что, кроме совершенно естественного понятия малости рационального числа, существует другое, связанное с некоторым простым числом p. Связанное с этим понятием малости расширение рациональных чисел приводит к возникновению p-адических чисел, которые имеют в настоящее время важное применение в теории чисел и описаны в книге.

Величинами, для которых возможны алгебраические операции, являются так называемые вычеты по простому модулю p. Рациональные функции некоторой величины t, где коэффициентами служат вычеты по модулю p, образуют систему величин, в которой возможны операции сложения, вычитания, умножения и деления, а также естественно возникает понятие малости. Дополняя эту систему рациональных функций таким образом, чтобы вновь полученная система величин была с точки зрения предельного перехода полной, т. е. чтобы условие Коши являлось необходимым и достаточным условием сходимости, мы приходим к изучению бесконечных рядов относительно величины t. Это еще одна система величин, в которой возможны алгебраические операции и предельный переход. В конце книги формулируется теорема Ковальского, описывающая до некоторой степени любую систему величин, в которой имеются алгебраические операции и предельный переход.

Книга посвящена описанию таких систем величин с алгебраическими операциями и предельным переходом, которые являются логически возможными обобщениями чисел. Налагая на эту систему величин некоторые очень простые и естественные ограничения, мы приходим к результату, что никаких других логических возможностей для построения приемлемых в математике величин, аналогичных действительным и комплексным числам, кроме действительных и комплексных чисел, не существует. Это показывает, что действительные и комплексные числа сложились в математике не в результате случайного процесса исторического развития, а как единственные логически возможные величины, удовлетворяющие тем требованиям, которые естественно предъявить к числам.

В заключение я выражаю благодарность С. М. Асееву за большую помощь при редактировании этой книги.

Глава 1

Комплексные числа

§ 1. Историческая справка 11
§ 2. Определение комплексных чисел 13
§ 3. Геометрическое изображение комплексных чисел 16

Здесь я прежде всего очень кратко рассказываю о том, как возникли в математике и постепенно утвердились в ней комплексные числа. Затем даю определение комплексных чисел, действий над ними и их геометрическую интерпретацию. Попутно доказываются формулы косинуса и синуса суммы, тесно связанные с умножением комплексных чисел.

§ 1. Историческая справка

Из курса математики известно, что отрицательные числа введены прежде всего для того, чтобы операция вычитания, обратная к операции сложения, была всегда возможна. По аналогичной причине в математике появились комплексные числа. Если рассматривать только действительные числа, то операция извлечения квадратного корня, обратная к операции возведения в квадрат, не всегда возможна, так как нельзя извлечь квадратный корень из отрицательного числа. Этого, однако, недостаточно, чтобы заводить в математике новые числа. Оказалось, что

Джироламо Кардано (1501–1576)

если производить вычисления по обычным правилам над выражениями, в которых встречается корень квадратный из отрицательного числа, то можно прийти к результату, уже не содержащему корень квадратный из отрицательного числа. В XVI веке Кардано нашел формулу для решения кубического уравнения (Квант, 1976, № 9, с. 2). Оказалось, что именно в том случае, когда кубическое уравнение имеет три действительных корня, в формуле Кардано встречается корень квадратный из отрицательного числа (там же, с. 11). Обнаружилось таким образом, что, производя вычисления с выражениями, содержащими корень квадратный из отрицательного числа, можно получить вполне понятные результаты. Поэтому эти корни стали употреблять в математике. Назвали их мнимыми числами, и тем самым они как бы приобрели право на нелегальное существование. Полные гражданские права мнимым числам на грани XVIII–XIX столетий дал Гаусс (Квант, 1977, № 8, с. 2), который назвал их комплексными числами, дал им геометрическую интерпретацию и, что самое главное, доказал основную теорему алгебры, утверждающую, что каждый многочлен имеет хотя бы один действительный или комплексный корень.

§ 2. Определение комплексных чисел

Мы будем исходить из того, что действительные числа нам известны. Мы знаем, что для них определены два основных действия — сложение и умножение — и имеются обратные к ним действия — вычитание и деление. Для этих действий выполняются хорошо известные правила, которые обычно употребляются совершенно автоматически, и поэтому я не буду их здесь формулировать.

• **Поле**

Множество объектов, для которых определены действия сложения и умножения и обратные к ним действия вычитания и деления, причем выполнены обычные правила, имеющие место для действительных чисел, называется в современной абстрактной алгебре полем.

Таким образом, с точки зрения современной абстрактной алгебры множество D всех действительных чисел представляет собой поле. Поставим теперь перед собой задачу расширить понятие числа, или, как говорят в абстрактной алгебре, расширить поле D до поля K^2 таким образом, чтобы в этом новом поле K^2 уравнение

• **Расширение поля действительных чисел**

$$z^2 + 1 = 0$$

имело решение. Элемент поля K^2, который удовлетворяет этому уравнению, обозначим через i. Таким образом, для i имеем

Мнимая единица

$$\boxed{i^2 = -1.} \qquad (1)$$

Так как поле K^2 содержит все действительные числа и элемент i и так как в нем возможны действия сложения и умножения, то в поле K^2 должны содержаться всевозможные многочлены относительно i с действительными коэффициентами, в частности все многочлены первой степени, т. е. выражения вида

Алгебраическая форма комплексного числа

$$\boxed{z = x + yi = x + iy,}$$

где x и y — действительные числа. Эти выражения и называются комплексными числами. Действия над ними мы определим как действия над многочленами, учитывая при этом условие (1). Комплексные числа вида

$$z = x + 0i = x$$

являются действительными числами. Комплексные числа вида

Чисто мнимое число

$$\boxed{z = 0 + yi = yi}$$

называются чисто мнимыми числами.

Пусть

$$z_1 = x_1 + y_1 i,$$
$$z_2 = x_2 + y_2 i$$

— два комплексных числа. Согласно высказанному правилу сумма и произведение этих комплексных чисел определяются равенствами

$$z_1 + z_2 = (x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + x_2) + (y_1 + y_2)i, \tag{2}$$

• **Операции над комплексными числами**

$$z_1 z_2 = (x_1 + y_1 i)(x_2 + y_2 i) = x_1 x_2 + (x_1 y_2 + y_1 x_2)i + y_1 y_2 i^2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i. \tag{3}$$

При получении последнего равенства мы использовали условие (1).

В случае, если число $z_1 = x_1$ — действительное, получаем

$$x_1 z_2 = x_1 x_2 + x_1 y_2 i. \tag{4}$$

Из формул (2) и (3) видно, что сумма и произведение двух комплексных чисел есть также комплексное число.

Для того чтобы убедиться, что действие вычитания, обратное действию сложения, существует, достаточно найти число $-z$, противоположное числу z, а для того чтобы убедиться в том,

что возможно деление, достаточно для $z \neq 0$ указать число z^{-1}, обратное числу $z = x + yi$. Числа эти, как легко видеть, задаются формулами

$$-z = -x - yi, \quad z^{-1} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\, i.$$

Таким образом, величина z^{-1}, обратная к z, существует всегда, когда $z \neq 0$.

§ 3. Геометрическое изображение комплексных чисел

Обозначим через P плоскость нашего чертежа и выберем на ней прямоугольную систему координат (рис. 1). Комплексное число $z = x + iy$ поместим в точку z с координатами x, y. Обозначим также через z вектор, идущий из начала координат O в точку z. Таким образом, буква z обозначает одновременно комплексное число, точку z, изображающую это комплексное число, и вектор z, соответствующий этому комплексному числу. При таком изображении действительные числа попадают на ось

Комплексная плоскость

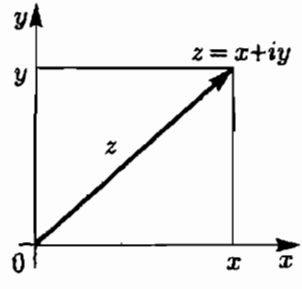


Рис. 1

абсцисс — поэтому ось абсцисс называется действительной осью плоскости P комплексного переменного, а чисто мнимые числа попадают на ось ординат — поэтому ось ординат называется мнимой осью плоскости P комплексного переменного. Нуль попадает в начало координат.

• **Модуль комплексного числа**

Длина вектора z называется модулем комплексного числа $z = x + iy$ и обозначается $|z|$:

$$|z| = +\sqrt{x^2 + y^2}.$$

Комплексные числа z, удовлетворяющие условию $|z| = 1$, составляют окружность радиуса 1 с центром в начале координат. На этой окружности лежит число 1. Из точки 1 отложим по окружности дугу заданной длины φ в направлении против часовой стрелки. Конец этой дуги обозначим через (φ). Если φ — отрицательное число, то для получения (φ) нужно отложить от точки 1 длину дуги $|\varphi|$ по часовой стрелке. Как известно, абсцисса точки (φ) называется $\cos\varphi$, а ее ордината — $\sin\varphi$. Таким образом, комплексное число (φ) задается формулой

$$(\varphi) = \cos\varphi + i\sin\varphi. \qquad (5)$$

Итак, всякое комплексное число z, по модулю равное 1, записывается в виде (5). Если z — произвольное комплексное число, модуль

которого $|z| = \rho$ отличен от 0, то число z/ρ является комплексным числом, по модулю равным 1, и потому записывается в виде (5). Из равенства

$$\frac{z}{\rho} = \cos\varphi + i\sin\varphi$$

Тригонометрическая форма комплексного числа

мы получаем

$$z = \rho(\cos\varphi + i\sin\varphi). \qquad (6)$$

Аргумент комплексного числа

Запись (6) называется тригонометрической формой комплексного числа. Число φ называется аргументом комплексного числа. Если модуль ρ комплексного числа z отличен от нуля, то аргумент определен с точностью до слагаемого $2k\pi$, где k — целое число. Если же модуль ρ комплексного числа равен 0, то формула (6) также имеет место, однако в этом случае аргумент комплексного числа вовсе не определен.

Числа ρ и φ называются полярными координатами точки z.

Дадим теперь геометрическое истолкование действий над комплексными числами.

Из формул (2) и (4) следует, что комплексные числа складываются и умножаются на действительные числа, как векторы.

Геометрический смысл сложения комплексных чисел

Геометрический смысл сложения комплексных чисел очевиден: вектор z_1+z_2 — это диагональ параллелограмма, построенного на векторах z_1 и z_2.

Отсюда вытекает важное неравенство:

$$|z_1 + z_2| \leqslant |z_1| + |z_2|. \qquad (7)$$

• **Неравенство треугольника**

Для того чтобы дать геометрическое истолкование умножения комплексных чисел, нужно употребить операцию поворота вектора или, что то же самое, комплексного числа. Повернув вектор z против часовой стрелки на угол α, мы получим некоторый новый вектор, который обозначим через $R_\alpha(z)$. Геометрически ясно, что операция поворота R_α имеет следующее свойство: если a — действительное число, то

$$R_{\alpha+\beta}(z) = R_\alpha\big(R_\beta(z)\big),$$
$$R_\alpha(az) = aR_\alpha(z),$$
$$R_\alpha(z_1 + z_2) = R_\alpha(z_1) + R_\alpha(z_2).$$

Из последних двух формул следует, что если a_1 и a_2 — два действительных числа, то имеет место соотношение

$$R_\alpha(a_1z_1 + a_2z_2) = a_1R_\alpha(z_1) + a_2R_\alpha(z_2). \qquad (8)$$

Непосредственно ясно также, что

$$R_\alpha(1) = \cos\alpha + i\sin\alpha. \qquad (9)$$

Докажем теперь, что

• **Геометрический смысл умножения комплексных чисел**

поворот комплексного числа $z = x + yi$ на угол α равносилен умножению его на комплексное число $\cos\alpha + i\sin\alpha$, *т. е. что*

$$\boxed{R_\alpha(z) = (\cos\alpha + i\sin\alpha)z.} \qquad (10)$$

Доказательство. Для этого рассмотрим сначала поворот на угол $d = \pi/2$. В этом случае

$$\cos d + i \sin d = i,$$

и равенство (10) принимает вид $R_d(z) = iz$. С одной стороны, геометрически очевидно, что $R_d(1) = i$, $R_d(i) = -1$. С другой стороны, $i \cdot 1 = i$, $i \cdot i = -1$. Таким образом,

$$R_d(1) = i \cdot 1, \quad R_d(i) = i \cdot i.$$

Из формулы (8) непосредственно вытекает:

$$iz = i \cdot (x+iy) = x \cdot i + y(-1) = xR_d(1) + yR_d(i) =$$
$$= R_d(x \cdot 1 + y \cdot i) = R_d(x + iy) = R_d(z).$$

Таким образом, формула (10) доказана для $\alpha = \dfrac{\pi}{2}$.

Пусть теперь α — произвольное действительное число. При $\widehat{z} = \cos\alpha + i \sin\alpha$ получаем

$$\widehat{z} \cdot i = i\widehat{z} = R_d(\widehat{z}) = R_d(\cos\alpha + i\sin\alpha) =$$
$$= \cos\left(\alpha + \frac{\pi}{2}\right) + i \sin\left(\alpha + \frac{\pi}{2}\right) =$$
$$= R_\alpha\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right) = R_\alpha(i). \quad (11)$$

Таким образом, формула (10) доказана при $z = i$.

Перейдем теперь к доказательству формулы (10) для произвольного комплексного числа

$$z = x + iy.$$

Из формул (8), (9), (11) имеем

$$\begin{aligned} R_\alpha(z) &= R_\alpha(x+iy) = xR_\alpha(1) + yR_\alpha(i) = \\ &= x(\cos\alpha + i\sin\alpha) + y(\cos\alpha + i\sin\alpha)i = \\ &= (\cos\alpha + i\sin\alpha)(x+yi) = \\ &= (\cos\alpha + i\sin\alpha)z. \end{aligned}$$

Таким образом, формула (10) полностью доказана. ■

Применяя формулу (10) к комплексному числу $z = \cos\beta + i\sin\beta$, получаем

$$\begin{aligned} &(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \\ &\quad = R_\alpha(\cos\beta + i\sin\beta) = R_\alpha\big(R_\beta(1)\big) = \\ &\quad = R_{\alpha+\beta}(1) = \cos(\alpha+\beta) + i\sin(\alpha+\beta). \end{aligned}$$

Таким образом,

$$\begin{aligned} &(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \\ &\quad = \cos(\alpha+\beta) + i\sin(\alpha+\beta). \end{aligned}$$

Производя перемножение комплексных чисел, стоящих в левой части, по формуле (3) получим

$$\begin{aligned} &(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \\ &\quad = (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + \\ &\qquad + (\sin\alpha\cos\beta + \cos\alpha\sin\beta)i. \end{aligned}$$

Значит, мы получили формулы для косинуса и синуса суммы:

$$\begin{aligned} \cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta, \\ \sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta. \end{aligned}$$

Для произвольных комплексных чисел, которые мы запишем в виде $r(\cos\alpha + i\sin\alpha)$, $s(\cos\beta + i\sin\beta)$, получаем

$$r(\cos\alpha + i\sin\alpha)\cdot s(\cos\beta + i\sin\beta) = \\ = rs[\cos(\alpha+\beta) + i\sin(\alpha+\beta)]. \tag{12}$$

Таким образом,

при перемножении двух комплексных чисел их модули перемножаются, а аргументы складываются.

Формулу (12) очевидным образом можно распространить на произвольное число сомножителей. Если все эти сомножители равны между собой и равны комплексному числу

$$r(\cos\alpha + i\sin\alpha),$$

то мы получаем

Формула Муавра

$$[r(\cos\alpha + i\sin\alpha)]^n = r^n(\cos n\alpha + i\sin n\alpha).$$

Эта формула очень интересна. Она дает возможность извлечь корень n-й степени из произвольного комплексного числа $\rho(\cos\varphi + i\sin\varphi)$. Именно, оказывается, что

Корень n-й степени комплексного числа

число корней n-й степени из числа

$$\rho(\cos\varphi + i\sin\varphi) \neq 0$$

равно n, причем корни эти расположены на окружности радиуса $\sqrt[n]{\rho}$ с центром в начале координат и составляют вершины правильного n-угольника.

Это утверждение я предоставляю для доказательства читателям.

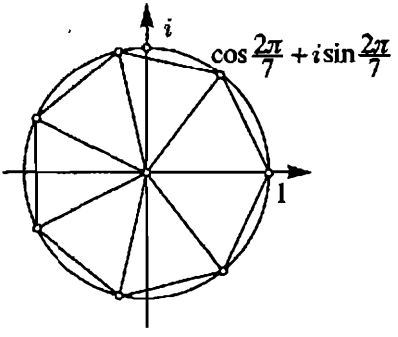


Рис. 2

В частности, корень n-й степени из единицы имеет n значений, которые являются вершинами правильного n-угольника, вписанного в единичный круг, причем одна из его вершин есть единица (рис. 2). В виде формулы эти корни записываются следующим образом:

$$\sqrt[n]{1} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0, 1, 2, \ldots, n-1.$$

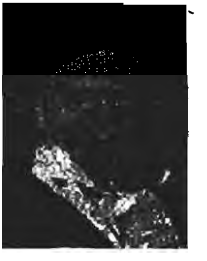
Глава 2

Основная теорема алгебры

§ 4. Пути в плоскости комплексного переменного 28
§ 5. Комплексные функции комплексного переменного 37

Здесь будет доказана основная теорема алгебры, утверждающая, что всякий многочлен с комплексными коэффициентами имеет по крайней мере один комплексный корень. При этом действительные числа считаются частным случаем комплексных чисел.

Основная теорема алгебры впервые была доказана Гауссом в 1799 году для частного случая многочленов с действительными коэффициентами. Гаусс показал, что всякий такой многочлен имеет по крайней мере один действительный или комплексный корень. С точки зрения современной абстрактной алгебры теорема эта показывает, что поле комплексных чисел алгебраически замкнуто: это значит, что, рассматривая корни алгебраических уравнений (т. е. корни многочленов) в этом поле, мы не можем получить новых чисел.



Карл Фридрих Гаусс (1777–1855)

В этом смысле поле комплексных чисел радикально отличается от поля действительных чисел, которое не является алгебраически замкнутым. При этом стоит заметить, что поле комплексных чисел получено из поля действительных чисел присоединением лишь одного корня

уравнения

$$z^2 + 1 = 0.$$

Доказательство основной теоремы алгебры опирается не на соображения абстрактной алгебры, а на конкретное рассмотрение поля комплексных чисел. Строгое ее доказательство должно опираться на точное определение действительного числа и на точное определение непрерывности функций. Я здесь привожу не строгое, но геометрически убедительное доказательство, основанное на рассмотрении путей в плоскости комплексного переменного и их деформаций. Доказательство это не только доказывает теорему, но до некоторой степени объясняет, почему она верна.

Как следствие основной теоремы алгебры мы покажем, как многочлен с комплексными (в частности, действительными) коэффициентами раскладывается на множители.

§ 4. Пути в плоскости комплексного переменного

Если точка z в плоскости P комплексного переменного перемещается во времени, когда время t меняется в пределах $t_0 \leqslant t \leqslant t_1$, то мы считаем,

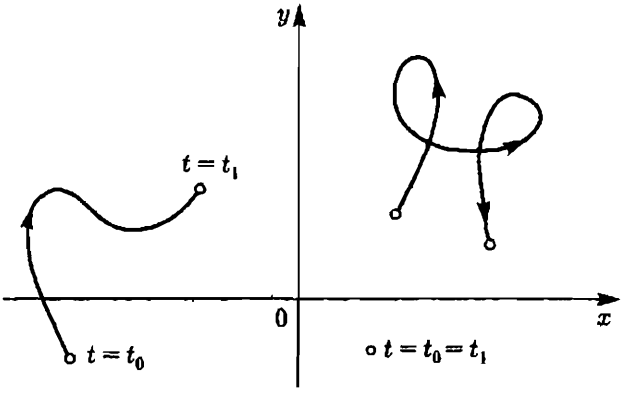


Рис. 3. Примеры путей

что в плоскости P задан путь (рис. 3). Таким образом,

• **Путь**

путь есть функция $z(t)$ действительного переменного t, принимающая комплексные значения, заданная на отрезке $t_0 \leqslant t \leqslant t_1$:

$$z(t), \quad t_0 \leqslant t \leqslant t_1.$$

Формула эта задает путь. Речь здесь идет о движении точки, осуществляемом естественно, без скачков. Так что функция $z(t)$ является непрерывной функцией. Мы не уточняем здесь понятие непрерывности, считая, что оно интуитивно ясно, как движение точки. Следует отчетливо понимать, что путь есть процесс движения, а не та линия, которую описывает движущаяся точка. Одну и ту же линию можно описать разными способами.

В процессе движения точка $z(t)$ в разные моменты времени может попадать в одну и ту же точку плоскости, так что не исключается равенство

$$z(t_2) = z(t_3) \quad \text{при} \quad t_2 \neq t_3.$$

Таким образом, путь может иметь самопересечения. Он может даже состоять из одной точки, именно в случае, когда точка $z(t)$ вовсе не перемещается при изменении t.

В дальнейшем, если это не будет оговорено специально, мы всегда будем предполагать, что путь не проходит через начало координат, т. е. что величина $z(t)$ ни при каком значении (t) не обращается в нуль.

Замкнутый путь

Точка $z(t_0) = z_0$ называется началом пути, а точка $z(t_1) = z_1$ — его концом. Если имеет место равенство $z_0 = z_1$, то путь называется замкнутым (рис. 4).

Так как комплексное число $z(t)$ не обращается в нуль, для всякого значения t определен аргумент $\varphi(t)$ комплексного числа $z(t)$, но он определен лишь с точностью до слагаемого $2k\pi$. Эта неоднозначность для нас нежелательна. Для того чтобы освободиться от нее, выберем для начальной точки z_0 вполне определенный аргумент $\varphi_0 = \varphi(t_0)$.

Затем по мере возрастания t будем выбирать аргумент $\varphi(t)$ точки $z(t)$ так, чтобы при

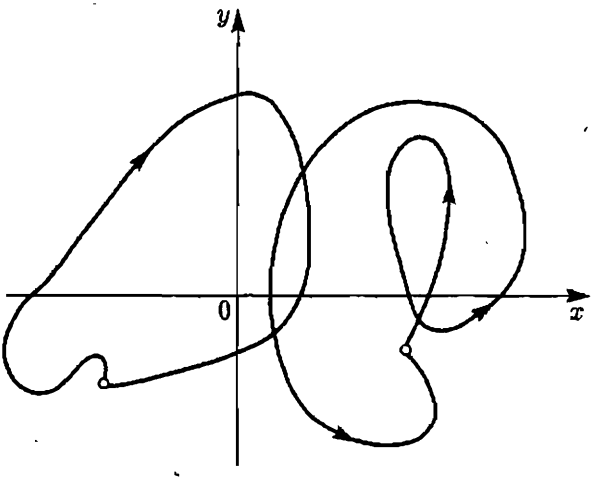


Рис. 4. Замкнутые пути

малых изменениях t он менялся мало. Этим неоднозначность выбора аргумента будет устранена. Добавление к аргументу числа $2k\pi$ при $k \neq 0$ привело бы сразу к резкому изменению величины $\varphi(t)$. Выбрав начальное значение аргумента $\varphi(t_0) = \varphi_0$ и следя за тем, чтобы аргумент $\varphi(t)$ точки $z(t)$ менялся вместе с t непрерывно, мы получаем вполне определенную функцию $\varphi(t)$, меняющуюся непрерывно, т. е. без скачков. Если выбрать начальное значение аргумента φ_0 иначе, изменив его на $2k\pi$, то он будет отличаться от ранее выбранного ровно на $2k\pi$ на всем протяжении изменения t. Отсюда следует, что при таком способе построения функции $\varphi(t)$ величина

$$\varphi(t_1) - \varphi(t_0) \qquad (1)$$

не зависит от случайно выбранного начального значения аргумента числа z_0.

Если путь замкнут, то точки z_0 и z_1 совпадают и, следовательно, их аргументы $\varphi(t_0)$ и $\varphi(t_1)$ могут отличаться лишь на $2k\pi$. Поэтому число (1) в случае замкнутого пути есть $2k\pi$.

Индекс замкнутого пути

Целое число k называется индексом замкнутого пути в плоскости комплексного переменного z. Следует еще раз подчеркнуть, что индекс замкнутого пути можно определить лишь в том случае, когда путь не проходит через начало координат.

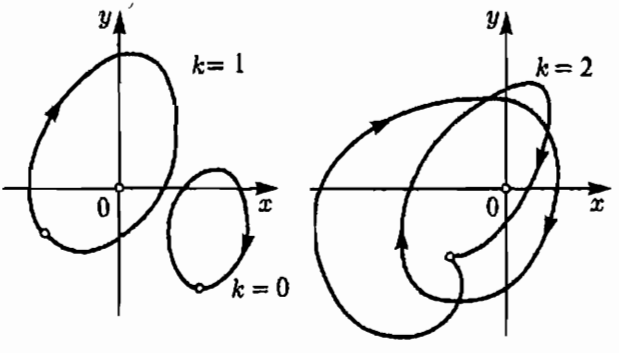


Рис. 5. Пути с индексами 0, 1, 2

Геометрический смысл индекса замкнутого пути

Индекс k имеет простой геометрический смысл. Именно, он

указывает, сколько раз точка $z(t)$, описывая замкнутый путь, обходит начало координат (рис. 5).

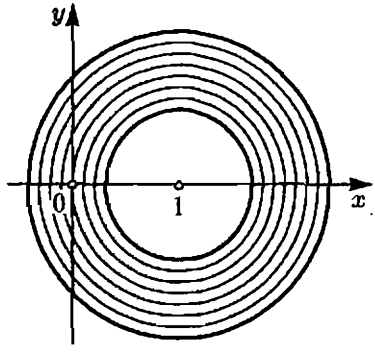


Рис. 6. Деформация пути $1 + r(\cos\alpha + i\sin\alpha)$ при изменении r

Рассмотрим простой пример.

Пример 4.1. Путь

$$1 + r(\cos t + i\sin t), \quad 0 \leqslant t \leqslant 2\pi, \qquad (2)$$

является замкнутым. Он описывает окружность с центром в точке 1 и радиусом r и проходит эту окружность в течение времени t равномерно против часовой стрелки. Если число $r < 1$, то окружность не содержит внутри себя начало координат и индекс пути равен 0. Если $r > 1$, то окружность содержит внутри себя начало координат и индекс пути равен 1 (проверьте это самостоятельно). В случае $r = 1$ путь проходит через начало координат и его индекс не определен. Если число r меняется, то путь (2), как говорят, деформируется (рис. 6).

Мы видим на этом примере, что во время деформации замкнутого пути его индекс не ме-

няется, если только путь в какой-то момент деформации не проходит через начало координат.

Говоря, что путь описывается движением точки во времени, мы лишь хотели придать более интуитивный характер определению пути. В действительности же речь идет о зависимости комплексного переменного z от некоторого действительного параметра t (который можно обозначить и другой буквой). Так, например, путь (2) можно записать в виде

$$1 + r(\cos\alpha + i\sin\alpha), \quad 0 \leqslant \alpha \leqslant 2\pi, \qquad (3)$$

где параметром уже является не t, а α. Ясно, что путь (3) описывается точкой $1 + z$, когда точка z описывает путь

$$r(\cos\alpha + i\sin\alpha), \quad 0 \leqslant \alpha \leqslant 2\pi.$$

Здесь r есть числовой параметр, от которого зависит сам путь. Говорят, что при изменении r путь (3) деформируется.

Введем понятие деформации пути. Будем считать, что

Деформация пути

путь деформируется, если он постепенно меняется без скачков в зависимости от некоторого параметра, который для пути (3) обозначен через r, а вообще может быть обозначен и другой буквой, например, s (рис. 7).

Таким образом, деформирующийся путь записывается формулой

$$z(\alpha, s), \quad \alpha_0 \leqslant \alpha \leqslant \alpha_1, \quad s_0 \leqslant s \leqslant s_1. \qquad (4)$$

Здесь при каждом фиксированном значении параметра s имеем определенный путь, описываемый во время изменения α от α_0 до α_1, а при изменении s сам путь меняется, деформируясь. Ясно, что если путь (4) замкнут, т. е. если при любом значении s имеет место равенство

$$z(\alpha_0, s) = z(\alpha_1, s),$$

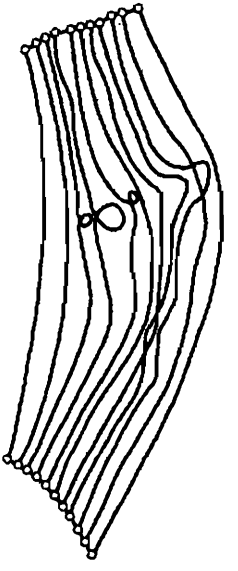


Рис. 7. Деформация пути

то в течение деформации индекс пути должен меняться без скачков. А так как он есть целое число, то индекс этот остается постоянным. Конечно, это верно только в том случае, когда для произвольного значения s путь (4) не проходит через начало координат. В противном случае для этого значения s индекс пути не определен. Таким образом, мы можем высказать следующее утверждение:

Теорема об индексе пути

если замкнутый путь непрерывно деформируется, не проходя в процессе деформации через начало координат, то индекс его не меняется.

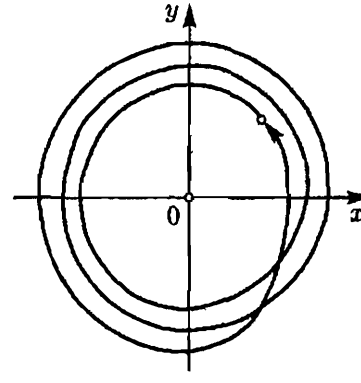


Рис. 8

Пример 4.2. Дадим еще один пример замкнутого пути:

$$r^n(\cos n\alpha + i \sin n\alpha), \quad 0 \leqslant \alpha \leqslant 2\pi. \qquad (5)$$

Ясно, что путь этот описывается точкой z^n, когда точка z описывает замкнутый путь

$$r(\cos \alpha + i \sin \alpha), \quad 0 \leqslant \alpha \leqslant 2\pi.$$

Видно, что когда α меняется от 0 до 2π, аргумент точки z^n меняется от 0 до $2n\pi$. Таким образом, индекс пути (5) равен n (см. рис. 8, где схематически показан случай $n = 3$).

§ 5. Комплексные функции комплексного переменного

Если числовое значение комплексной переменной величины w можно найти, зная числовое значение другой комплексной переменной величины z, то переменная величина w называется функцией переменной величины z, что записывается в форме

$$w = f(z).$$

• **Аналитическая функция комплексного переменного**

Если комплексная функция $f(z)$ комплексного переменного z имеет производную, то она называется аналитической функцией.

Теория аналитических функций является теперь одним из важнейших разделов математики. Здесь нас будут интересовать лишь аналитические функции очень частного вида, именно многочлены.

Рассмотрим многочлен

$$w = f(z) = z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n, \tag{6}$$

где $a_1, a_2, \ldots, a_n$ суть комплексные коэффициенты, а n — неотрицательное целое число, которое называется степенью многочлена. Целью

нашего исследования будет доказательство того, что

Основная теорема алгебры

многочлен (6) *положительной степени имеет корень, т. е. что уравнение*

$$f(z) = 0,$$

где $f(z)$ — *многочлен* (6) *и* $n > 0$, *имеет решение.*

Доказательство. Для доказательства этого рассмотрим замкнутый путь

$$f[r(\cos\alpha + i\sin\alpha)], \quad 0 \leqslant \alpha \leqslant 2\pi, \qquad (7)$$

который описывает точка $f(z)$, когда точка z описывает замкнутый путь

$$r(\cos\alpha + i\sin\alpha), \quad 0 \leqslant \alpha \leqslant 2\pi.$$

Случай, когда свободный член a_n многочлена $f(z)$ равен 0, не требует рассмотрения, так как в этом случае многочлен $f(z)$ имеет очевидный корень $z = 0$. Поэтому мы будем считать, что $a_n \neq 0$. Замкнутый путь (7) зависит от параметра r и при изменении параметра r деформируется. При $r = 0$ число z равно 0 и путь $f(z)$ состоит из неподвижной точки a_n. Таким образом, его индекс при $r = 0$ равен 0. Мы докажем, что если взять r достаточно большим, то индекс пути (7) равен n. Но по предположению $n \neq 0$, поэтому при изменении числа r от большого значения к нулю путь (7), деформируясь,

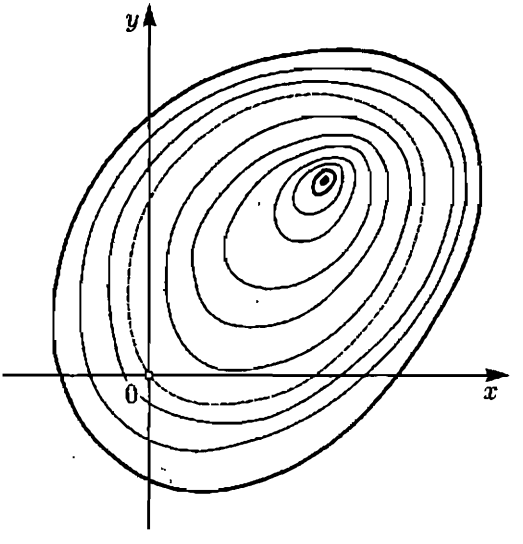


Рис. 9

пройдет при каком-то значении r через начало координат, а это и значит, что при некотором значении z функция $f(z)$ обратится в нуль, т. е. корень у этого многочлена существует (рис. 9).

Для доказательства того, что при достаточно большом r замкнутый путь (7) имеет индекс, равный n, продеформируем этот путь в более простой, индекс которого легко сосчитать.

Прежде всего мы разобьем многочлен $f(z)$ на сумму двух многочленов:

$$f(z) = z^n + g(z),$$

где $g(z)$ задается формулой

$$g(z) = a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_{n-1} z + a_n.$$

Так как коэффициенты $a_1, a_2, \ldots, a_n$ многочлена $g(z)$ суть вполне определенные числа, то все они не превосходят по модулю некоторую константу c. Из доказанного в § 3 неравенства (7), распространенного на произвольное число слагаемых, следует, что при $|z| > 1$

$$|g(z)| \leqslant nc|z^{n-1}|. \tag{8}$$

Рассмотрим многочлен $f(z, s)$, зависящий от параметра s, $0 \leqslant s \leqslant 1$, задаваемый следующей формулой:

$$f(z, s) = z^n + sg(z).$$

Мы имеем равенство

$$z^n = f(z, s) - sg(z),$$

откуда

$$\begin{aligned} |z^n| &\leqslant |f(z, s)| + |-sg(z)| \leqslant \\ &\leqslant |f(z, s)| + nc|z^{n-1}|s \leqslant \\ &\leqslant |f(z, s)| + nc|z^{n-1}| \end{aligned}$$

(см. (8)). Отсюда следует

$$|f(z, s)| \geqslant |z^n| - nc|z^{n-1}|.$$

Обозначим $|z|$ через r, тогда последнее неравенство принимает вид

$$|f(z, s)| \geqslant r^n - ncr^{n-1} = r^{n-1}(r - cn).$$

Таким образом, при $r > cn$ правая часть предыдущего неравенства положительна. Следовательно, модуль функции $f(z, s)$не обращается

в нуль ни при каком значении s, если только $r > cn$.

Обратим внимание теперь на тот факт, что при $s = 0$ многочлен $f(z, s)$ превращается в известный нам многочлен z^n. А индекс пути z^n, когда z описывает окружность $r(\cos\alpha + i\sin\alpha)$, нами уже сосчитан (см. (5)). Он равен n. При $s = 1$ многочлен $f(z, s)$ превращается в многочлен $f(z)$, и определяемый им путь (7) имеет индекс, тоже равный n. Итак, мы доказали, что индекс пути (7), определяемый многочленом $f(z)$, при $r > cn$ равен n. Таким образом, можно считать, что при меняющемся r от 0 до $cn + \varepsilon$, где $\varepsilon > 0$, путь (7) деформируется, причем при $r = 0$ этот путь превращается в одну точку и его индекс равен 0, а при $r = cn + \varepsilon$ его индекс равен n. Из этого видно, что в процессе изменения r путь (7) при некотором значении r проходит через начало координат, и следовательно, многочлен $f(z)$ при некотором значении z, $|z| \leqslant cn + \varepsilon$, обращается в нуль.

Итак, основная теорема алгебры доказана. ■

Глава 3

Алгоритм Евклида

§ 6. Деление многочленов 45
§ 7. Разложение многочлена на множители 49
§ 8. Общий наибольший делитель двух многочленов 55
§ 9. Устранение кратных корней 59
§ 10. Подсчет числа действительных корней многочлена на заданном отрезке 63

При делении целого положительного числа a на целое положительное число b приходим к равенству

$$a = bh + k, \qquad (1)$$

где h и k — целые неотрицательные числа и $k < b$. Число h называется частным, а k — остатком при делении числа a на число b. Способ деления целых чисел хорошо известен из арифметики. Но так же, как целые числа, можно делить друг на друга и многочлены.

• **Деление многочленов**

§ 6. Деление многочленов

Будем исходить из двух многочленов

$$a(z) = a_0 z^p + a_1 z^{p-1} + \ldots + a_p,$$

$$b(z) = b_0 z^q + b_1 z^{q-1} + \ldots + b_q.$$

Предположим здесь, что числа a_0 и b_0 не равны нулю, так что многочлен $a(z)$ имеет степень p, а многочлен $b(z)$ имеет степень q.

В результате деления многочлена $a(z)$ на многочлен $b(z)$ мы придем к следующему равен-

ству, аналогичному равенству (1):

$$a(z) = b(z)h(z) + k(z), \qquad (2)$$

где степень многочлена $k(z)$ *меньше* q.

Многочлены $h(z)$ и $k(z)$ называются соответственно частным и остатком при делении многочлена $a(z)$ на многочлен $b(z)$.

Если $k \equiv 0$, то говорят, что многочлен $a(z)$ делится на многочлен $b(z)$, а $h(z)$ является частным от их деления.

Евклид
(330–275)

Алгоритм Евклида

Равенство (1) доказано в арифметике, а равенство (2) должно доказываться в алгебре. Но деление многочленов не входит в ныне действующую школьную программу. Чтобы доказать (2), мы должны построить такие многочлены $h(z)$ и $k(z)$, которые удовлетворяют этому равенству. Процесс этого построения представляет собою очень важный алгоритм, так называемый *алгоритм Евклида*. Опишем его.

Если $p < q$, то $h(z) = 0$, $k(z) = a(z)$ и равенство (2) выполнено.

Теперь мы будем строить многочлены $h(z)$ и $k(z)$ в предположении, что $p \geqslant q$. Сначала построим равенство

$$a(z) = b(z)h_1(z) + a_1(z), \qquad (3)$$

в котором степень многочлена $a_1(z)$ меньше p. Для этого положим

$$h_1(z) = \frac{a_0}{b_0} z^{p-q}.$$

Тогда разность

$$a(z) - b(z)h_1(z) = a_1(z)$$

имеет степень меньше, чем p, так как в этом многочлене коэффициент при z^p равен нулю, а остальные степени z, входящие в этот многочлен, очевидно, меньше p. Таким образом, равенство (3) построено.

Если многочлен $a_1(z)$ имеет степень меньшую, чем q, то равенство (3) уже является равенством (2). В противоположном случае к многочлену $a_1(z)$ применим ту же процедуру, которая применялась к многочлену $a(z)$ при построении равенства (3). Тогда получим для него равенство

$$a_1(z) = b(z)h_2(z) + a_2(z),$$

причем степень многочлена $a_2(z)$ уже меньше, чем степень многочлена $a_1(z)$. Если многочлен $a_2(z)$ уже имеет степень меньшую, чем q, то, подставляя $a_1(z)$ из последнего равенства в равенство (3), получим

$$a(z) = b(z)(h_1(z) + h_2(z)) + a_2(z),$$

которое уже является равенством (2). Если многочлен $a_2(z)$ тоже имеет степень большую, чем q, то мы продолжим наше построение дальше и в конце концов докажем нужное равенство (2).

Здесь мы описали процесс деления многочлена $a(z)$ на многочлен $b(z)$, т. е. нахождение многочленов $h(z)$ и $k(z)$, входящих в равенство (2). Докажем теперь, что многочлены $h(z)$ и $k(z)$ однозначно определены многочленами $a(z)$ и $b(z)$. Допустим, что наряду с равенством (2) имеет место равенство

$$a(z) = b(z)h_0(z) + k_0(z),$$

причем степень многочлена $k_0(z)$ меньше q. Вычитая это равенство из равенства (2), получим

$$b(z)(h(z) - h_0(z)) = k_0(z) - k(z).$$

Так как степень многочлена $b(z)$ равна q, а степень многочлена $k_0(z) - k(z)$ меньше q, то последнее равенство может иметь место лишь при условии

$$h(z) - h_0(z) \equiv 0,$$

так что и

$$k(z) - k_0(z) \equiv 0.$$

Заметим, что

при делении многочленов не могут возникнуть комплексные числа. Именно, если многочлены $a(z)$ и $b(z)$ имеют действительные коэффициенты, то многочлены $h(z)$ и $k(z)$ также имеют действительные коэффициенты.

§ 7. Разложение многочлена на множители

Теперь существующий по основной теореме алгебры корень многочлена

$$f_0(z) = z^n + a_1 z^{n-1} + \ldots + a_n, \quad n > 0,$$

с комплексными коэффициентами обозначим через α_1. Докажем, что

многочлен $f_0(z)$ делится на двучлен $(z - \alpha_1)$.

Доказательство. Производя деление многочлена $f_0(z)$ на многочлен первой степени $(z - \alpha_1)$ по правилам, описанным в § 6, мы получим частное, которое обозначим через $f_1(z)$, и некоторый остаток в виде многочлена нулевой степени, т. е. числа, которое мы обозначим через k. Таким образом, имеем

$$f_0(z) = f_1(z)(z - \alpha_1) + k.$$

Так как $f_0(\alpha_1) = 0$, то, полагая в предыдущем равенстве $z = \alpha_1$, получаем $k = 0$. ■

Итак, многочлен $f_0(z)$ делится на $(z - \alpha_1)$, и мы имеем

$$f_0(z) = (z - \alpha_1) f_1(z),$$

где $f_1(z)$ — многочлен степени $n - 1$, который, очевидно, начинается с члена z^{n-1}. Если $n > 1$, то $n - 1 > 0$; тогда многочлен $f_1(z)$ будет положительной степени и по доказанному ранее имеет

некоторый корень α_2. Таким образом, по только что доказанному многочлен $f_1(z)$ разлагается на множители

$$f_1(z) = (z - \alpha_2) f_2(z). \tag{4}$$

Продолжая этот процесс дальше, мы получим разложение $f_0(z)$ на n линейных множителей

Разложение многочлена на множители

$$f_0(z) = (z - \alpha_1)(z - \alpha_2) \dots (z - \alpha_n).$$

Числа $\alpha_1, \alpha_2, \dots, \alpha_n$ являются корнями многочлена $f_0(z)$, и других корней многочлен $f_0(z)$, очевидно, не имеет. Однако может оказаться, что один и тот же корень встречается в этом разложении несколько раз. Группируя равные между собой корни, получаем разложение

$$f_0(z) = (z - \alpha_1)^{k_1} (z - \alpha_2)^{k_2} \dots (z - \alpha_q)^{k_q}, \tag{5}$$

где все корни $\alpha_1, \alpha_2, \dots, \alpha_q$ различны. Число k_1 называется кратностью корня α_1, число k_2 — кратностью корня α_2 и так далее, число k_q — кратностью корня α_q. Таким образом, число различных корней многочлена $f_0(z)$ может быть и меньше, чем n. Однако если учитывать кратность каждого корня, то сумма кратностей в точности равна n. В этом смысле многочлен $f_0(z)$ имеет ровно n корней.

Кратность корня многочлена

Рассмотрим теперь случай, когда все коэффициенты многочлена $f_0(z)$ — действительные числа. О корнях такого многочлена можно высказать некоторые весьма интересные дополнительные соображения.

Для рассмотрения многочлена с действительными коэффициентами введем понятие числа $\bar{z}$, комплексно сопряженного данному комплексному числу z. Именно,

• **Комплексно сопряженное число**

если

$$z = x + iy,$$

то по определению число

$$\bar{z} = x - iy \qquad (6)$$

называется комплексно сопряженным с z.

Таким образом,

число $\bar{z}$, комплексно сопряженное с числом z, является зеркальным образом числа z относительно оси действительных чисел.

Если

$$z = r(\cos\alpha + i\sin\alpha),$$

то

$$\bar{z} = r(\cos\alpha - i\sin\alpha) =$$
$$= r[\cos(-\alpha) + i\sin(-\alpha)]. \qquad (7)$$

Таким образом,

аргументы двух комплексно сопряженных чисел отличаются лишь знаком.

Из формулы (6) следует, что

Свойства комплексного сопряжения

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

(см. главу 1 (2)). Из формулы (7) следует, что

$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$$

(см. главу 1 (12)). Заметим еще, что

равенство

$$\bar{z} = z$$

имеет место тогда и только тогда, когда z есть действительное число.

Из трех предыдущих формул легко получить, что

для многочлена $f_0(z)$ с действительными коэффициентами имеет место равенство

$$\overline{f_0(z)} = f_0(\bar{z}).$$

Из этого равенства следует, что

если α_1 есть корень многочлена $f_0(z)$ с действительными коэффициентами, то $\bar{\alpha}_1$ есть также его корень.

В случае, если α_1 есть действительное число, это утверждение бессодержательно. В случае, если α_1 не есть действительное число, утверждение указывает на существование наряду с корнем α_1 отличного от него корня $\bar{\alpha}_1$. Таким образом, если α_1 — не действительное число, то многочлен $f_1(z)$ (см. (4)) имеет делитель $(z-\bar{\alpha}_1)$, и мы получаем разложение на множители

$$f_0(z) = (z-\alpha_1)(z-\bar{\alpha}_1)f_2(z).$$

Таким образом, мы выделили у многочлена $f_0(z)$ квадратичный множитель

$$g_2(z) = (z-\alpha_1)(z-\bar{\alpha}_1) = \\ = z^2 - (\alpha_1+\bar{\alpha}_1)z + \alpha_1\bar{\alpha}_1.$$

Многочлен $g_2(z)$ очевидным образом имеет действительные коэффициенты и не разлагается на действительные множители, так как не имеет действительных корней. Отсюда следует, что многочлен $f_2(z)$ — также многочлен с действительными коэффициентами, так как он получается в результате деления многочлена $f_0(z)$ на действительный квадратичный трехчлен $g_2(z)$ (см. конец § 6).

Таким образом, если α_1 — действительный корень, то мы имеем разложение

$$f_0(z) = g_1(z) f_1(z),$$

где $g_1(z) = z - \alpha_1$, а если α_1 — не действительный корень, то мы имеем разложение

$$f_0(z) = g_2(z) f_2(z).$$

Таким образом, в обоих случаях $f_0(z)$ делится на действительный многочлен первой или второй степени, не разложимый на действительные множители.

Неприводимый многочлен

Многочлен с действительными коэффициентами, не разложимый на действительные множители, называется неприводимым.

Значит,

многочлен $f_0(z)$ разлагается на действительные неприводимые множители степени один или два.

Из этого вытекает важный вывод:

каждый корень многочлена $f_0(z)$ является корнем неприводимого многочлена первой или второй степени.

§ 8. Общий наибольший делитель двух многочленов

Многочлен $b(z)$ считается делителем многочлена $a(z)$, если при делении $a(z)$ на $b(z)$ не получается остатка, т. е. в формуле (2) $k(z) \equiv 0$.

• **Делитель многочлена**

Многочлен $b(z)$ считается общим делителем двух многочленов $a_0(z)$ и $a_1(z)$, если он является делителем каждого из этих двух многочленов.

• **Общий делитель двух многочленов**

Общий делитель $c(z)$ двух многочленов $a_0(z)$ и $a_1(z)$ называется их общим наибольшим делителем, если он делится на каждый общий делитель $b(z)$ многочленов $a_0(z)$ и $a_1(z)$.

• **Общий наибольший делитель двух многочленов**

Существование общего наибольшего делителя двух многочленов не очевидно. Ниже оно будет доказано при помощи последовательного деления многочленов друг на друга, т. е. при помощи таких операций, которые совершаются без особых трудностей, кроме громоздких вычислений. Но прежде всего мы докажем, что

Единственность общего наибольшего делителя •

два общих наибольших делителя $c_0(z)$ и $c_1(z)$ двух многочленов $a_0(z)$ и $a_1(z)$ по существу совпадают. Именно, они могут отличаться друг от друга только числовым множителем, отличным от нуля.

Докажем это.

Доказательство. Так как $c_0(z)$ является общим наибольшим делителем многочленов $a_0(z)$ и $a_1(z)$, а $c_1(z)$ — их общим делителем, то $c_0(z)$ делится на $c_1(z)$, и следовательно, мы имеем тождество

$$c_0(z) = h_1(z)c_1(z). \tag{8}$$

Аналогично мы имеем формулу

$$c_1(z) = h_0(z)c_0(z). \tag{9}$$

Подставляя выражение $c_1(z)$ из формулы (9) в формулу (8), получаем

$$c_0(z) = h_0(z)h_1(z)c_0(z).$$

А так как при перемножении многочленов степени их складываются, то из последней формулы следует, что многочлены $h_0(z)$ и $h_1(z)$ имеют степень нуль, т. е. являются числами.

Таким образом, единственность общего наибольшего делителя многочленов $a_0(z)$ и $a_1(z)$ доказана. ■

Перейдем теперь к построению общего наибольшего делителя $c(z)$ многочленов $a_0(z)$ и $a_1(z)$. Для этого произведем деление многочлена

• **Существование общего наибольшего делителя**

$a_0(z)$ на многочлен $a_1(z)$. Запишем формулу (2) в виде

$$a_0(z) = a_1(z)h_1(z) + a_2(z), \qquad (10)$$

т. е. обозначим остаток от этого деления через $a_2(z)$. Теперь подвергнем многочлен $a_1(z)$ делению на многочлен $a_2(z)$, и формулу (2) запишем в виде

$$a_1(z) = a_2(z)h_2(z) + a_3(z), \qquad (11)$$

т. е. обозначим остаток от деления через $a_3(z)$. Теперь подвергнем делению многочлен $a_2(z)$ на многочлен $a_3(z)$ и запишем формулу (2) в виде

$$a_2(z) = a_3(z)h_3(z) + a_4(z).$$

Так как в процессе этого построения степень остаточного многочлена все время снижается, то мы дойдем до такого остатка, который либо равен нулю, либо будет иметь степень нуль, а при делении на многочлен степени нуль остаток, очевидно, равен нулю. Таким образом, в конце концов мы получим тождества

$$a_{n-2}(z) = a_{n-1}(z)h_{n-1}(z) + a_n(z), \qquad (12)$$

$$a_{n-1}(z) = a_n(z)h_n(z). \qquad (13)$$

Если теперь $b(z)$ — общий делитель многочленов $a_0(z)$ и $a_1(z)$, то из формулы (10) следует, что он является делителем $a_2(z)$. Из формулы (11) следует, что многочлен $b(z)$ является делителем многочлена $a_3(z)$. Таким образом, докажем последовательно, что многочлен $b(z)$

является делителем всех построенных нами многочленов

$$a_0(z),\ a_1(z),\ a_2(z),\ \ldots,\ a_n(z),$$

в частности многочлена $a_n(z)$. А из формулы (13) следует, что многочлен $a_n(z)$ является делителем $a_{n-1}(z)$, из формулы (12) следует, что он является делителем $a_{n-2}(z)$. В конце концов мы установим, что $a_n(z)$ является делителем многочленов $a_0(z)$ и $a_1(z)$. Таким образом, доказано, что $a_n(z)$ делится на любой делитель многочленов $a_0(z)$ и $a_1(z)$ и сам является их делителем. Следовательно, многочлен $a_n(z)$ является общим наибольшим делителем многочленов $a_0(z)$ и $a_1(z)$.

Докажем теперь следующий важный результат, имеющий многочисленные применения в алгебре.

Общий наибольший делитель $c(z)$ двух многочленов $a_0(z)$ и $a_1(z)$ может быть записан в виде формулы

Вид ОНД двух многочленов

$$\boxed{c(z) = p_0(z)a_0(z) + p_1(z)a_1(z),} \qquad (14)$$

где $p_0(z), p_1(z)$ — некоторые многочлены.

Докажем это утверждение.

Доказательство. Подставляя выражение многочлена $a_2(z)$ из формулы (10) в формулу (11), получим

$$a_3(z) = p_2(z)a_0(z) + q_0(z)a_1(z).$$

Продолжая этот процесс дальше, мы получим формулу (14). Таким образом, формула (14) доказана. ■

§ 9. Устранение кратных корней

Нахождение корней многочлена является одной из наиболее старых и трудных задач алгебры. Первоначально ее пытались решить при помощи формулы, состоящей из алгебраических выражений, включающих извлечение корней. Это очень удачно сделано для квадратного уравнения. Для кубического уравнения также имеется формула, но уже мало значительная в смысле приложений. Для уравнений четвертой степени также есть формула, но лишенная всякого практического значения. Позже было доказано, что для уравнений выше четвертой степени общей формулы решения уравнений в радикалах не существует. Полная теория о возможностях нахождения корней многочлена при помощи радикалов была построена Галуа. На пути решения проблемы отыскания корней многочлена лежит следующая, гораздо более простая задача.

Для многочлена $f(z)$, имеющего как простые, так и кратные корни, найти такой многочлен $g(z)$, который имеет те же самые корни, что и $f(z)$, но только простые.

Эта задача решается при помощи алгоритма Евклида, т. е. при помощи деления многочленов. Ее решение будет рассмотрено в этом параграфе.

Пусть $a(z)$ и $b(z)$ — два многочлена, а $p(z)$ — их произведение,

$$p(z) = a(z)b(z).$$

Обозначим через

$$\alpha_1, \alpha_2, \ldots, \alpha_q$$

совокупность всех чисел, каждое из которых является корнем хотя бы одного из многочленов $a(z)$ и $b(z)$. Тогда эти многочлены могут быть записаны в следующем виде (см. (5)):

$$a(z) = (z - \alpha_1)^{k_1}(z - \alpha_2)^{k_2} \ldots (z - \alpha_q)^{k_q}, \quad (15)$$

$$b(z) = (z - \alpha_1)^{l_1}(z - \alpha_2)^{l_2} \ldots (z - \alpha_q)^{l_q}. \quad (16)$$

В обоих этих разложениях некоторые показатели степеней могут равняться нулю. Мы будем считать, что кратность соответствующих корней равна нулю. Очевидно, мы имеем

$$p(z) = (z - \alpha_1)^{k_1+l_1}(z - \alpha_2)^{k_2+l_2} \ldots (z - \alpha_q)^{k_q+l_q}.$$

Таким образом,

при перемножении многочленов кратности корней у них складываются.

Исходя из разложения многочленов $a(z)$, $b(z)$ на множители (см. (15) и (16)), легко найти

их общий наибольший делитель $c(z)$. Для этого обозначим через m_1 наименьшее из чисел k_1 и l_1, через m_2 — наименьшее из чисел k_2 и l_2 и т. д., через m_q — наименьшее из чисел k_q и l_q. Тогда наибольший общий делитель многочленов $a(z)$ и $b(z)$ задается формулой

$$c(z) = (z - \alpha_1)^{m_1}(z - \alpha_2)^{m_2} \dots (z - \alpha_q)^{m_q}.$$

Этот простой способ нахождения общего наибольшего делителя двух многочленов требует, однако, нахождения всех корней обоих многочленов, и потому он практически мало пригоден, так как сводит простую задачу к очень трудной. Между тем нахождение общего наибольшего делителя двух многочленов, как было показано в § 8, представляет собой очень простую, решающуюся при помощи алгоритма Евклида, т. е. при помощи деления многочленов, задачу.

Выясним теперь, как связаны между собой кратности корней многочленов $a_0(z)$ и $a_1(z) = a_0'(z)$, т. е. кратности корней многочлена $a_0(z)$ и его производной $a_0'(z)$.

Оказывается, что если корень α многочлена $a_0(z)$ имеет кратность k, то тот же корень для многочлена $a_1(z) = a_0'(z)$ имеет кратность $k - 1$. Но, конечно, кроме корней, являющихся корнями многочлена $a_0(z)$, многочлен $a_0'(z)$ может иметь и другие корни.

Докажем, что

если α есть корень многочлена $a_0(z)$ кратности k, то тот же корень является корнем многочлена $a_1(z) = a_0'(z)$ кратности $k-1$.

Доказательство. Из разложения (5) многочлена $a_0(z)$ на множители следует, что если α есть корень многочлена $a_0(z)$ кратности k, то

$$a_0(z) = (z-\alpha)^k b(z),$$

причем $b(z)$ уже не делится на $(z-\alpha)$ и, следовательно, не имеет α своим корнем. Дифференцируя последнее соотношение, получаем

$$a_0'(z) = a_1(z) = \\ = k(z-\alpha)^{k-1} b(z) + (z-\alpha)^k b'(z), \quad (17)$$

$$(z-\alpha)^{k-1} b(z) = \frac{1}{k} a_1(z) + \frac{1}{k}(z-\alpha)^k b'(z). \quad (18)$$

Из формулы (17) видно, что $a_1(z)$ делится на $(z-\alpha)^{k-1}$, а из формулы (18) следует, что $a_1(z)$ не делится на $(z-\alpha)^k$. В самом деле, если бы $a_1(z)$ делилось на $(z-\alpha)^k$, то $b(z)$ делилось бы на $(z-\alpha)$. Таким образом, кратность корня α для многочлена $a_0'(z)$ есть $k-1$. ■

В частности, если α — простой корень многочлена $a_0(z)$, то α не будет корнем многочлена $a_0'(z)$.

Таким образом, если $a_0(z)$ имеет разложение (5), то общим наибольшим делителем многочленов $a_0(z)$ и $a_0'(z)$ является многочлен

$$c(z) = (z-\alpha_1)^{k_1-1}(z-\alpha_2)^{k_2-1} \dots (z-\alpha_q)^{k_q-1}.$$

Отсюда видно, что многочлен $a_0(z)$ делится на многочлен $c(z)$ и частное имеет вид

$$\frac{a_0(z)}{c(z)} = (z - \alpha_1)(z - \alpha_2) \dots (z - \alpha_q).$$

Таким образом, сформулированная в начале параграфа задача о нахождении многочлена $g(z)$, имеющего те же самые корни, что и многочлен $f(z)$, но только кратности 1, решена.

§ 10. Подсчет числа действительных корней многочлена на заданном отрезке

Нахождение комплексных корней многочлена является задачей более сложной, чем нахождение его действительных корней, так как в случае комплексного корня нам приходится фактически решать уравнение с двумя неизвестными, которыми являются действительная часть корня и его коэффициент при мнимой части.

Поскольку в предыдущем параграфе приведен способ, позволяющий свести вычисление корней многочлена к вычислению корней многочлена, имеющего только простые корни, то мы займемся здесь именно этим случаем простых корней. Здесь будет дан результат, позволяющий

в значительной степени облегчить приближенное вычисление действительных корней многочлена.

Будем рассматривать многочлен $a_0(x)$ действительного переменного x, имеющего только простые корни, и дадим способ определения числа этих корней на заданном отрезке $\xi_0 \leqslant x \leqslant \xi_1$. Так как все корни многочлена $a_0(x)$ простые, то многочлены $a_0(x)$ и $a_1(x) = a_0'(x)$ не имеют общих корней и ни для какого значения x не могут одновременно обращаться в нуль.

Для решения этой задачи рассмотрим последовательность действительных чисел

$$a_0, a_1, a_2, \ldots, a_n. \tag{19}$$

Будем считать, что ни одно из этих чисел не обращается в нуль. Почти что само собой понятно, что значит число перемен знака в этой последовательности (19). Определим его формально. Мы будем считать, что

Перемена знака между числами

> между a_0 и a_1 имеется перемена знака, если одно из этих чисел положительно, а другое отрицательно.

Обозначим через p_1 в этом случае число 1. Если же числа a_0 и a_1 либо оба положительные, либо оба отрицательные, то будем считать, что перемены знака между ними нет. В этом случае обозначим через p_1 число, равное нулю. Точно так же определим число p_2, которое оценивает перемену знака между a_1 и a_2. Таким образом,

мы получим последовательность нулей и единиц

$$p_1, p_2, \ldots, p_n.$$

Сумма всех чисел из этой последовательности есть число перемен знака последовательности (19).

Исходя из многочленов $a_0(x)$ и $a_1(x)=a_0'(x)$, путем последовательного деления построим последовательность многочленов.

Разделим многочлен $a_0(x)$ на многочлен $a_1(x)$ и запишем формулу (2) в виде

$$a_0(x) = h_1(x)a_1(x) - a_2(x).$$

Разделим теперь многочлен $a_1(x)$ на многочлен $a_2(x)$ и запишем формулу (2) в виде

$$a_1(x) = h_2(x)a_2(x) - a_3(x).$$

На k-м шаге этого процесса мы получим тождество

$$a_{k-1}(x) = h_k(x)a_k(x) - a_{k+1}(x). \qquad (20)$$

Продолжая этот процесс до конца, мы придем к последовательности многочленов

$$a_0(x),\ a_1(x),\ \ldots,\ a_n(x). \qquad (21)$$

Процесс построения этой последовательности почти в точности совпадает с процессом нахождения наибольшего общего делителя двух многочленов. Так как многочлены $a_0(x)$ и $a_n(x)$ взаимно просты, то последний член последовательности, а именно $a_n(x)$, есть число.

Заметим прежде всего, что ни при каком значении $x = x_0$ два рядом стоящие многочлена последовательности (21) не могут обращаться в нуль. В самом деле, если $a_k(x_0) = a_{k+1}(x_0) = 0$, то из соотношения (20) следует, что $a_{k-1}(x_0) = 0$.

Продолжая этот процесс, мы придем к выводу, что многочлены $a_0(x)$ и $a_1(x)$ обращаются в нуль при $x = x_0$, а это невозможно, так как они не имеют общих корней.

Пусть теперь x возрастает, начиная от значения ξ_0 и кончая ξ_1. Ясно, что при таком росте x число перемен знака последовательности чисел (21) может измениться. А это может произойти только при прохождении x через такое значение x_0, при котором один из членов последовательности (21) меняет знак, т. е. проходит через нуль. Допустим, что при $x = x_0$ мы имеем $a_k(x_0) = 0$ и при росте x вблизи точки x_0 знак функции $a_k(x)$ меняется. Полагая в соотношении (20) $x = x_0$, получим равенство

$$a_{k-1}(x_0) = -a_{k+1}(x_0).$$

Таким образом, числа $a_{k-1}(x_0)$ и $a_{k+1}(x_0)$ имеют противоположные знаки. Если при x, близком к x_0, число $a_k(x)$ имеет знак, совпадающий со знаком $a_{k-1}(x)$, то знаки чисел $a_k(x)$ и $a_{k+1}(x)$ различны. Таким образом, между $a_{k-1}(x)$ и $a_k(x)$ перемены знака нет, а между $a_k(x)$ и $a_{k+1}(x)$ перемена знака есть. Если при прохождении точки x через x_0 знак числа $a_k(x)$ меняется, то для

этого x между $a_{k-1}(x)$ и $a_k(x)$ перемена знака есть, а между $a_k(x)$ и $a_{k+1}(x)$ — нет. Таким образом, устанавливается, что при прохождении точки x через x_0, при котором $a_k(x_0)$ обращается в нуль, число перемен знаков в трехчленной последовательности

$$a_{k-1}(x),\ a_k(x),\ a_{k+1}(x)$$

не меняется. Номер k обладает лишь тем свойством, что у него есть предыдущий номер $k-1$ и последующий $k+1$. Таким образом, число перемен знаков последовательности (21) может измениться лишь тогда, когда при прохождении x через x_0 меняет свой знак либо первый член последовательности (21), либо самый последний. Но последний член не может менять знака, так как это есть константа.

Посмотрим теперь, как меняется число перемен знака последовательности (21), когда в точке x_0 первый член последовательности (21) обращается в нуль. Если при x, близком к x_0, но меньшем x_0, $a_0(x) > 0$, то при прохождении x через точку x_0 функция $a_0(x)$ изменит знак. Но при $x = x_0$ число $a_1(x_0)$ будет иметь отрицательный знак, так как при этом функция $a_0(x)$ убывает, следовательно, производная ее $a_1(x)$ отрицательна. Таким образом, при x, близком к x_0, но меньшем x_0, между $a_0(x)$ и $a_1(x)$ имеется перемена знака, а при x, большем x_0, но близком к x_0, между $a_0(x)$ и $a_1(x)$ перемены знака нет.

Таким образом, при прохождении точки x через x_0, при котором функция $a_0(x)$ обращается в нуль и убывает, перемена знаков между $a_0(x)$ и $a_1(x)$ исчезает. Точно так же устанавливается, что если при переходе через точку x_0 функция $a_0(x)$ возрастает, то перемена знака между $a_0(x)$ и $a_1(x)$ исчезает. Таким образом, установлено, что число перемен знаков последовательности (21) при изменении x может произойти лишь тогда, когда x проходит через корень многочлена $a_0(x)$, при этом каждый раз одна перемена знака исчезает. Следовательно, когда x растет от ξ_0 до ξ_1, в последовательности (21) происходит потеря одной перемены знака при прохождении x через корень многочлена $a_0(x)$. И, следовательно, для нахождения числа корней многочлена $a_0(x)$ между ξ_0 и ξ_1 надо сравнить числовые последовательности

$$a_0(\xi_0),\ a_1(\xi_0),\ \ldots,\ a_n(\xi_0), \tag{22}$$

$$a_0(\xi_1),\ a_1(\xi_1),\ \ldots,\ a_n(\xi_1). \tag{23}$$

Число перемен знаков последовательности (22) может быть лишь больше, чем число перемен знаков последовательности (23).

Число корней многочлена на отрезке

Потеря числа перемен знаков при переходе последовательности (22) *в последовательность* (23) *есть число корней многочлена* $a_0(x)$, *находящихся в промежутке* $\xi_0 \leqslant x \leqslant \xi_1$.

Глава 4

Кватернионы

§ 11. Векторные пространства 71
§ 12. Евклидово векторное пространство . . 85
§ 13. Кватернионы 99
§ 14. Геометрические применения кватернионов 106

Описанию кватернионов я предпосылаю некоторые сведения о векторных пространствах, которые мне понадобятся при изучении кватернионов, так как кватернионы составляют четырехмерное евклидово векторное пространство.

§ 11. Векторные пространства

Последовательность

$$x = (x^1, x^2, \ldots, x^n) \qquad (1)$$

из n действительных чисел, расположенных в определенном порядке, указанном в формуле (1), называется n-мерным вектором.

• **n-мерный вектор**

Совокупность A^n всех n-мерных векторов называется n-мерным векторным пространством.

• **n-мерное векторное пространство**

Координаты вектора

Числа

$$x^1, x^2, \ldots, x^n$$

называются координатами вектора x (см. (1)).

Нулевой вектор

Вектор считается равным нулю и обозначается через 0, если все его координаты равны нулю.

Операции над векторами

Произвольный вектор x из A^n может быть умножен на действительное число α.

Для получения этого произведения каждая координата вектора x должна быть умножена на число α. Таким образом, в виде формулы произведение αx записывается так:

$$\alpha x = (\alpha x^1, \alpha x^2, \ldots, \alpha x^n). \qquad (2)$$

Каждые два вектора, x (см. (1)) и

$$y = (y^1, y^2, \ldots, y^n)$$

из A^n могут быть сложены.

Для этого координаты их следует сложить. В виде формулы это записывается следующим образом:

$$x + y = (x^1 + y^1, x^2 + y^2, \ldots, x^n + y^n). \qquad (3)$$

Если теперь

$$x_1, x_2, \ldots, x_k \qquad (4)$$

— совокупность k векторов пространства A^n, то, пользуясь операциями (2) и (3), можно составить их линейную форму

$$z = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k, \qquad (5)$$

где $\alpha_1, \ldots, \alpha_k$ — действительные числа.

• **Линейная комбинация векторов**

Совокупность из k векторов (4) считается линейно независимой, если вектор, определенный формулой (5), обращается в нуль лишь при условии, что

$$\alpha_1 = 0, \quad \alpha_2 = 0, \quad \ldots, \quad \alpha_k = 0.$$

• **Линейная независимость**

В противном случае, т. е.

если существуют такие числа

$$\alpha_1, \alpha_2, \ldots, \alpha_k, \qquad (6)$$

не все равные нулю, что вектор z, определяемый формулой (5), обращается в нуль, совокупность (4) называется линейно зависимой.

• **Линейная зависимость**

Если к совокупности линейно зависимых векторов (4) прибавить еще несколько векторов

$$x_{k+1}, x_{k+2}, \ldots, x_l,$$

то расширенная совокупность

$$x_1, x_2, \ldots, x_l$$

будет линейно зависимой. Именно, если совокупность коэффициентов (6) осуществляет линейную зависимость векторов (4), то мы имеем соотношение

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k + 0 \cdot x_{k+1} + \ldots + 0 \cdot x_l = 0,$$

причем не все числа последовательности

$$\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_{k+1} = 0, \quad \ldots, \quad \alpha_l = 0$$

равны нулю.

Координатное подпространство

Если в векторном пространстве A^n, состоящем из всех векторов вида (1), рассмотреть те векторы, для которых i-я координата обращается в нуль, то мы получим также векторное пространство A^{n-1}, но размерности $n-1$, которое называется координатным подпространством пространства A^n.

Докажем теперь следующее важное предложение.

А) *Совокупность* (4) *векторов* n*-мерного пространства* A^n *при* $k > n$ *всегда линейно зависима.*

Доказательство. Для доказательства достаточно рассмотреть случай $k = n + 1$. Доказательство будем вести индуктивно. Отметим прежде всего, что для $n = 1$ утверждение А) справедливо. Пусть x, y — два вектора пространства A^1, причем

$$x = (x^1), \quad y = (y^1).$$

Если числа x^1, y^1 равны нулю, то мы имеем соотношение

$$\alpha x + \beta y = 0$$

при произвольных α и β, так что в этом случае векторы x и y линейно зависимы. Если не оба числа x^1, y^1 равны нулю, то мы имеем соотношение

$$y^1 x - x^1 y = 0.$$

Таким образом, при $n = 1$ утверждение А) верно.

Пусть теперь

$$x_1, x_2, \ldots, x_{n+1} \qquad (7)$$

— совокупность из $(n+1)$-го вектора пространства A^n. Сосредоточим внимание на последней координате всех векторов совокупности (7). Если все они равны нулю, то совокупность векторов (7) принадлежит к $(n-1)$-мерному пространству. Согласно предположению индукции совокупность (7) линейно зависима. Допустим теперь, что хотя бы один вектор, например x_{n+1}, имеет последнюю координату, отличную от нуля. Для каждого вектора x_j совокупности (7) при $j \leqslant n$ можно подобрать такое число α_j, что все вектора y_j, определяемые формулой

$$y_j = x_j - \alpha_j x_{n+1}; \quad j = 1, \ldots, n, \qquad (8)$$

имеют последнюю координату, равную нулю, и потому лежат в $(n-1)$-мерном векторном

пространстве. Следовательно, по предположению индукции они линейно зависимы. Таким образом, существует совокупность чисел

$$\beta_1, \beta_2, \ldots, \beta_n$$

(причем не все эти числа равны нулю) такая, что имеется соотношение

$$\beta_1 \boldsymbol{y}_1 + \beta_2 \boldsymbol{y}_2 + \ldots + \beta_n \boldsymbol{y}_n = 0.$$

Из этого и из формулы (8) вытекает:

$$\beta_1 \boldsymbol{x}_1 + \beta_2 \boldsymbol{x}_2 + \ldots + \beta_n \boldsymbol{x}_n - \\ - (\beta_1 \alpha_1 + \beta_2 \alpha_2 + \ldots + \beta_n \alpha_n) \boldsymbol{x}_{n+1} = 0.$$

Таким образом, совокупность векторов (7) линейно зависима. Итак, предложение А) доказано. ■

В) Базис векторного пространства.

Обозначим через $\boldsymbol{e}_i$ вектор из A^n, все координаты которого равны нулю, за исключением одной координаты с номером i, которая равна 1, т. е. положим

$$\boldsymbol{e}_1 = (1, 0, \ldots, 0),$$
$$\boldsymbol{e}_2 = (0, 1, \ldots, 0),$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\boldsymbol{e}_n = (0, 0, \ldots, 1).$$

Ясно, что вектор $\boldsymbol{x}$ (см. (1)) записывается в виде

$$\boldsymbol{x} = x^1 \boldsymbol{e}_1 + x^2 \boldsymbol{e}_2 + \ldots + x^n \boldsymbol{e}_n,$$

причем коэффициенты $x^1, x^2, \ldots, x^n$, входящие в эту формулу, однозначно определены вектором x. Таким образом,

• **Базис векторного пространства**

каждый вектор x в векторном пространстве A^n выражается в виде линейной формы относительно векторов

$$e_1, e_2, \ldots, e_n, \qquad (9)$$

причем коэффициенты этой линейной формы определены однозначно. Система векторов, обладающая этим свойством, называется базисом векторного пространства A^n.

Построенный нами базис (9) *не является единственным.*

Доказательство. Оказывается, что любая линейно независимая система векторов

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n, \qquad (10)$$

содержащая n векторов пространства A^n, является базисом этого пространства.

Действительно, пусть x — произвольный вектор пространства A^n. Тогда векторы

$$x, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$$

линейно зависимы, поскольку содержат $n + 1$ вектор (см. А)). Таким образом, мы имеем соотношение

$$\alpha x + \alpha_1 \varepsilon_1 + \alpha_2 \varepsilon_2 + \ldots + \alpha_n \varepsilon_n = 0, \qquad (11)$$

причем в этом соотношении не все коэффициенты равны нулю. В частности, коэффициент α не может быть равен нулю, так как если бы он был равен нулю, то оказалось бы, что векторы системы (10) линейно зависимы. Пользуясь этим, разделим соотношение (11) на величину $-\alpha$. Для того чтобы не вводить новые обозначения, будем считать, что $\alpha = -1$, а остальные коэффициенты сохраним. Таким образом, получаем

Разложение вектора по базису

$$\boxed{x = \alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 + \ldots + \alpha_n\varepsilon_n.} \qquad (12)$$

Если бы вектор x мог быть записан аналогично через систему (10), но с другими коэффициентами, т. е. имело бы место соотношение

$$x = \beta_1\varepsilon_1 + \beta_2\varepsilon_2 + \ldots + \beta_n\varepsilon_n,$$

то, вычитая последнее соотношение из соотношения (12), мы получили бы соотношение

$$(\alpha_1 - \beta_1)\varepsilon_1 + (\alpha_2 - \beta_2)\varepsilon_2 + \ldots$$
$$\ldots + (\alpha_n - \beta_n)\varepsilon_n = 0,$$

что ввиду линейной независимости векторов системы (10) приводит к равенству $\alpha_i = \beta_i$, $i = 1, \ldots, n$. ■

C)

• Дополнение системы векторов до базиса

Пусть

$$x_1, x_2, \ldots, x_p \qquad (13)$$

— некоторая линейно независимая система векторов из A^n. Если $p < n$, то систему (13) можно дополнить векторами $x_{p+1}, \ldots, x_n$ так, что система

$$x_1, x_2, \ldots, x_p, x_{p+1}, \ldots, x_n$$

линейно независима.

Доказательство. Если C) неверно, то, присоединяя к системе (13) вектор e_1 (см. B)), мы получим линейно зависимую расширенную систему

$$e_1, x_1, \ldots, x_p.$$

Вектор e_1 — ненулевой. Поэтому найдется вектор x_q, линейно выражающийся через остальные векторы расширенной системы. Исключим его из расширенной системы. Тогда любой вектор из A^n можно линейно выразить через оставшиеся векторы расширенной системы. Добавив к оставшимся векторам расширенной системы вектор e_2, мы получим линейно зависимую систему, из которой можно исключить один из векторов

$$x_1, \ldots, x_{q-1}, x_{q+1}, \ldots, x_p.$$

Продолжая этот процесс, мы исключим из расширенной системы все векторы (13) и придем

к выводу, что любой вектор из A^n линейно выражается через векторы $e_1, \ldots, e_p$, что неверно. Следовательно, утверждение C) справедливо. ■

Из предложения B) видно, что данное в начале при помощи координат вектора (см. (1)) определение n-мерного векторного пространства A^n не является инвариантным, так как оно зависит от случайно выбранного базиса (9), а базисов в пространстве A^n существует бесчисленное множество. Поэтому мы дадим другое инвариантное определение n-мерного векторного пространства A^n.

D)

Инвариантное определение n-мерного векторного пространства

Векторным пространством называется множество A элементов, в котором определены две операции — сложение и умножение на действительные числа, причем выполнено условие: если α и β — два числа, а x и y — два элемента пространства A, т. е. два вектора, то имеют место соотношения

$$(\alpha+\beta)x = \alpha x + \beta x,$$

$$\alpha(x+y) = \alpha x + \alpha y.$$

При помощи операций, имеющихся в векторном пространстве A, можно составить линейную комбинацию произвольной системы из векторов

$$x_1, \ldots, x_n,$$

т. е. построить вектор

$$z = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

где $\alpha_1, \ldots, \alpha_n$ — действительные числа.

Таким образом, можно ввести понятие линейной зависимости векторов и линейной независимости, как это было сделано раньше (см. В)).

• **Размерность векторного пространства**

Если в векторном пространстве A имеется n линейно независимых векторов, но нет $n+1$ линейно независимого вектора, то считается, что векторное пространство A имеет размерность n и обозначается через A^n.

Выбирая в пространстве A^n n линейно независимых векторов, мы получим базис и при помощи него — координатную запись любого вектора.

Е) Векторное подпространство.

• **Векторное подпространство**

Пусть A — векторное пространство и пусть B — такое подмножество его векторов, что наряду с двумя векторами x и y из B в B входит также $x + y$, а наряду с вектором x в B входит и его произведение на произвольное действительное число, т. е. вектор αx. Тогда B, очевидно, представляет собой векторное пространство в силу тех операций, которые имеются в A. Множество B называется векторным подпространством пространства A.

Размерность векторного подпространства

Если векторное пространство A имеет конечную размерность n, то его подпространство B имеет размерность, не превосходящую n.

Разложение ВП в прямую сумму подпространств

F) *Пусть A^n — n-мерное векторное пространство, а B^p и C^q — два его векторных подпространства размерности p и q соответственно. Если векторные подпространства B^p и C^q имеют единственный общий вектор нуль, а $p+q=n$, то векторное пространство A^n распадается в прямую сумму своих векторных подпространств B^p и C^q. Именно, каждый вектор x из A^n представляется в виде суммы*

$$x = y + z,$$

где y — вектор из B^p, а z — вектор из C^q, причем слагаемые y и z однозначно определены вектором x.

Доказательство. Для доказательства этого утверждения выберем в подпространстве B^p базис

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p, \tag{14}$$

состоящий из p элементов, а в подпространстве C^q — базис

$$\varepsilon_{p+1}, \varepsilon_{p+2}, \ldots, \varepsilon_n, \tag{15}$$

состоящий из q элементов. Объединяя совокупность векторов (14) и (15), получим совокупность

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n. \tag{16}$$

Докажем, что совокупность эта составляет базис пространства A^n. Так как число векторов системы (16) равно размерности пространства A^n, то достаточно доказать, что векторы системы (16) линейно независимы. Допустим, что имеет место противоположное. Именно, имеет место соотношение

$$\alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 + \ldots + \alpha_p\varepsilon_p + \\ + \alpha_{p+1}\varepsilon_{p+1} + \ldots + \alpha_n\varepsilon_n = 0, \qquad (17)$$

причем не все коэффициенты, входящие в это соотношение, равны нулю. Обозначая через y сумму первых p членов суммы (17) и через z — сумму остальных членов этой суммы, получаем два вектора y и z, причем оба они одновременно не могут обращаться в нуль, так что хотя бы один из них отличен от нуля. При этом соотношение (17) переписывается в виде

$$y + z = 0,$$

или, иначе,

$$y = -z,$$

где $y \in B^p$, $-z \in C^q$.

Таким образом, мы приходим к выводу, что векторные подпространства B^p и C^q имеют общий вектор, отличный от нуля, что противоречит нашему предположению.

Таким образом, система (16) является базисом пространства A^n и каждый вектор x из A^n

может быть записан в виде

$$x = \alpha_1 \varepsilon_1 + \ldots + \alpha_p \varepsilon_p + \alpha_{p+1} \varepsilon_{p+1} + \ldots + \alpha_n \varepsilon_n.$$

Обозначая через y сумму первых p слагаемых последней суммы, а через z — сумму остальных слагаемых, мы приходим к выводу, что

$$x = y + z,$$

где $y \in B^p$, $z \in C^q$. Таким образом, утверждение F) доказано. ■

G)

Линейное отображение

Пусть X и Y — два векторных пространства и f — отображение, ставящее в соответствие каждому вектору $x \in X$ некоторый вектор $f(x) \in Y$, удовлетворяющее следующим условиям:

$$f(x_1 + x_2) = f(x_1) + f(x_2),$$
$$f(\alpha x) = \alpha f(x),$$

где α — произвольное действительное число. Такое отображение f векторного пространства X называется линейным.

Говорят, что отображение есть отображение пространства X на пространство Y, вместо того, чтобы сказать, что есть отображение в пространство Y, в случае, если в каждый элемент пространства Y переходит хоть один элемент пространства X.

Отображение f называется изоморфным, если в нуль пространства Y переходит только нуль пространства X, т. е. если из соотношения $f(x) = 0$ следует, что $x = 0$.

• **Изоморфное отображение**

В этом случае f есть взаимно однозначное отображение пространства X на векторное подпространство $f(X)$ пространства Y.

Доказательство. В самом деле, два различных вектора x_1 и x_2 пространства X не могут перейти в один и тот же вектор пространства Y, так как тогда их разность $x_1 - x_2 \neq 0$ переходила бы в нуль пространства Y. ■

§ 12. Евклидово векторное пространство

Векторное пространство A^n называется евклидовым, если в нем определено скалярное произведение.

• **Евклидово пространство**

А) Говорят, что

в векторном пространстве A^n определено скалярное произведение, если каждой паре векторов x и y этого пространства поставлено в соответствие действительное число,

• **Скалярное произведение**

которое обозначается (x, y) и называется скалярным произведением векторов x и y, причем выполнены условия симметрии и линейности. Условие симметрии:

$$(x, y) = (y, x). \qquad (18)$$

Условие линейности: если x_1 и x_2 — два вектора из пространства A^n, α — действительное число, то имеют место соотношения

$$(x_1 + x_2, y) = (x_1, y) + (x_2, y),$$
$$(\alpha x, y) = \alpha(x, y).$$

Так как имеет место симметрия, то

линейность выполнена и по второму вектору y.

Именно:

$$(x, y_1 + y_2) = (x, y_1) + (x, y_2),$$
$$(x, \beta y) = \beta(x, y).$$

Пусть

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$$

— некоторый базис пространства A^n, так что

$$x = x^1\varepsilon_1 + x^2\varepsilon_2 + \ldots + x^n\varepsilon_n,$$
$$y = y^1\varepsilon_1 + y^2\varepsilon_2 + \ldots + y^n\varepsilon_n.$$

Положим

$$(\varepsilon_i, \varepsilon_j) = g_{i,j}.$$

В силу симметрии (см. (18)) мы имеем

$$g_{i,j} = g_{j,i}.$$

В силу линейности мы имеем

$$(x, y) = \sum_{i,j=1}^{n} x^i y^j g_{i,j} = \sum_{i,j=1}^{n} g_{i,j} x^i y^j. \qquad (19)$$

• **Координатная запись скалярного произведения**

Это есть координатная запись скалярного произведения. На скалярное произведение (x, y) накладывается еще одно очень важное условие.

Скалярный квадрат вектора, т. е. его скалярное произведение самого на себя, считается квадратом его длины и потому всегда больше или равно нулю и обращается в нуль лишь при $x = 0$:

$$(x, x) \geqslant 0; \quad \textit{если} \quad (x, x) = 0, \quad \textit{то} \quad x = 0.$$

Длину вектора x обозначают через $|x|$, так что

$$|x|^2 = (x, x).$$

• **Длина вектора**

Оказывается, что,

зная так определенную длину каждого вектора пространства A^n, *можно вычислить скалярное произведение двух любых векторов этого пространства.*

Доказательство. В силу симметрии и линейности мы имеем

$$(x + y, x + y) = (x, x) + 2(x, y) + (y, y).$$

Таким образом, получаем

$$(x, y) = \frac{1}{2}\left(|x + y|^2 - |x|^2 - |y|^2\right). \quad (20)$$

■

Здесь слева стоит скалярное произведение (x, y) двух произвольных векторов пространства A^n, а справа — длины трех различных векторов, которые по предположению известны.

B)

Ортонормальность системы векторов

Система векторов

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p \quad (21)$$

называется ортонормальной, если имеет место соотношение

$$(\varepsilon_j, \varepsilon_j) = \begin{cases} 1, & i = j; \\ 0, & i \neq j; \end{cases} \qquad i, j = 1, \ldots, p. \quad (22)$$

Таким образом, каждые два различные вектора системы (21) ортогональны между собой, а длина каждого вектора (21) равна единице.

Ортонормальная система (21) *всегда линейно независима.*

• **Линейная независимость ортонормальной системы**

Доказательство. Действительно, если имеет место соотношение

$$\alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 + \ldots + \alpha_p\varepsilon_p = 0,$$

то, умножая это соотношение скалярно на ε_i, получаем $\alpha_i = 0$. Таким образом, если $p = n$, то система (21) является ортонормальным базисом

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \qquad (23)$$

пространства A^n. ■

В случае ортонормального базиса (23) скалярное произведение (19) в координатной форме записывается в виде

$$(x, y) = \sum_{i=1}^{n} x^i y^i.$$

Базис (23), удовлетворяющий условию (22), называется ортонормальным потому, что, во-первых, каждые два различных его вектора ортогональны между собой, во-вторых, он нормирован, т. е. длина каждого его вектора равна единице.

• **Ортонормальный базис**

С) *Каждая линейно независимая система векторов*

$$x_1, x_2, \ldots, x_p \qquad (24)$$

однозначно определяет ортонормальную систему векторов

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p. \tag{25}$$

Ортонормирование системы векторов

Процесс перехода от системы векторов (24) к системе векторов (25) называется ортонормированием.

Опишем его.

Так как система векторов (24) линейно независима, то вектор $x_1 \neq 0$ и, следовательно, его длина $|x_1| \neq 0$. Мы полагаем

$$\varepsilon_1 = \frac{x_1}{|x_1|}.$$

Далее, полагаем

$$\varepsilon_2' = x_2 - (x_2, \varepsilon_1)\varepsilon_1.$$

Мы имеем

$$(\varepsilon_2', \varepsilon_1) = (x_2, \varepsilon_1) - (x_2, \varepsilon_1) = 0.$$

Таким образом, векторы ε_1 и ε_2' ортогональны между собой. При этом вектор $\varepsilon_2' \neq 0$, так как векторы x_1 и x_2 — линейно независимы, а следовательно, линейно независимы векторы ε_1 и ε_2'. Теперь нормируем вектор ε_2'. Именно, положим

$$\varepsilon_2 = \frac{\varepsilon_2'}{|\varepsilon_2'|}.$$

Таким образом, получаем

$$(\varepsilon_2, \varepsilon_2) = 1.$$

Пусть $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_i$ уже построены так, что они составляют ортонормальную систему. Построим вектор ε'_{i+1}. Положим

$$\varepsilon'_{i+1} = x_{i+1} - (x_{i+1}, \varepsilon_1)\varepsilon_1 - \\ - (x_{i+1}, \varepsilon_2)\varepsilon_2 - \ldots - (x_{i+1}, \varepsilon_i)\varepsilon_i.$$

Прежде всего вектор $\varepsilon'_{i+1} \neq 0$, так как из линейной независимости векторов $x_1, x_2, \ldots, x_{i+1}$ следует линейная независимость векторов

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_i, x_{i+1}.$$

Умножая вектор ε'_{i+1} на произвольный вектор ε_j, $j \leqslant i$, получаем

$$(\varepsilon'_{i+1}, \varepsilon_j) = 0.$$

Таким образом, построенный вектор ε'_{i+1} ортогонален ко всем векторам $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_i$ и отличен от нуля. Нормируя вектор ε'_{i+1}, т. е. полагая

$$\varepsilon_{i+1} = \frac{\varepsilon'_{i+1}}{|\varepsilon'_{i+1}|},$$

мы получаем вектор ε_{i+1}. Таким образом, индуктивное построение ортонормированной системы (25) проведено. Заметим, что переход от системы (24) к системе (25) является непрерывным. Это значит, что при непрерывном изменении системы (24) соответствующая система (25) также меняется непрерывно.

D) *Каждое векторное подпространство B^p евклидова векторного пространства A^n само естественным образом является евклидовым векторным пространством.*

Доказательство. Действительно, каждая пара векторов из B^p является парой векторов из A^n и потому для нее определено скалярное произведение. ■

Вектор z пространства A^n, ортогональный каждому вектору из подпространства B^p, считается ортогональным ко всему пространству B^p. Обозначим через C совокупность всех векторов пространства A^n, ортогональных векторному подпространству B^p. Оказывается, что C является векторным подпространством пространства A^n размерности $q = n - p$, причем векторное пространство A^n распадается в прямую сумму своих подпространств B^p и $C = C^q$.

Ортогональное дополнение подпространства

Подпространство C^q называется ортогональным дополнением подпространства B^p.

Теорема об ортогональном дополнении

Оказывается, что

подпространство B^p является ортогональным дополнением подпространства C^q.

Доказательство. Для доказательства данного утверждения выберем в евклидовом векторном пространстве B^q ортонормальный базис

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p.$$

Данную систему векторов дополним до максимальной линейно независимой системы векторами $x_{p+1}, \ldots, x_n$ (см. § 11 С)). Тогда мы получим максимальную линейно независимую систему

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p, x_{p+1}, \ldots, x_n.$$

Теперь подвергнем эту систему процессу ортонормирования (см. С)). При этом первые p векторов $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ не изменятся, а векторы $x_{p+1}, x_{p+2}, \ldots, x_n$ заменятся другими векторами. Вновь полученную систему запишем в виде

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p, \varepsilon_{p+1}, \ldots, \varepsilon_n.$$

Последняя система является ортонормальным базисом пространства A^n, так что каждый вектор x пространства A^n записывается в виде

$$x = x^1\varepsilon_1 + \ldots + x^p\varepsilon_p + x^{p+1}\varepsilon_{p+1} + \ldots + x^n\varepsilon_n.$$

Для того чтобы вектор x был нормальным ко всему пространству B^p, необходимо, чтобы он был нормальным к каждому вектору ε_i, $i = 1, \ldots, p$. Таким образом, должно быть выполнено условие

$$(x, \varepsilon_i) = 0; \quad i = 1, \ldots, p.$$

Из последнего условия вытекает

$$x^1 = 0, \quad \ldots, \quad x^p = 0.$$

Таким образом, вектор z, нормальный ко всему пространству B^p, записывается в виде

$$z = x^{p+1}\varepsilon_{p+1} + \ldots + x^n\varepsilon_n.$$

Совокупность всех векторов такого вида составляет векторное подпространство C^q пространства A^n размерности $q = n - p$, которое является ортогональным дополнением подпространства B^p. ■

Ясно, что подпространство B^p, в свою очередь, является ортогональным дополнением подпространства C^q.

Дадим геометрическое описание скалярного произведения двух векторов пространства A^n.

Е) Пусть

$$x, y$$

— два линейно независимых вектора пространства A^n. Совокупность всех векторов

$$u = \alpha x + \beta y,$$

где α и β — произвольные действительные числа, составляет двумерное векторное подпространство A^2 векторного пространства A^n. Пространство A^2 является векторным двумерным евклидовым пространством, иначе говоря, евклидовой плоскостью. Таким образом, векторы x и y являются линейно независимыми векторами плоскости A^2, и ясно, что такое угол между ними. Обозначим его через φ. Оказывается, что

Геометрическое описание скалярного произведения

скалярное произведение векторов x и y выражается в следующем виде:

$$(x, y) = |x| \cdot |y| \cos \varphi. \qquad (26)$$

Доказательство. Для доказательства формулы (26) ортонормируем пару векторов x, y. Мы получим два вектора

$$\varepsilon_1, \varepsilon_2,$$

составляющих базис двумерного евклидова пространства A^2. При этом

$$\begin{aligned} x &= |x|\varepsilon_1; \\ y &= |y|(\varepsilon_1 \cos\varphi + \varepsilon_2 \sin\varphi). \end{aligned} \tag{27}$$

Отсюда получаем

$$\begin{aligned} (x, y) &= \big(|x|\varepsilon_1,\ |y|(\varepsilon_1 \cos\varphi + \varepsilon_2 \sin\varphi)\big) = \\ &= |x| \cdot |y| \cos\varphi. \end{aligned}$$

Таким образом, формула (26) доказана. В случае, если x и y линейно зависимы, то следует считать, что угол φ между ними равен нулю или π. При этом оба они выражаются через один и тот же вектор:

$$\begin{aligned} x &= |x|\varepsilon_1; \\ y &= \pm|y|\varepsilon_1. \end{aligned}$$

Тогда мы имеем

$$(x, y) = |x| \cdot |y| \cos 0$$

или

$$(x, y) = |x| \cdot |y| \cos\pi.$$

Таким образом, формула (26) имеет место для любых двух векторов x и y из A^n. ■

F)

Векторное произведение

Пусть A^3 — евклидово векторное пространство размерности 3 и

$$\varepsilon_1, \varepsilon_2, \varepsilon_3 \tag{28}$$

— его ортонормальный базис. Определим векторное произведение

$$z = [x, y]$$

двух векторов

$$x = x^1\varepsilon_1 + x^2\varepsilon_2 + x^3\varepsilon_3,$$
$$y = y^1\varepsilon_1 + y^2\varepsilon_2 + y^3\varepsilon_3.$$

Зададим координаты z^1, z^2, z^3 вектора z в базисе (28) с помощью формул:

$$\begin{aligned} z^1 &= x^2y^3 - x^3y^2, \\ z^2 &= x^3y^1 - x^1y^3, \\ z^3 &= x^1y^2 - x^2y^1. \end{aligned} \tag{29}$$

Инвариантность этого определения векторного произведения относительно выбора базиса (28) мы рассмотрим позже (см. § 14). Здесь отметим только, что

$$[x, y] = -[y, x]; \quad [x, x] = 0.$$

Вычислим векторное произведение z, пользуясь формулами (27). Для этого выберем ортонормальный базис пространства A^3 специальным

образом — так, чтобы векторы x и y записывались при помощи формул (27), и вычислим векторное произведение z, пользуясь этими формулами. Из них и из формул (29) вытекает:

$$z^1 = 0, \quad z^2 = 0, \quad z^3 = |x| \cdot |y| \sin \varphi,$$

где φ — угол между векторами x и y. Таким образом,

векторное произведение векторов x и y ортогонально к ним и его модуль равен произведению модулей $|x|$ и $|y|$ на модуль синуса угла между ними, а направление его определяется углом φ.

G)

• **Изоморфизм евклидовых векторных пространств**

Отображение ψ евклидова векторного пространства A^n на евклидово векторное пространство $\widehat{A}^n$ называется изоморфным, если оно линейно (см. § 11 G)) и сохраняет скалярное произведение, т. е. если для любых двух векторов x и y из A^n имеет место формула

$$(\psi(x), \psi(y)) = (x, y). \qquad (30)$$

Заметим, что в силу формулы (20) сохранение скалярного произведения вытекает из сохранения длины векторов при отображении ψ. Именно, если для любого вектора $x \in A^n$ имеет

место соотношение

$$|\psi(x)| = |x|,$$

то при отображении ψ сохраняется и скалярное произведение (см. (30)). Пусть ψ_t — изоморфное отображение евклидова векторного пространства A^n самого на себя, непрерывно зависящее от параметра t, меняющегося в пределах $0 \leqslant t \leqslant 1$, причем ψ_0 есть тождественное отображение A^n на себя, т. е. выполнено условие

$$\psi_0(x) = x.$$

Таким образом, отображение ψ_1 получается из тождественного отображения путем непрерывного его изменения или, иначе говоря, путем его непрерывной деформации.

Вращение евклидова пространства

Изоморфное отображение евклидова векторного пространства самого на себя, которое получается путем непрерывной деформации тождественного отображения φ_0, называется вращением евклидова векторного пространства A^n.

Следует отметить, что

не всякое изоморфное отображение евклидова векторного пространства самого на себя может быть получено путем вращения.

Это будет доказано в § 14.

В евклидовом векторном пространстве определено расстояние $\rho(x, y)$ между каждыми двумя его точками x и y, или, что то же самое, между любыми двумя векторами с концами x и y, выходящими из начала координат. Оно задается формулой

$$\rho(x, y) = |x - y|. \tag{31}$$

• **Расстояние между двумя точками A_n**

§ 13. Кватернионы*

Комплексные числа играют в математике огромную роль. В связи с этим возникло желание дать дальнейшее обобщение действительных чисел. На этом пути были построены кватернионы, роль которых в математике оказалась незначительной.

Уильям Роуан Гамильтон (1805–1865)

Кватернионы получаются в результате присоединения к действительным числам не одной, а трех мнимых единиц, которые обозначаются через

$$i, j, k, \tag{32}$$

* Система кватернионов предложена в 1843 г. У. Гамильтоном (W. Hamilton) (Мат. энциклопедия. Т. 2. М., 1979).

так что каждый кватернион x записывается в форме

$$x = x^0 + x^1 i + x^2 j + x^3 k, \qquad (33)$$

где

$$x^0, x^1, x^2, x^3$$

— действительные числа, являющиеся координатами кватерниона x.

Таким образом,

совокупность K^4 всех кватернионов представляет собой четырехмерное векторное пространство с базисом

$$1, i, j, k.$$

Если считать этот базис ортонормальным, то векторное пространство K^4 становится евклидовым четырехмерным пространством.

Сумма кватернионов

Сумма кватернионов

$$x = x^0 + x^1 i + x^2 j + x^3 k$$

и

$$y = y^0 + y^1 i + y^2 j + y^3 k$$

определяется как сумма векторов, т. е. задается формулой

$$x + y = x^0 + y^0 + (x^1 + y^1)i + \\ + (x^2 + y^2)j + (x^3 + y^3)k.$$

Кватернион x превращается в действительное число x^0, если его координаты x^1, x^2, x^3 равны нулю. Таким образом, в множестве K^4 всех кватернионов содержится действительная ось D, состоящая из действительных кватернионов. Действительное число x^0 считается действительной частью кватерниона x (33). Все кватернионы x, для которых $x^0 = 0$, считаются чисто мнимыми. Они составляют трехмерное подпространство I пространства K^4. Пространства I и D являются взаимно ортогональными дополнениями. В соответствии с этим запишем кватернион x в виде

• **Действительная и мнимая части кватерниона**

$$x = x^0 + \hat{x},$$

где $\hat{x} = x^1 i + x^2 j + x^3 k$. При этом x^0 — действительная часть кватерниона, а $\hat{x}$ — его мнимая часть. Точно так же запишем кватернион y, положив

$$y = y^0 + \hat{y},$$

где $\hat{y} = y^1 i + y^2 j + y^3 k$.

• **Сопряженный кватернион**

Кватернион $\bar{x}$, сопряженный к кватерниону x, определяется формулой

$$\bar{x} = x^0 - \hat{x}.$$

Аналогично

$$\bar{y} = y^0 - \hat{y}.$$

Перейдем теперь к описанию правил умножения кватернионов. Будем считать, что при перемножении координаты кватерниона, являющиеся действительными числами, перестановочны с мнимыми единицами (32). После этого остается задать лишь правила перемножения мнимых единиц (32). Они суть следующие:

$$i^2 = j^2 = k^2 = -1; \tag{34}$$

Правила перемножения мнимых единиц

$$\begin{aligned} ij &= -ji = k; \\ jk &= -kj = i; \\ ki &= -ik = j. \end{aligned} \tag{35}$$

Пользуясь этими правилами, перемножим сначала чисто мнимые кватернионы $\widehat{x}$ и $\widehat{y}$. Мы имеем:

$$\widehat{x}\widehat{y} = -\left(x^1y^1 + x^2y^2 + x^3y^3\right) + \left(x^2y^3 - x^3y^2\right)i + \\ + \left(x^1y^3 - x^3y^1\right)j + \left(x^1y^2 - x^2y^1\right)k.$$

Вспоминая правила скалярного и векторного перемножения (см. § 12 B), F)) векторов $\widehat{x}$ и $\widehat{y}$ трехмерного евклидова пространства I, мы можем переписать эту формулу в виде

Произведение кватернионов

$$\widehat{x}\widehat{y} = -(\widehat{x}, \widehat{y}) + [\widehat{x}, \widehat{y}]. \tag{36}$$

Пользуясь этой формулой, произведение кватернионов x и y можно записать в следующем виде:

$$xy = x^0y^0 - (\widehat{x}, \widehat{y}) + x^0\widehat{y} + y^0\widehat{x} + [\widehat{x}, \widehat{y}]. \quad (37)$$

Выпишем теперь произведение кватерниона x и сопряженного кватерниона $\bar{x}$. Мы имеем

• **Произведение сопряженных кватернионов**

$$x\bar{x} = (x^0)^2 + (\widehat{x}, \widehat{x}) = (x, x) = |x|^2. \quad (38)$$

Таким образом,

произведение $x\bar{x}$ есть скалярный квадрат вектора x в евклидовом пространстве K^4.

Из этого следует, что

• **Обратный кватернион**

каждый кватернион x, отличный от нуля, имеет обратный кватернион x^{-1}, удовлетворяющий условию

$$xx^{-1} = x^{-1}x = 1,$$

причем

$$x^{-1} = \frac{\bar{x}}{|x|^2}. \quad (39)$$

Пользуясь формулой (37), выпишем теперь произведение кватернионов $\bar{y}, \bar{x}$. Мы имеем:

$$\bar{y}\,\bar{x} = x^0y^0 - (\widehat{x}, \widehat{y}) - x^0\widehat{y} - y^0\widehat{x} - [\widehat{x}, \widehat{y}].$$

Из этой формулы следует важная формула

Сопряженное произведению кватернионов

$$\boxed{\overline{xy} = \bar{y}\,\bar{x}.} \tag{40}$$

Докажем теперь, что

Модуль произведения кватернионов

$$\boxed{|xy| = |x| \cdot |y|.} \tag{41}$$

Действительно, в силу формулы (38)

$$|xy|^2 = xy\,\overline{xy} = xy\,\bar{y}\,\bar{x} = \\ = x|y|^2\bar{x} = x\bar{x}|y|^2 = |x|^2|y|^2.$$

Из формулы (38) следует, что если модуль кватерниона ε равен 1, то

$$\varepsilon^{-1} = \bar{\varepsilon}. \tag{42}$$

Совокупность всех кватернионов, по модулю равных 1, обозначим через H. Множество H представляет собой трехмерную сферу в пространстве K^4 радиуса 1 с центром в нуле.

Заметим, что

каждый кватернион a, по модулю равный 1, *может быть записан в форме*

$$\boxed{a = \cos\alpha + (\sin\alpha)u,} \tag{43}$$

где α есть угол, удовлетворяющий условию $|\alpha| \leqslant \pi$, а u — чисто мнимый кватернион,

по модулю равный единице; и наоборот, каждый кватернион, записанный в форме (43), *имеет модуль, равный единице.*

Доказательство. Докажем формулу (43). Так как пространство K^4 распадается в прямую сумму своих подпространств D и I, то

$$a = \xi + \eta u,$$

где ξ, η — действительные числа, а u — чисто мнимый кватернион, по модулю равный единице. Далее,

$$1 = |a|^2 = a\bar{a} = (\xi + \eta u)(\xi - \eta u) = \\ = \xi^2 - \eta^2 u^2 = \xi^2 + \eta^2.$$

Следовательно, $\xi^2 + \eta^2 = 1$ и найдется такой угол α, $|\alpha| \leqslant \pi$, что $\xi = \cos\alpha$, $\eta = \sin\alpha$. Таким образом, формула (43) доказана. ■

Так как кватернионы складываются как векторы, то мы имеем

$$|x + y| \leqslant |x| + |y|. \qquad (44)$$

Оказывается, что

• **Непрерывность операций сложения и умножения кватернионов**

операции сложения и умножения, имеющиеся для кватернионов, непрерывны. Именно, если кватернион x' мало отличается от кватерниона x, а кватернион y' мало отличается от кватерниона y, то кватернион $x' + y'$ мало отличается от кватерниона $x + y$, а кватернион $x'y'$ мало отличается от кватерниона xy.

Доказательство. Мы имеем:

$$(x' + y') - (x + y) = (x' - x) + (y' - y).$$

Так как по предположению $y' - y$ и $x' - x$ — малые кватернионы, то в силу формулы (44) кватернион $(x' + y') - (x + y)$ мал.

Перейдем к умножению. Имеем

$$x'y' - xy = x'y' - x'y + x'y - xy = \\ = x'(y' - y) + (x' - x)y.$$

Так как $y' - y$ и $x' - x$ — малые кватернионы, то в силу формулы (41) кватернионы $x'(y' - y)$ и $(x' - x)y$ малы. А в силу формулы (44) их сумма тоже мала. ■

§ 14. Геометрические применения кватернионов

В предыдущем параграфе мы построили совокупность K^4 кватернионов, представляющую собой евклидово векторное пространство размерности четыре. Было установлено, что пространство это распадается в прямую сумму действительных кватернионов D и чисто мнимых кватернионов I, причем линейные подпространства D и I векторного пространства K^4 являются взаимно ортогональными дополнениями.

В пространстве K^4 было выделено множество H кватернионов, по модулю равных единице и представляющее собой трехмерную сферу радиуса 1 с центром в начале координат.

А) Каждому кватерниону a из H поставим в соответствие отображение f_a евклидова векторного пространства K^4 на себя, задаваемое формулой

$$f_a(x) = axa^{-1}. \tag{45}$$

Легко проверяется, что при последовательном применении двух отображений f_a и f_b имеет место соотношение

$$f_a f_b = f_{ab}.$$

Оказывается, что

отображение f_a всех кватернионов на себя является изоморфизмом, т. е. сохраняет операции, имеющиеся в множестве кватернионов K^4. Именно, выполняются соотношения

$$\begin{aligned} f_a(x+y) &= f_a(x) + f_a(y), \\ f_a(xy) &= f_a(x) f_a(y). \end{aligned} \tag{46}$$

Далее, оказывается, что

линейное отображение f_a евклидова векторного пространства K^4 является вращением

(*см.* § 12 G)). *Кроме того, отображение* f_a *переводит линейные векторные подпространства* D *и* I *каждое само в себя.*

Доказательство. Прежде всего докажем соотношение (46). Это доказательство осуществляется автоматически. Именно, мы имеем

$$f_a(x+y) = a(x+y)a^{-1} = axa^{-1} + aya^{-1} = \\ = f_a(x) + f_a(y).$$

Далее,

$$f_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = f_a(x)f_a(y).$$

Докажем теперь, что при отображении f_a длина вектора x сохраняется. Для этого заметим прежде всего, что

$$\overline{axa^{-1}} = \overline{a^{-1}}\,\bar{x}\,\bar{a} = a\bar{x}a^{-1}$$

(см. формулы (40) и (42)).

В силу формулы (38) длина вектора axa^{-1} определяется формулой

$$|axa^{-1}|^2 = axa^{-1}\overline{axa^{-1}} = axa^{-1}a\bar{x}a^{-1} = \\ = ax\bar{x}a^{-1} = |x|^2.$$

Как было доказано в § 12, из того, что длина каждого вектора сохраняется при отображении f_a, следует, что скалярное произведение, имеющееся в евклидовом векторном пространстве K^4, также сохраняется при отображении f_a.

Таким образом, отображение f_a является изоморфным отображением трехмерного векторного пространства I на себя.

Далее, мы имеем, при x из D

$$axa^{-1} = xaa^{-1} = x.$$

Таким образом, $f_a(x) = x$, т. е. f_a есть тождественное отображение D самого на себя. Так как ортогональность при отображении f_a сохраняется, то ортогональное дополнение I к D также переходит само в себя.

Докажем теперь, что отображение f_a является вращением евклидова векторного пространства K^4. В силу формулы (43)

$$a = \cos\alpha + (\sin\alpha)u.$$

Полагая $a(t) = \cos\alpha t + (\sin\alpha t)u$, получаем кватернион $a(t)$, по модулю равный единице, который при изменении t от 0 до 1 непрерывно меняется от 1 до a. Таким образом, отображение $f_{a(t)}$ осуществляет непрерывный переход тождественного отображения f_1 в отображение f_a, и, следовательно, f_a есть вращение евклидова векторного пространства K^4. ■

В) Пусть u, v — ортонормальная пара векторов из I. Рассматривая их как кватернионы, составим произведение

$$w = uv.$$

Оказывается, что

для кватернионов

$$u, v, w \tag{47}$$

выполнены те же соотношения, что и для первоначально взятых мнимых единиц кватернионов (32). *Именно, имеют место соотношения*

$$u^2 = v^2 = w^2 = -1. \tag{48}$$

Далее,

$$\begin{aligned} uv &= -vu = w; \\ vw &= -wv = u; \\ wu &= -uw = v \end{aligned} \tag{49}$$

(ср. с (34), (35)).

Доказательство. Докажем соотношения (48) и (49); следуя формуле (36), мы имеем

$$uu = -(u, u) + [u, u] = -1.$$

Точно так же

$$vv = -(v, v) + [v, v] = -1.$$

В силу той же формулы (36) имеем

$$uv = [u, v] = -[v, u] = -vu.$$

Таким образом, кватернион $w = uv$ определяется в трехмерном евклидовом пространстве I как векторное произведение векторов u, v, а потому

принадлежит I. При этом также имеет место соотношение

$$uv = -vu = w.$$

Таким образом, первое соотношение (49) доказано. Далее имеем

$$(uv)^2 = uv\,uv = -uuv \cdot v = -1,$$

так что последнее из соотношений (48) тоже доказано. Докажем теперь последние два из соотношений (49). Мы имеем

$$vw = vuv = -v^2u = u,$$

$$wu = uvu = -vu^2 = v.$$

Итак, все соотношения (49) доказаны. ■

С) Пусть u, v — произвольная ортонормальная пара из I. Произведение кватернионов u, v обозначим через w, т. е. положим $w = uv$.

Плоскость из I с базисом v, w обозначим через P. Положим

$$a = \cos\alpha + \sin\alpha \cdot u, \quad |\alpha| \leqslant \pi$$

(см. (43)). Оказывается тогда, что

вращение f_a (см. (45)) пространства I есть вращение вокруг оси u, при котором плоскость P вращается в направлении от вектора v к вектору w на угол 2α. При этом угол α может быть и отрицательным; в этом случае вращение происходит в противоположную сторону.

Доказательство. Докажем утверждение C). Вычислим кватернионы

$$f_a(u) = aua^{-1},$$
$$f_a(v) = ava^{-1},$$
$$f_a(w) = awa^{-1}.$$

Так как кватернион a равен $\cos\alpha + \sin\alpha \cdot u$, то он перестановочен с u, следовательно, мы имеем:

$$f_a(u) = aua^1 = uaa^{-1} = u.$$

Далее, имеем:

$$\begin{aligned} f_a(v) &= (\cos\alpha + \sin\alpha \cdot u)v(\cos\alpha - \sin\alpha \cdot u) = \\ &= (\cos\alpha + \sin\alpha \cdot u)(\cos\alpha + \sin\alpha \cdot u)v = \\ &= (\cos 2\alpha + \sin 2\alpha \cdot u)v = \\ &= \cos 2\alpha \cdot v + \sin 2\alpha \cdot w. \end{aligned}$$

Далее,

$$\begin{aligned} f_a(w) &= (\cos\alpha + \sin\alpha \cdot u)w(\cos\alpha - \sin\alpha \cdot u) = \\ &= (\cos\alpha + \sin\alpha \cdot u)(\cos\alpha + \sin\alpha \cdot u)w = \\ &= (\cos 2\alpha + \sin 2\alpha \cdot u)w = \\ &= \cos 2\alpha \cdot w - \sin 2\alpha \cdot v. \end{aligned}$$

Из последних двух соотношений следует, что преобразование f_a осуществляет вращение плоскости P в направлении от вектора v к вектору w на угол 2α. ■

D) *Пусть x, y — два кватерниона из I, по модулю равные единице. Существует тогда вращение f_a такое, что*

$$f_a(x) = y.$$

Таким образом, существует вращение пространства I, при котором вектор x переходит в вектор y и которое задается в виде f_a. При этом, если x и y мало отличаются друг от друга, то угол α мал, и потому кватернион a близок к единице.

Доказательство. Для доказательства предложения D) проведем через векторы x и y плоскость P; и пусть u — кватернион из I, ортогональный к P и по модулю равный единице. В P выберем произвольный вектор v, $|v| = 1$. Тогда u, v образуют ортонормальную пару в I. Полагая

$$w = uv,$$

мы получим ортонормальный базис (47) пространства I, причем ортонормальная пара v, w составляет базис плоскости P, в которой лежат векторы x и y. Очевидно, существует такой угол α, что поворот на угол 2α в направлении от v к w будет переводить вектор x в вектор y, при этом α может быть и отрицательным. Но если при этом x и y мало отличаются друг от друга, то угол α будет мал. Таким образом, предложение D) доказано. ■

E) *Существует такое вращение* f_c (*см.* A)), *что*

$$f_c(i) = u,$$
$$f_c(j) = v,$$
$$f_c(k) = w,$$

где u, v, w — кватернионы, построенные в B). *При этом, если ортонормальная система i, j, k* (32) *близка к ортонормальной системе u, v, w* (47), *то кватернион c близок к единице, и следовательно, вращение f_c мало.*

Доказательство. Докажем предложение E). В силу предложения D) существует вращение f_a, переводящее кватернион i в кватернион u, т. е.

$$f_a(i) = u.$$

При этом, если ортонормальные системы (32) и (47) близки, то кватернион a близок к единице. Пусть P — плоскость с ортонормальным базисом j, k и

$$P' = f_a(P),$$

тогда плоскость P' содержит кватернионы $f_a(j)$, $f_a(k), v, w$.

Теперь существует такое вращение f_b, $b = \sin\beta + \cos\beta \cdot u$ вокруг оси u, при котором кватернион $f_a(j)$ переходит в кватернион v; при этом, если ортонормальные системы (32) и (47) близки между собой, то кватернион b близок к единице.

Таким образом, мы имеем

$$f_b(f_a(j)) = v.$$

Положив $c = ba$, получим

$$f_c(i) = u, \quad f_c(j) = v.$$

Далее,

$$f_c(k) = f_c(ij) = f_c(i) f_c(j) = uv = w,$$

при этом, если ортонормальные системы (32) и (47) близки друг к другу, то кватернионы a и b близки к единице, а следовательно, близок к единице и кватернион c. ■

F) *Пусть*

$$u_0, v_0, w_0; \quad u_1, v_1, w_1$$

— две ортонормальные тройки в пространстве I, мало отличающиеся друг от друга. Тогда существует такое вращение f_c, где c — кватернион, близкий к единице, при котором

$$\begin{aligned} f_c(u_0) &= u_1, \\ f_c(v_0) &= v_1, \\ f_c(w_0) &= w_1. \end{aligned} \tag{50}$$

Доказательство. Докажем утверждение F). Так как кватернион $w_0' = u_0 v_0$ ортогонален к кватернионам u_0, v_0, то мы имеем

$$w_0' = \varepsilon_0 w_0, \quad \text{где} \quad \varepsilon_0 = \pm 1.$$

Поскольку кватернион $w_1' = u_1 v_1$ ортогонален к кватернионам u_1, v_1, то мы имеем

$$w_1' = \varepsilon_1 w_1, \quad \text{где} \quad \varepsilon_1 = \pm 1.$$

Так как кватернионные пары u_0, v_0; u_1, v_1 близки между собой, то их произведения w_0' и w_1' также близки. А из близости кватернионов w_0' и w_1' вытекает, что $\varepsilon_0 = \varepsilon_1 = \varepsilon$, где $\varepsilon = \pm 1$.

Кватернионные тройки

$$u_0, v_0, \varepsilon w_0 \quad \text{и} \quad u_1, v_1, \varepsilon w_1,$$

близкие между собой, составляют ортонормальные системы в I, которые могут служить мнимыми единицами системы K^4 (см. B)). Поэтому в силу предложения E) существует вращение f_c, где c — кватернион, близкий к единице, при котором

$$f_c(u_0) = u_1,$$
$$f_c(v_0) = v_1,$$
$$f_c(\varepsilon w_0) = \varepsilon w_1.$$

Таким образом, соотношения (50) имеют место. Утверждение F) доказано. ■

Теорема о вращении чисто мнимых кватернионов

Теорема 1. *Всякое вращение g векторного пространства I всех чисто мнимых кватернионов может быть записано в виде*

$$\boxed{g(x) = f_a(x) = axa^{-1},}$$

где a — некоторый кватернион, по модулю равный единице. Если два кватерниона a и b равны по модулю единице, то вращения f_a и f_b совпадают тогда и только тогда, когда a и b либо совпадают, либо отличаются знаком, то есть

$$b = \pm a.$$

Доказательство. Так как g есть вращение, то оно получается в результате непрерывного перехода φ_t от тождественного отображения φ_0 к вращению $\varphi_1 = g$ (см. § 12 G)). Здесь $0 \leqslant t \leqslant 1$,

а φ_t есть вращение, непрерывно зависящее от параметра t. Разобьем отрезок $[0, 1]$ на n равных частей длины δ, причем δ — настолько малое число, что вращения $\varphi_{p\delta}$ и $\varphi_{(p+1)\delta}$ мало отличаются друг от друга. Это значит, что для любого вектора x длины единица из I кватернионы $\varphi_{p\delta}(x)$ и $\varphi_{(p+1)\delta}(x)$ близки друг к другу.

Пусть i, j, k — кватернионные единицы из I (32). Тогда, так как ортонормальные тройки

$$\begin{array}{lll} \varphi_{p\delta}(i), & \varphi_{p\delta}(j), & \varphi_{p\delta}(k); \\ \varphi_{(p+1)\delta}(i), & \varphi_{(p+1)\delta}(j), & \varphi_{(p+1)\delta}(k) \end{array}$$

близки между собой, то в силу F) существует такой кватернион c_p, близкий к единице, что вращение f_{c_p} переводит первую из этих троек во вторую (см. F)). Таким образом, последовательное применение вращений $f_{c_1}, f_{c_2}, \ldots, f_{c_n}$ переведет ортонормальную тройку i, j, k в ортонормальную тройку

$$g(i),\ g(j),\ g(k).$$

Таким образом, вращение g будет получено как последовательное применение вращений $f_{c_1}, \ldots, f_{c_n}$, так что искомый кватернион a задается формулой

$$a = c_n c_{n-1} \ldots c_1.$$

Тем самым первая часть теоремы доказана.

Докажем теперь, что вращения f_a и f_b совпадают тогда и только тогда, когда $a = \pm b$.

Если последнее равенство имеет место, то очевидно, что вращения f_a и f_b совпадают. Докажем обратное утверждение. Рассмотрим вращение $f_c = f_{a^{-1}} f_b$. Тогда $c = a^{-1}b$. Если вращения f_a и f_b совпадают, то вращение f_c является тождественным. Пусть

$$c = \cos\alpha + \sin\alpha \cdot u, \quad |\alpha| \leqslant \pi$$

(см. D)). Тогда в силу предложения B) вращение f_c является вращением вокруг оси u на угол 2α. Такое вращение является тождественным лишь при условии, когда $2\alpha = 2q\pi$, т. е. $\alpha = q\pi$. В этом случае $c = \pm 1$, и следовательно, $a = \pm b$. Итак, теорема 1 полностью доказана. ■

Займемся теперь вращением четырехмерного евклидова векторного пространства K^4, состоящего из всех кватернионов.

G) Каждой паре кватернионов $a, b \in H$, по модулю равных единице, поставим в соответствие отображение

$$f_{a,b}(x) = axb^{-1},$$

где x — произвольный вектор из K^4, т. е. произвольный кватернион. Оказывается, что

Вращение четырехмерного евклидова векторного пространства

$f_{a,b}$ есть вращение евклидова векторного пространства K^4.

Доказательство. Для доказательства этого докажем, что отображение $f_{a,b}$ не меняет длины век-

тора, т. е. модуля кватерниона x. В силу формулы (41) мы имеем

$$|axb^{-1}| = |a| \cdot |x| \cdot |b^{-1}| = |x|^2.$$

Таким образом, модули кватернионов x и $f_{a,b}(x)$ равны между собой и, следовательно, в силу формулы (20) $f_{a,b}$ есть изоморфное отображение евклидова векторного пространства K^4 самого на себя.

Докажем теперь, что изоморфное отображение $f_{a,b}$ евклидова векторного пространства K^4 является вращением, т. е. получается в результате непрерывного перехода φ_t, $0 \leqslant t \leqslant 1$, тождественного отображения φ_0 в отображение $\varphi_1 = \varphi_{a,b}$. Для этого запишем кватернионы a и b в форме D):

$$a = \cos\alpha + \sin\alpha \cdot u,$$
$$b = \cos\beta + \sin\beta \cdot v.$$

Положим далее

$$a(t) = \cos\alpha t + \sin\alpha t \cdot u,$$
$$b(t) = \cos\beta t + \sin\beta t \cdot v.$$

Кватернионы $a(t)$ и $b(t)$ непрерывно зависят от параметра t и по модулю равны единице. Таким образом, отображение $f_{a(t),b(t)}$ есть изоморфное отображение евклидова векторного пространства K^4 самого на себя, непрерывно зависящее от t и переводящее тождественное

отображение в отображение $f_{a,b}$. Таким образом, $f_{a,b}$ есть вращение евклидова векторного пространства K^4. ■

Теорема о вращении евклидова векторного пространства

Теорема 2. *Каждое вращение g евклидова векторного пространства K^4 задается формулой*

$$g(x) = f_{a,b}(x) = axb^{-1} \tag{51}$$

(см. G)). *При этом вращения $f_{a,b}$ и $f_{a',b'}$ совпадают тогда и только тогда, когда кватернионы a' и b' совпадают с кватернионами a и b или одновременно отличаются от них знаком.*

Доказательство. Пусть

$$\varepsilon = g(1). \tag{52}$$

Здесь ε — кватернион, по модулю равный единице. Наряду с вращением g рассмотрим отображение, определяемое формулой

$$g' = \varepsilon^{-1} g. \tag{53}$$

Легко проверить, что отображение g' является вращением евклидова векторного пространства K^4, так как кватернион ε может быть получен из единичного кватерниона в результате непрерывного изменения $\varepsilon(t)$, где $|\varepsilon(t)| = 1$, и переводит единицу в кватернион ε. Кроме того, умножение всех кватернионов из K^4 на кватернион $\varepsilon(t)$, по модулю равный единице, является

изоморфным отображением евклидова векторного пространства K^4 самого на себя (см. F)). Итак, g' есть вращение евклидова векторного пространства K^4. Из соотношений (52), (53) следует, что вся действительная ось D в евклидовом векторном пространстве K^4 при отображении g' отображается тождественно сама на себя. А так как g' есть изоморфное отображение евклидова векторного пространства K^4 на себя, то ортогональное дополнение к D, а именно I, отображается при помощи g' само на себя. Таким образом, g' является вращением евклидова векторного пространства I.

Следовательно, в силу теоремы 1 оно может быть записано в виде

$$g'(x) = cxc^{-1}.$$

Отсюда следует, что отображение g записывается в виде

$$g(x) = \varepsilon cxc^{-1}. \qquad (54)$$

Полагая, что

$$\varepsilon c = a, \quad c = b,$$

мы видим, что формула (51) верна, и первая часть теоремы 2 доказана.

Перейдем к доказательству второй ее части.

Так как кватернион ε однозначно определяется отображением g, то из совпадения двух вращений g_1 и g_2 евклидова векторного пространства K^4 самого на себя следует и совпадение соответствующих им отображений g_1' и g_2'.

Следовательно, в силу формулы (54) кватернионы c_1 и c_2, соответствующие отображениям g_1 и g_2, по теореме 1 могут отличаться лишь знаком.

Отсюда следует, что отображения $f_{a,b}$ и $f_{a',b'}$ могут совпадать тогда и только тогда, когда кватернионы a, b совпадают с кватернионами a', b' или оба отличаются от них одним и тем же знаком.

Итак, теорема 2 доказана. ■

Покажем теперь, что

не всякое изоморфное отображение евклидова векторного пространства I самого на себя может быть получено как вращение.

Н) Кватернионные единицы i, j, k, лежащие в I, представляют собой ортонормальную систему, которая может служить базисом пространства I. Тем же свойством обладают кватернионы $i, j, -k$. Существует поэтому изоморфное отображение f трехмерного евклидова векторного пространства I, при котором

$$f(i) = i, \quad f(j) = j, \quad f(k) = -k.$$

Отображение f не может быть записано формулой

$$f = f_a$$

(см. (45)).

Доказательство. Действительно, если бы это равенство имело место, то мы имели бы

$$f_a(i) = i, \quad f_a(j) = j, \quad f_a(k) = -k.$$

Но это невозможно. Действительно,

$$f_a(k) = f_a(ij) = f_a(i)f_a(j) = ij = k.$$

Итак, не всякое изоморфное отображение евклидова векторного пространства I на себя может быть получено как отображение f_a, а между тем в силу теоремы 1 любое вращение пространства I может быть записано в форме f_a. Таким образом, не всякое изоморфное отображение f евклидова векторного пространства I на себя является вращением. ■

Докажем теперь

инвариантность определения векторного произведения $[x, y]$ двух векторов x, y из I, которое дано было в координатной форме при помощи ортонормального базиса i, j, k

(см. § 12, F)).

• **Инвариантность векторного произведения относительно ортонормальных базисов**

Доказательство. В евклидовом векторном пространстве I имеется базис

$$i, j, k, \tag{55}$$

а также ортонормальный базис

$$u, v, w \tag{56}$$

(см. B)), получаемый из базиса (55) путем вращения в евклидовом векторном пространстве I

(см. Е)). При этом правило перемножения кватернионов (56) полностью совпадает с правилом перемножения кватернионов (55).

Пусть теперь x и y — два кватерниона из I. Запишем их в базисах (55) и (56):

$$\begin{aligned} x &= x^1 i + x^2 j + x^3 k, \\ y &= y^1 i + y^2 j + y^3 k. \end{aligned} \tag{57}$$

Далее, имеем

$$\begin{aligned} x &= \xi^1 u + \xi^2 v + \xi^3 w, \\ y &= \eta^1 u + \eta^2 v + \eta^3 w. \end{aligned} \tag{58}$$

Векторное произведение $[x, y]$ при помощи координат, связанных с базисом (55), было определено формулой

$$[x, y] = (x^2 y^3 - x^3 y^2) i + (x^3 y^1 - x^1 y^3) j + \\ + (x^1 y^2 - x^2 y^1) k.$$

После этого было доказано, что кватернионное произведение xy выражается формулой

$$xy = -(x, y) + [x, y],$$

при этом доказательство опиралось на правило перемножения кватернионов (55).

Составим теперь кватернионное произведение xy при помощи базиса (56).

Так как правило перемножения кватернионов (56) полностью совпадает с правилами перемножения кватернионов (55), то кватернионное произведение xy запишется при помощи

координат (58) в форме

$$xy = -(x, y) + [x, y].$$

Но вместо координат (57) будут стоять координаты (58). Так как координатная запись скалярного произведения (x, y) инвариантна относительно выбора ортонормального базиса, то векторное произведение $[x, y]$ двух векторов x и y, взятых в двух ортонормальных базисах (55) и (56), которые могут быть переведены один в другой путем вращения, оказывается одинаковым.

Но это относится только к ортонормальным базисам, которые можно перевести друг в друга путем вращения. ■

Глава 5

Другие обобщения чисел

§ 15. Алгебраические тела и поля 129
§ 16. Поле вычетов по простому модулю p . 137
§ 17. Теорема Фробениуса 145

Для того чтобы вполне точно ставить вопрос об обобщениях чисел, мы в первую очередь должны точно определить те правила действий, которые должны иметь место, а эти правила формулируются как правила действий, имеющиеся в алгебраических телах и полях. Поэтому первый параграф настоящей главы посвящен определению алгебраических тел и полей.

Во втором параграфе этой главы доказывается теорема Фробениуса о том, что других обобщений действительных чисел, кроме комплексных чисел и кватернионов, не существует.

В следующей главе будут рассматриваться другие обобщения чисел.

§ 15. Алгебраические тела и поля

В этой книге мы уже имели дело с несколькими видами чисел или, лучше сказать, величин, так как кватернионы не принято называть числами.

Я имею в виду рациональные, действительные, комплексные числа и кватернионы. Все упомянутые четыре вида величин имеют некоторые общие черты. В каждом из упомянутых четырех множеств величин имеются два действия — сложение и умножение. Для каждого из этих действий выполнены определенные правила. Прежде чем формулировать эти правила, скажем,

Тело и поле

что совокупность величин, в которой определены два действия — сложение и умножение, связанные такого рода правилами, — называется в алгебре телом, а в случае, если умножение коммутативно, — полем.

Совокупность или множество всех величин, составляющих тело, обозначим через K. Сформулируем теперь те правила, которым удовлетворяют действия, имеющиеся в K.

Коммутативность сложения

1. По сложению тело K коммутативно. Это значит, что если x и y — две величины из K, то имеет место равенство

$$x + y = y + x. \tag{1}$$

Ассоциативность сложения

2. Сложение ассоциативно. Это значит, что если x, y, z — три величины из K, то выполнено следующее правило;

$$(x + y) + z = x + (y + z).$$

3. В K имеется единственный элемент, называемый нулем сложения и обозначаемый знаком 0. Он удовлетворяет следующему условию:

• **Существование и единственность нуля сложения**

$$\boxed{x + 0 = x,}$$

следовательно (см. (1)), $0 + x = x$.

4. Для каждой величины x из K имеется противоположная ей величина, обозначаемая $-x$ и удовлетворяющая следующему условию:

• **Существование и единственность противоположного элемента**

$$\boxed{x + (-x) = 0.}$$

Из сформулированных правил следует, что соотношение

$$x + y = z \qquad (2)$$

(y и z — заданные величины), рассматриваемое как уравнение относительно x, разрешимо. Для его решения к обеим частям равенства (2) прибавим $-y$. Тогда получим

$$x = z + (-y) = z - y.$$

• **Вычитание**

Таким образом, в K имеется действие вычитание, обратное сложению.

Из сказанного видно, что

совокупность всех элементов, входящих в K, по сложению образует коммутативную группу.

Правила умножения

Для умножения выполнены правила, аналогичные тем, которые были перечислены для сложения, за исключением одного — первого — коммутативности.

Ассоциативность умножения

5. Умножение в K ассоциативно. Именно, если x, y, z — три величины из K, то выполнено условие

$$(xy)z = x(yz).$$

Существование единицы умножения

6. В K существует единица e умножения, удовлетворяющая следующему условию:

$$ez = ze = z.$$

Существование обратного элемента

7. Для каждого элемента z из K, отличного от 0, имеется обратный элемент, обозначаемый z^{-1}, удовлетворяющий условию

$$z^{-1}z = zz^{-1} = e.$$

Из сформулированных правил умножения, имеющихся в K, вытекает, что соотношения

$$xy = z, \tag{3}$$

$$yx = z, \tag{4}$$

где y, z — заданные элементы K, причем $y \neq 0$, могут быть разрешены относительно x. Для решения уравнения (3) умножим обе его части

справа на y^{-1}. Тогда получим

$$x = zy^{-1}.$$

Для решения уравнения (4) умножим обе его части слева на y^{-1}. Тогда получим

$$x = y^{-1}z.$$

Таким образом,

по умножению все элементы из K, отличные от 0, образуют группу.

Наконец, действия сложения и умножения, имеющиеся в K, связаны следующим правилом.

• **Дистрибутивность**

8. Дистрибутивность. Именно, если x, y, z — три произвольных элемента из K, то имеют место соотношения

$$\boxed{\begin{aligned}(x+y)z &= xz + yz;\\ z(x+y) &= zx + zy.\end{aligned}}$$

Из сформулированных правил вытекает

$$\boxed{0z = z0 = 0.} \qquad (5)$$

Доказательство. Действительно, мы имеем

$$0z = (0+0)z = 0z + 0z.$$

Вычитая из обеих частей этого соотношения $0z$, получим

$$0 = 0z.$$

Второе из соотношений (5) доказывается аналогично. ■

С другой стороны, из соотношения

$$xy = 0 \qquad (6)$$

следует, что один из множителей (x или y) равен 0.

Это свойство тела формулируют, говоря, что

в теле K нет делителей нуля.

Доказательство. Допустим, что $y \neq 0$, и докажем, что x тогда равен 0. Умножая обе части соотношения (6) справа на y^{-1}, получим $x = 0y^{-1} = 0$. Аналогично доказывается, что если $x \neq 0$, то $y = 0$. ■

Естественным образом определяется умножение произвольного элемента x тела K на целое неотрицательное число n: именно,

$$0x = 0;$$
$$1x = x;$$
$$2x = x + x;$$
$$3x = x + x + x;$$
$$\ldots\ldots\ldots\ldots$$

Легко проверяется, что

если m и n — два целых неотрицательных числа, то

$$\boxed{mx + nx = (m + n)x;} \qquad (7)$$

$$(mx)\,(ny) = mnxy. \qquad (8)$$

Определим теперь так называемую характеристику тела K, которая равна либо 0, либо простому числу p. Для этого составим последовательность элементов тела K

• **Характеристика тела**

$$0e, 1e, 2e, \ldots, ne \ldots . \qquad (9)$$

Если в последовательности элементов (9) только один элемент $0e$ равен 0, то считают, что тело K имеет характеристику 0.

Если это не имеет места, то в последовательности величин (9) встречаются нулевые элементы, отличные от $0e$. В множестве элементов (9) определены операции сложения и умножения (см. (7), (8)). Оказывается, что

в случае, когда характеристика не равна 0, *множество* (9) *содержит лишь конечное число различных элементов, составляющих поле* P^p *вычетов по простому модулю* p (*см.* § 16).

В этом случае характеристикой тела считается простое число p.

Пример. Очевидно, что поле R всех рациональных чисел имеет характеристику 0. Оказывается, что в известном смысле поле R является простейшим полем характеристики 0.

Определение 1

Изоморфные тела

Два тела K и K' считаются изоморфными, если существует взаимно однозначное соответствие между элементами множеств K и K', причем операции, имеющиеся в K и K', переходят друг в друга. Более детально: существует такое взаимно однозначное отображение f множества K на множество K', при котором операции умножения и сложения сохраняются, т. е. выполнены условия

$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x)\,f(y).$$

Изоморфизм тел

Отображение f тела K на тело K' называется изоморфным или изоморфизмом.

Ясно, что

при изоморфизме нуль переходит в нуль, единица в единицу, противоположный элемент в противоположный, обратный в обратный.

При определении характеристики тела K мы рассматривали последовательность (9) элементов тела. В случае, если характеристика тела K равна нулю, мы, пользуясь операциями вычитания и деления, имеющимися в теле K, можем определить естественным образом произведение любого рационального числа r на еди-

ницу e. Таким образом, в теле K имеется совокупность всех элементов вида re, где r — рациональное число. Совокупность всех таких элементов естественным образом составляет поле, лежащее в теле K, и поле это изоморфно полю рациональных чисел. Следовательно, поле рациональных чисел является простейшим телом характеристики нуль.

Определение 2

Если в теле K содержится множество элементов K_1, которое в силу операций сложения и умножения, имеющихся в K, составляет тело, то тело K_1 называется подтелом K, а тело K — расширением тела K_1.

• **Подтело и расширение тела**

Приведем теперь описание простейшего поля характеристики p. Оно является полем вычетов по модулю p.

§ 16. Поле вычетов по простому модулю p

A)

Пусть $m > 1$ — некоторое натуральное число. Говорят, что целые числа a и b сравнимы

• **Сравнимость целых чисел**

между собой по модулю m, и пишут

$$a \equiv b (\mathrm{mod}\, m),$$

если разность $b - a$ делится на m, т. е. если

$$b = a + cm, \qquad (10)$$

где c — целое число.

Очевидно, что

если два числа сравнимы с одним и тем же числом по модулю m, то они сравнимы и между собой по модулю m.

В)

Вычет по модулю

Множество всех чисел, сравнимых с некоторым заданным числом a по модулю m, называется вычетом по модулю m. Будем обозначать это множество через $[a]$.

Очевидно, что каждые два числа множества $[a]$ сравнимы между собой по модулю m. Если b — произвольное число из множества $[a]$, то множества $[a]$ и $[b]$ совпадают между собой:

$$[a] = [b].$$

Ясно, что совокупность

$$[0],\ [1],\ [2],\ \ldots,\ [m-1]$$

составляет совокупность всех вычетов по модулю m. Таким образом, имеется ровно m вычетов по модулю m.

C) Пусть a_1 и a_2 — два целых числа, $[a_1]$ и $[a_2]$ — содержащие эти числа вычеты по модулю m; b_1, b_2 — два целых числа, принадлежащих соответственно вычетам $[a_1]$, $[a_2]$. Тогда в силу (10) мы имеем

$$b_1 = a_1 + c_1 m, \quad b_2 = a_2 + c_2 m.$$

И, следовательно,

$$b_1 + b_2 = a_1 + a_2 + (c_1 + c_2)m.$$

Отсюда видно, что сумма $b_1 + b_2$ принадлежит вычету $[a_1 + a_2]$. Таким образом,

складывая произвольное число из вычета $[a_1]$ с произвольным числом из вычета $[a_2]$, мы всегда получим число, принадлежащее вычету $[a_1 + a_2]$.

Следовательно, вычет $[a_1 + a_2]$ однозначно определен вычетами $[a_1]$ и $[a_2]$. Этот вычет не зависит от случайного выбора чисел b_1 и b_2 из вычетов $[a_1]$ и $[a_2]$. Вычет $[a_1 + a_2]$ считается суммой вычетов $[a_1]$ и $[a_2]$:

$$\boxed{[a_1] + [a_2] = [a_1 + a_2].}$$

• **Сумма вычетов**

Таким образом, в совокупности всех вычетов по модулю m определена операция сложения. Нулем этого сложения является $[0]$. Точно так же можно определить разность двух вычетов по модулю m и произведение двух вычетов по модулю m. Причем единицей умножения служит $[1]$.

• **Другие операции над вычетами**

Мы видим, что в совокупности всех вычетов по модулю m определены операции сложения, вычитания и умножения.

D) Если m — не простое число, т. е. если оно разложимо на два множителя

$$m = rs,$$

где r и s оба отличны от единицы, то ясно, что

$$[r][s] = [0].$$

Таким образом,

в случае не простого числа m в совокупности всех вычетов имеются «делители нуля».

В этом случае совокупность всех вычетов по модулю m с определенными в этой совокупности операциями не может составлять поле. Оказывается, что

Поле вычетов по модулю простого числа

если $m = p$ есть простое число, то совокупность всех вычетов по модулю p составляет поле.

Доказательство. Пусть

$$[1],\ [2],\ \ldots,\ [p-1] \qquad (11)$$

— совокупность всех вычетов по простому модулю p, отличных от нуля. Произведение двух вычетов $[r]$ и $[s]$ из последовательности (11) не может обращаться в нуль. Если бы было

$$[r][s] = [0],$$

то это означало бы, что rs делится на p, а это значит, что один из этих множителей делится на p, т. е. соответствующий ему вычет равен нулю и, следовательно, не принадлежит последовательности (11). Если $[a_1]$, $[a_2]$ и $[a]$ — три произвольных вычета последовательности (11), то равенство

$$[a_1][a] = [a_2][a] \qquad (12)$$

возможно лишь в случае, если $[a_1] = [a_2]$. Действительно, из равенства (12) следует

$$([a_1] - [a_2])[a] = [0].$$

Так как $[a]$ не равно нулю, то первый множитель равен нулю и, следовательно, $[a_1] = [a_2]$. Таким образом, умножая все вычеты последовательности (11) на один и тот же вычет $[a]$, мы получим ровно $p - 1$ вычет, причем все они будут различны. Это значит, что умножение на $[a]$ последовательности (11) отображает ее на себя взаимно однозначно. Таким образом, найдется такой вычет $[a']$, что

$$[a][a'] = [1].$$

Это значит, что для вычета $[a]$ существует обратный вычет $[a']$, и потому совокупность всех вычетов по простому модулю p составляет поле. ■

Это поле называется полем вычетов по модулю p, причем p — простое число. Мы будем обозначать это поле через P^p.

E) *Если в последовательности* (9) *элементов некоторого тела* K *имеется равный нулю элемент, отличный от элемента* $0e$, *то обозначим через* m *минимальное натуральное число, при котором* $me = 0$. *Оказывается тогда, что если целое число* t *удовлетворяет условию* $te = 0$, *то* t *делится на* m.

Доказательство. Действительно, разделив t на m, мы получим

$$t = qm + r,$$

где q — частное, r — остаток, причем $r < m$. Умножая это равенство на e справа, мы получим:

$$0 = 0 + re.$$

Таким образом, $re = 0$, причем $r < m$, что противоречит нашему предположению. ■

Очевидно, что если два целых числа a и b обладают тем свойством, что $ae = be$, то a и b сравнимы по модулю m. Таким образом, устанавливается взаимно однозначное соответствие между элементами тела K вида (9), § 15, и вычетами по модулю m, при котором сохраняются операции сложения и умножения. Так как в теле K отсутствуют делители нуля, то число m должно быть простым (см. D)). Следовательно,

совокупность всех элементов вида (9) *тела* K *изоморфна полю вычетов* P^p *по простому модулю* p.

• **Характеристика тела**

Простое число p называется характеристикой тела K. Тем самым

поле вычетов P^p является простейшим телом характеристики p.

Непосредственно к предложению D) примыкает так называемая малая теорема Ферма, отличная от великой теоремы Ферма, пользующейся широкой известностью. В дальнейшем малая теорема Ферма не будет использована в этой книге. Я привожу ее здесь вместе с доказательством, так как она является нетривиальным применением вычетов.

• **Малая теорема Ферма**

Пусть p — простое число, a — произвольное целое число, не делящееся на p. Тогда имеет место следующее сравнение:

$$\boxed{a^{p-1} \equiv 1 (\mathrm{mod}\, p).} \qquad (13)$$

Доказательство. Последовательность (9) состоит из всех величин поля P^p, отличных от нуля. Умножая все эти величины на вычет $[a]$ из поля P^p, мы, как это было доказано в предложении D), получим те же самые величины последовательности (9), расположенные в другом порядке. Таким образом, в поле P^p имеет место следующее равенство:

$$[a]^{p-1}[1][2]\ldots[p-1] = [1][2]\ldots[p-1].$$

Величина, стоящая в правой части этого равенства, отлична от нуля в поле P^p, поэтому последнее равенство можно на нее разделить. Так что мы получаем равенство

$$[a]^{p-1} = [1].$$

Это равенство, имеющее место в поле P^p, равносильно числовому сравнению (13), которое содержится в формулировке малой теоремы Ферма. Таким образом, малая теорема Ферма доказана. ■

Пример. Проверим малую теорему Ферма на простом числовом примере. Пусть $p = 5$, $a = 2$. Имеем $2^4 = 16$, а 16 очевидно сравнимо с 1 по модулю 5.

Рассмотрим теперь вычеты по простейшим модулям 2, 3 и 4.

Имеются два вычета по модулю 2: [0] и [1]. Для этих вычетов имеются следующие правила сложения и умножения:

$$[0] + [1] = [1], \quad [1] + [1] = [0],$$
$$[0]\,[1] = [0], \qquad [1]\,[1] = [1].$$

Из этих правил видно, что вычеты по модулю 2 составляют поле, которое мы обозначаем через P^2.

Вычетов по модулю 3 имеется три: [0], [1], [2]. Выпишем правило сложения и умножения для этих вычетов. Мы имеем

$$[1] + [1] = [2], \quad [1] + [2] = [0], \quad [2] + [2] = [1],$$
$$[1]\,[1] = [1], \qquad [2]\,[2] = [1].$$

Из этих правил видно, что вычеты по модулю 3 составляют поле, которое мы обозначаем через P^3.

Вычетов по модулю 4 имеется четыре: [0], [1], [2], [3].

Выпишем правила сложения и умножения для этих вычетов. Мы имеем

$$[1]+[2]=[3],\quad [1]+[3]=[0],$$
$$[2]+[3]=[1],\quad [3]+[3]=[2],$$
$$[2][2]=[0],\qquad [2][3]=[2],\quad [3][3]=[1].$$

Из этих правил видно, что вычеты по модулю 4 не составляют поле, так как квадрат вычета [2] равен нулю. В частности, по этой причине нельзя равенство $[2][3]=[2]$ сократить на величину [2], так как для величины [2] нет обратной.

§ 17. Теорема Фробениуса

Теорема 3. *Пусть L — алгебраическое тело, содержащее в качестве подтела тело D действительных чисел, причем каждый элемент из L коммутативен по умножению с элементами из D, а каждый элемент x из K записывается в виде*

$$x = x^0 + x^1 i_1 + \ldots + x^n i_n, \qquad (14)$$

где $x^0, x^1, \ldots, x^n$ — действительные числа, являющиеся координатами величины x так, что x есть $(n+1)$-мерный вектор. Таким образом предполагается, что величины

$$1, i_1, \ldots, i_n$$

• **Теорема Фробениуса**

Фердинанд Георг Фробениус (1849–1917)

составляют базис векторного пространства L. Для определения умножения в L достаточно задать правило перемножения величин $i_1, \ldots, i_n$ так, чтобы каждое произведение $i_r i_s$ записывалось в форме (14). *Оказывается тогда, что L либо совпадает с полем D, то есть изоморфно полю действительных чисел, либо изоморфно полю K^2 комплексных чисел, либо изоморфно телу K^4 кватернионов.*

Доказательство. Поле D действительных чисел состоит из всех величин x вида (14), для которых только координата x^0 может быть отлична от нуля. Множество D представляет собой одномерное векторное подпространство векторного пространства L. Тело L, очевидно, имеет характеристику 0.

Для того чтобы сделать доказательство более обозримым, разобьем его на пункты A), B), C).

A) В теле L выделим величины, которые естественно считать чисто мнимыми. Совокупность всех их обозначим через I. К I мы отнесем всякую величину z из L, квадрат которой действителен, т. е. принадлежит D, и неположителен. Таким образом, I состоит из тех z, для которых

$$z^2 \in D; \quad z^2 \leqslant 0.$$

Последнее неравенство может превратиться в равенство только в случае $z = 0$. Ясно, что множества I и D пересекаются только в нуле.

Величины из I обладают следующими свойствами.

Если α — действительное число, а $z \in I$, то

$$\alpha z \in I. \tag{15}$$

Далее, если $z \in I$ и $z \neq 0$, то

$$z^{-1} \in I. \tag{16}$$

Оказывается, что каждая величина x из L единственным способом разлагается в сумму

$$x = a + z, \tag{17}$$

где $a \in D$, $z \in I$.

Докажем утверждение А). Начнем с утверждения (15). Мы имеем $(\alpha z)^2 = \alpha^2 z^2$. Так как $\alpha^2 \geqslant 0$, $z^2 \leqslant 0$, то $(\alpha z)^2 \leqslant 0$. И, следовательно, $\alpha z \in I$.

Для доказательства (16) составим произведение

$$z^2(z^{-1})^2 = zzz^{-1}z^{-1} = 1.$$

Таким образом, $(z^{-1})^2 = (zz)^{-1}$ и, следовательно, отрицательно. Так что $z^{-1} \in I$.

Докажем теперь, что имеет место разложение (17). Для этого составим последовательность величин

$$1, x, x^2, \ldots, x^{n+1}. \tag{18}$$

Так как размерность векторного пространства L равна $n + 1$, а число величин последовательности (18) равно $n + 2$, то в силу предложения А) § 11 величины последовательности (18)

линейно зависимы, т. е. имеет место соотношение

$$\alpha_0 + \alpha_1 x + \ldots + \alpha_{n+1} x^{n+1} = 0,$$

где коэффициенты $\alpha_0, \alpha_1, \ldots, \alpha_{n+1}$ суть действительные числа, не все равные нулю. Таким образом, величина x является корнем многочлена с действительными коэффициентами, и потому в силу результатов § 7 является корнем либо многочлена g_1 первой степени, либо многочлена g_2 второй степени. Так что для x выполнено одно из двух соотношений

$$x - \alpha = 0; \quad x^2 - 2ax + b = 0,$$

где $a^2 - b < 0$. В первом случае x есть действительное число α, и для разложения (17) мы имеем $a = \alpha$, $z = 0$. Во втором случае мы имеем $(x - a)^2 = a^2 - b < 0$. Таким образом, величина $x - a$ принадлежит I; обозначим ее через z. Тогда мы получаем $x = a + z$, и разложение (17) доказано.

Установим теперь единственность разложения (17). Допустим, что наряду с (17) мы имеем разложение

$$x = a_0 + z_0, \tag{19}$$

где $a_0 \in D$, $z_0 \in I$. Докажем, что тогда $a_0 = a$, $z_0 = z$. Вычитая (19) из разложения (17), мы получим

$$z = z_0 + (a_0 - a).$$

Возводя это равенство в квадрат, получаем

$$z^2 = z_0^2 + 2z_0(a_0 - a) + (a_0 - a)^2,$$

или, иначе,

$$2z_0(a_0 - a) = z^2 - z_0^2 - (a_0 - a)^2.$$

Здесь в левой части стоит чисто мнимая величина (см. (15)), а в правой — действительная. Таким образом, обе они равны нулю. То есть мы имеем $2z_0(a_0 - a) = 0$. Так как характеристика тела L не равна 2, то имеет место равенство $z_0(a_0 - a) = 0$, что возможно только тогда, когда один из множителей равен нулю. Допустим сперва, что $z_0 = 0$. Тогда из соотношения (19) следует, что x — действительное число a_0. А из соотношения (17) получаем $z = a_0 - a$. Таким образом, левая часть есть чисто мнимая величина, а правая — действительная. Следовательно, обе они равны нулю. Таким образом, мы пришли к выводу, что $z_0 = z = 0$, а отсюда следует, что $a_0 \neq a$. (При этом предполагалось, что $z_0 = 0$.) Если же равен нулю множитель $a_0 - a$, то $a_0 = a$, а из этого в силу соотношений (17) и (19) вытекает, что $z_0 = z$. Таким образом, единственность разложения (17) установлена и предложение А) полностью доказано.

В) Пусть u и v — две величины из I, а r и s — два действительных числа. Тогда, оказывается, имеют место два нижеследующих соотношения:

$$\xi = uv + vu \in D, \qquad (20)$$

$$\eta = ru + sv \in I. \qquad (21)$$

Из соотношения (21) следует, что I есть векторное подпространство векторного пространства L. А из этого и из предложения А) вытекает, что L распадается в прямую сумму своих векторных подпространств D и I.

Докажем предложение В). Рассмотрим сперва тот простой случай, когда величины $u, v, 1$ линейно зависимы. Тогда мы имеем

$$\alpha u + \beta v + \gamma = 0,$$

причем не все действительные числа α, β, γ равны нулю. Последнее равенство перепишем в виде

$$\alpha u = -\beta v - \gamma.$$

Здесь αu и $-\beta v$ — чисто мнимые величины в силу соотношения (15), и в силу единственности разложения (17) получаем $\gamma = 0$. Таким образом,

$$\alpha u = -\beta v.$$

Так как оба коэффициента α и β не могут быть равны нулю, то один из них отличен от нуля. Для определенности будем считать, что $\beta \neq 0$. Тогда

$$v = -\frac{\alpha}{\beta} u.$$

Подставляя это выражение в (20), получаем

$$\xi = -\frac{2\alpha}{\beta} u^2,$$

т. е. ξ есть действительное число и соотношение (20) в этом случае доказано. Подставляя полученное выражение для v в (21), получаем

$$\eta = \left(r - \frac{s\alpha}{\beta}\right)u.$$

Так что в силу (15) η есть чисто мнимая величина.

Рассмотрим теперь случай, когда величины $u, v, 1$ линейно независимы. Утверждения (20) и (21) будем доказывать вместе. Мы будем рассматривать только тот случай, когда r и s оба отличны от нуля. В противном случае оба соотношения (20) и (21) легко проверяются. Для доказательства разложим величины ξ и η согласно (17). Положим

$$\xi = uv + vu = a + z, \tag{22}$$

где $a \in D$, $z \in I$;

$$\eta = ru + sv = a_0 + z_0, \tag{23}$$

где $a_0 \in D$, $z_0 \in I$.

Для доказательства соотношений (20) и (21) нам достаточно доказать, что $z = 0$ и $a_0 = 0$.

Возведем равенство (23) в квадрат. Тогда мы получим

$$r^2u^2 + s^2v^2 + rs(uv + vu) = a_0^2 + 2a_0z_0 + z_0^2.$$

Подставляя в левую часть этого соотношения вместо $uv + vu$ его выражение в силу равенства (22), мы получим

$$r^2u^2 + s^2v^2 + rs(a + z) = a_0^2 + 2a_0z_0 + z_0^2. \tag{24}$$

Левая и правая части этого равенства состоят из действительной и чисто мнимой части. В силу единственности разложения (17) эти части должны соответственно равняться друг другу. Мнимая часть левой части равенства (24) есть rsz, а мнимая часть правой части есть $2a_0z_0$, так что мы имеем равенство

$$rsz = 2a_0z_0. \tag{25}$$

Рассмотрим теперь два различных случая. Первый: $z = 0$; второй: $z \neq 0$.

В первом случае из равенства (25) мы имеем $a_0z_0 = 0$. Следовательно, либо a_0, либо z_0 обращается в нуль. Если $a_0 = 0$, то соотношение (21) верно, а соотношение (20) следует из предположения, что $z = 0$. Если $z_0 = 0$, то равенство (23) превращается в линейную зависимость между u, v и 1. Этот простой случай нами уже разобран. Таким образом, в предположении $z = 0$ (первый случай) доказательство предложения B) получено.

Рассмотрим случай $z \neq 0$. Поскольку r и s оба не равны нулю, то из соотношения (25) следует $a_0 \neq 0$, и соотношение (25) можно переписать в виде

$$z_0 = \frac{rs}{2a_0}z.$$

Подставляя это выражение для z_0 в равенство (23), получаем

$$ru + sv = a_0 + \frac{rs}{2a_0}z. \tag{26}$$

Заметим, что z не зависит от чисел r и s и равенство (26) доказано нами в предположении, что $z \neq 0$. Выпишем теперь равенство (26) для каких-нибудь двух других чисел r' и s'. Мы получим

$$r'u + s'v = a_0' + \frac{r's'}{2a_0'}z. \qquad (27)$$

Исключим из равенств (26) и (27) величину z, умножив равенство (27) на подходящее действительное число c и вычтя его из равенства (26). Тогда мы получим

$$(r - cr')u + (s - cs')v = a_0 - ca_0'. \qquad (28)$$

Поскольку числа r' и s' выбирались совершенно произвольным образом, лишь бы оба они не равнялись нулю, мы можем их выбрать так, чтобы не было пропорциональности. В этом предположении в равенстве (28) коэффициенты $r - cr'$ и $s - cs'$ не могут оба обращаться в нуль. Тогда равенство (28) превращается в линейную зависимость между величинами u, v и 1, т. е. в случай, разобранный нами в самом начале доказательства предложения B).

Таким образом, предложение B) доказано.

C) Пусть u и v — две величины из I, удовлетворяющие условиям

$$u^2 = -1, \quad v^2 = -1, \quad w = uv \in I. \qquad (29)$$

Тогда величины u, v, w удовлетворяют тем же условиям, что и кватернионные единицы

(см. § 13 (34), (35)), т. е. имеют место равенства

$$u^2 = v^2 = w^2 = -1, \tag{30}$$

$$uv = -vu = w,$$

$$vw = -wv = u, \tag{31}$$

$$wu = -uw = v.$$

Докажем предложение C). Для этого установим прежде всего, что

$$vu = (uv)^{-1}.$$

Действительно,

$$uv\,vu = u(-1)u = u^2(-1) = 1.$$

Таким образом, мы имеем

$$uv + vu = uv + (uv)^{-1}. \tag{32}$$

В силу соотношения (20) левая часть этого равенства есть действительное число. Правая же часть есть сумма двух чисто мнимых величин, так как $(uv)^{-1}$ в силу (16) есть чисто мнимая величина, и, значит, правая часть равенства (32) в силу (21) — чисто мнимая. Таким образом, обе части равенства (32) обращаются в нуль и, следовательно, мы имеем:

$$uv = -vu. \tag{33}$$

Таким образом, первое из равенств (31) нами уже доказано. Докажем теперь последнее из равенств (30). Мы имеем

$$w^2 = uv\,uv = -uv\,vu = -1.$$

Докажем теперь второе и третье из соотношений (31). Мы имеем

$$vw = vuv = -vvu = u. \tag{34}$$

Три величины v, w и $u = vw$ удовлетворяют тем же условиям, что и величины (29), а для величин (29) имеет место соотношение (33). Таким образом, здесь мы имеем

$$wv = -vw.$$

Таким образом, вместе с (34) это соотношение дает второе из соотношений (31).

Рассмотрим теперь

$$wu = uvu = -uuv = v.$$

Точно так же, как и перед этим, докажем, что

$$wu = -uw.$$

Таким образом, и третье соотношение из (31) доказано.

Итак, предложение C) доказано.

Перейдем теперь к заключительному этапу доказательства теоремы 3.

Если I содержит только нуль, то L совпадает с D и, следовательно, изоморфно полю действительных чисел D. Таким образом, в этом случае теорема 3 верна.

Допустим теперь, что в I есть вектор z_0, отличный от 0. Тогда, полагая

$$i = \frac{z_0}{\sqrt{-z_0^2}},$$

мы получаем элемент $i \in I$, удовлетворяющий условию

$$i^2 = -1.$$

Если размерность пространства I равна 1, то всякий элемент из I записывается в форме

$$bi,$$

где b — действительное число. Тогда каждый элемент из L записывается в виде

$$a + bi.$$

Таким образом, в случае, когда размерность векторного пространства I равна 1, тело L изоморфно полю комплексных чисел K^2.

Допустим теперь, что размерность пространства I больше единицы. Тогда в I существует такая величина z_1, что пара векторов

$$i, z_1$$

линейно независима.

Рассмотрим произведение iz_1. Согласно (17)

$$iz_1 = a + z.$$

Положим $j_1 = z_1 + ai$. Тогда мы имеем

$$ij_1 = iz_1 - a = z.$$

Полагая

$$j = \frac{j_1}{\sqrt{-j_1^2}},$$

мы получаем для j равенство

$$j^2 = -1.$$

Таким образом, величины i, j удовлетворяют условиям

$$i^2 = -1, \quad j^2 = -1; \quad i, j \in I.$$

Следовательно, величины

$$i, j, k = ij$$

в силу предложения С) удовлетворяют тем же условиям, что и величины u, v, w. Таким образом, совокупность всех величин из L, которые можно записать в виде

$$x = x^0 + x^1 i + x^2 j + x^3 k,$$

где x^0, x^1, x^2, x^3 суть действительные числа, составляет тело K^4 кватернионов.

Если пространство I имеет размерность три, то L совпадает с телом K^4, т. е. изоморфно телу кватернионов.

Допустим теперь, что размерность пространства I больше трех, и приведем это предположение к противоречию.

Если размерность пространства I больше трех, то в нем найдется такая величина z_2, что векторы

$$i, j, k, z_2$$

линейно независимы. В силу разложения (17) мы имеем

$$iz_2 = a + x, \quad jz_2 = b + y, \quad kz_2 = c + z,$$

где a, b, c — действительные числа, а x, y, z принадлежат I. Составим теперь величину

$$l_1 = z_2 + ai + bj + ck.$$

В силу (21) $l_1 \in I$, и в силу линейной независимости векторов i, j, k, z_2 имеем $l_1 \neq 0$.

Кроме того,

$$il_1 = iz_2 - a + bk + cj = x + bk + cj \in I$$

в силу (21). Точно так же доказывается, что $jl_1 \in I$ и $kl_1 \in I$.

Положим теперь

$$l = \frac{l_1}{\sqrt{-l_1^2}},$$

тогда

$$l^2 = -1,$$

и величины $i, l, il \in I$ удовлетворяют тем же условиям, что и величины u, v, w в предложении С). Так что мы имеем

$$il = -li.$$

Точно так же доказывается, что

$$jl = -lj \quad \text{и} \quad kl = -lk.$$

Теперь рассмотрим величину ilj. Мы имеем

$$ilj = i(-jl) = -kl, \quad ilj = -lij = -lk = kl.$$

Таким образом, мы приходим к выводу, что $2kl = 0$, что невозможно, так как характеристика тела L не равна двум.

Итак, теорема 3 полностью доказана. ■

Глава 6

Тополого-алгебраические тела

§ 18. Топологическое тело 164
§ 19. Топологические понятия
в топологическом теле L 173
§ 20. Теорема единственности 183
§ 21. p-адические числа 187
§ 22. Некоторые топологические свойства
поля K_0^p p-адических чисел 203
§ 23. Поле рядов над полем вычетов 209
§ 24. О структуре несвязных локально
компактных топологических тел 218

Рассмотренные нами три алгебраических тела — поле действительных чисел, поле комплексных чисел и тело кватернионов — являются евклидовыми пространствами размерности 1, 2, 4 соответственно. Поскольку в этих пространствах имеется метрика, т. е. определено расстояние между двумя точками (см. гл. 4), то имеется и понятие сходимости.

Будем обозначать любое из трех упомянутых тел через K. Если

$$a_1, a_2, \ldots, a_n, \ldots$$

есть некоторая последовательность элементов пространства K, то известно, что означает, что она сходится к элементу a. Это значит, что

• **Сходимость последовательности**

расстояние $\rho(a_n, a)$ между точками a_n и a с ростом n стремится к нулю. Этот факт в виде формулы записывается так:

$$\lim_{n\to\infty} a_n = a. \qquad (1)$$

Топологическое пространство •

Тот факт, что в пространстве K определена сходимость, мы будем выражать, говоря, что K является топологическим пространством.

Легко доказывается, что

алгебраические операции, имеющиеся в теле K, являются непрерывными относительно имеющейся там топологии. Более точно, если последовательность

$$b_1, b_2, \ldots, b_n, \ldots$$

элементов тела K сходится к элементу b, т. е. если

$$\lim_{n\to\infty} b_n = b,$$

то выполнены условия непрерывности операций сложения и умножения. Именно, имеют место соотношения

$$\lim_{n\to\infty}(a_n + b_n) = a + b, \qquad \lim_{n\to\infty} a_n b_n = ab.$$

Это показывает, что операции сложения и умножения, имеющиеся в K, являются непрерывными относительно топологии, имеющейся в K.

Так как операции вычитания и деления сводятся к операциям взятия противоположного и обратного элементов, то непрерывность операций вычитания и деления можно сформулировать следующим образом:

$$\lim_{n\to\infty}(-a_n) = -a.$$

Если $a \neq 0$, то

$$\lim_{n\to\infty} a_n^{-1} = a^{-1}.$$

• **Топологическое тело**

Если в некотором алгебраическом теле L имеется топология, т. е. имеется сходимость, иначе говоря, известно, что означает соотношение (1), а операции, имеющиеся в теле L, непрерывны в отношении этой топологии, то такое тело называется тополого-алгебраическим, или, короче, топологическим телом, если уже известно, что под телом подразумевается алгебраическое тело.

Изучение топологических тел составляет часть топологической алгебры. Интересным оказывается тот факт, что топологических тел существует не слишком много и все их можно обозримым образом описать. В § 18 дается аккуратное определение топологического тела.

Ясно, что соотношение (1) должно иметь место, если все элементы последовательности

$$a_1, a_2, \ldots, a_n, \ldots,$$

начиная с некоторого номера, совпадают между собой. Но если соотношение (1) имеет место только при этом условии, то существование сходимости не вносит ничего нового в алгебраическое тело L, и тела с такой топологией мы не будем рассматривать и не будем называть их топологическими.

Глава 6

§ 18. Топологическое тело

Как было сказано в начале настоящей главы, алгебраическое тело становится топологическим телом, если в нем наряду с алгебраическими операциями имеется еще операция предельного перехода, причем алгебраические операции непрерывны в отношении этого предельного перехода. Три рассмотренных нами тела являются евклидовыми пространствами, и предельный переход в них определяется при помощи расстояния. Так что для определения его нужно знать расстояние между каждыми двумя его точками. Можно, однако, определить предельный переход, не пользуясь расстоянием, т. е. способом, пригодным для общих топологических тел, пользуясь при этом операцией вычитания, определенной в K. В самом деле, утверждение, что расстояние между a_n и a стремится к нулю, равносильно утверждению, что $|a_n - a| \to 0$. Для того чтобы определить операцию предельного перехода (см. (1)), обозначим через U_n совокупность всех элементов x тела K таких, что

$$|x| < \frac{1}{n}. \tag{2}$$

Так что U_n есть шар радиуса $1/n$ с центром в нуле. Для того чтобы было выполнено соотношение (1), необходимо и достаточно, чтобы выполнялось следующее условие: для каждого

натурального числа n найдется такое натуральное число r, что при $p > r$ имеем

$$(a_p - a) \in U_n.$$

Перенесем теперь это построение на любое тело L. Для этого введем предварительно некоторые обозначения.

А) Если X и Y — два множества из L, то через $X+Y$ обозначим совокупность всех величин вида

$$x + y, \quad \text{где} \quad x \in X, \quad y \in Y,$$

а через $X-Y$ — все элементы вида

$$x - y, \quad \text{где} \quad x \in X, \quad y \in Y.$$

Далее, через XY обозначим совокупность всех элементов вида

$$xy, \quad \text{где} \quad x \in X, \quad y \in Y,$$

а через XY^{-1} совокупность всех элементов вида

$$xy^{-1}, \quad \text{где} \quad x \in X, \quad y \in Y.$$

Так как при $y = 0$ величина y^{-1} не определена, то в последней формуле будем рассматривать лишь те элементы $y \in Y$, которые не равны нулю.

Определение 3

• **Полная система окрестностей**

Убывающая бесконечная последовательность множеств

$$U_1, U_2, \ldots, U_n, \ldots \qquad (3)$$

из L, содержащих нуль тела L и пересекающихся только по нулю,

$$0 \in U_{n+1} \subset U_n,$$

называется полной системой окрестностей нуля топологического тела L, если выполнены следующие пять условий.

a) Для всякого натурального числа n существует настолько большое натуральное число p, что

$$(U_p + U_p) \subset U_n.$$

b) Для всякого натурального числа n существует настолько большое натуральное число p, что

$$U_p U_p \subset U_n.$$

c) Для всякого натурального числа n существует настолько большое натуральное число p, что

$$-U_p \subset U_n.$$

d) (Напомним, что через e обозначается единица тела L.) Для всякого натурального числа n существует настолько большое натуральное число p, что

$$(e + U_p)^{-1} \subset e + U_n.$$

е) Какой бы ни был элемент $a \in L$, для всякого натурального числа n существует настолько большое натуральное число p, что

$$U_p a \subset U_n, \quad a U_p \subset U_n.$$

В) Пользуясь полной системой окрестностей нуля (см. (3)), в теле L понятие сходимости можно определить точно так же, как это было сделано для тела K.

Определение 4

• **Понятие сходимости**

Последовательность

$$a_1, a_2, \ldots, a_n, \ldots$$

элементов из L считается сходящейся к элементу a,

$$\lim_{n\to\infty} a_n = a,$$

если для каждого натурального числа n существует настолько большое натуральное число r, что при $p > r$ имеем

$$(a_p - a) \in U_n.$$

Тогда имеет место теорема:

Теорема 4. *Если определить сходимость в L способом, указанным в* В), *то алгебраические операции, имеющиеся в теле L, оказываются*

Непрерывность алгебраических операций относительно заданной сходимости

непрерывными относительно этой сходимости. Именно, если имеют место соотношения

$$\lim_{n\to\infty} a_n = a, \quad \lim_{n\to\infty} b_n = b, \tag{4}$$

то

$$\lim_{n\to\infty} (a_n + b_n) = a + b, \tag{5}$$

$$\lim_{n\to\infty} (a_n b_n) = ab, \tag{6}$$

$$\lim_{n\to\infty} (-a_n) = -a. \tag{7}$$

Если $a \neq 0$, *то имеет место соотношение*

$$\lim_{n\to\infty} a_n^{-1} = a^{-1}. \tag{8}$$

Таким образом, последовательностью (3) *определена топология в теле* L.

Доказательство. Докажем соотношение (5). Из формулы (4) следует, что при произвольно большом натуральном числе r найдется такое большое натуральное число p, что при $p > r$ имеем

$$a_p \in a + U_r, \quad b_p \in b + U_r.$$

Тогда

$$a_p + b_p \in a + b + U_r + U_r. \tag{9}$$

В силу условия a) определения 3 для каждого натурального числа n найдется настолько большое натуральное число r, что

$$U_r + U_r \subset U_n.$$

Тогда из (9) следует

$$(a_p + b_p) - (a + b) \in U_n.$$

Таким образом, соотношение (5) доказано.

Докажем соотношение (6). Из (4) следует, что для произвольного натурального числа r найдется настолько большое натуральное число p, что при $p > r$ имеем

$$a_p \in a + U_r, \quad b_p \in b + U_r.$$

Тогда

$$a_p b_p \in (a + U_r)(b + U_r) = ab + aU_r + U_r b + U_r U_r.$$

В силу условий a), b) и e) определения 3 для всякого натурального числа n найдется настолько большое натуральное число r, что

$$aU_r + U_r b + U_r U_r \subset U_n.$$

Таким образом,

$$(a_p b_p - ab) \in U_n,$$

и, следовательно, соотношение (6) доказано.

Соотношение (7) следует из условия c) определения 3.

Докажем соотношение (8). Рассмотрим величину $a_p^{-1}a$. Для этого предварительно рассмотрим обратную ей величину $a^{-1}a_p$. Из формулы (4) следует, что для произвольно большого натурального числа q найдется настолько большое натуральное число p, что

$$a_p \in a + U_q.$$

Далее, для произвольно большого натурального числа s найдется настолько большое натуральное число q, что

$$a^{-1}(a + U_q) = (e + a^{-1}U_q) \subset e + U_s$$

(см. условие e) определения 3). Отсюда получаем, что при достаточно большом натуральном p выполняется включение

$$a^{-1}a_p \in (e + U_s).$$

В силу условия d) определения 3 из этого следует

$$a_p^{-1}a \in e + U_r,$$

где r — произвольно большое натуральное число, если p достаточно велико. Далее, мы имеем

$$(a_p^{-1}a - e) \in U_r, \quad (a_p^{-1} - a^{-1}) \in U_r a^{-1}.$$

В силу условия e) определения 3 для произвольного натурального числа n найдется настолько большое натуральное число r, что

$$U_r a^{-1} \subset U_n.$$

Таким образом,

$$(a_p^{-1} - a^{-1}) \in U_n.$$

И, следовательно, соотношение (8) доказано. Итак, теорема 4 доказана. ■

C) Оказывается, что

система окрестностей

$$U_1, U_2, \ldots, U_n, \ldots, \tag{10}$$

определенная в любом из трех рассмотренных тел K соотношением (2), *удовлетворяет всем условиям определения* 3.

Доказательство. Докажем это утверждение. Мы имеем для окрестностей (10)

$$U_p + U_p \in U_n,$$

где $p > 2n$. Из этого следует условие a) определения 3.

Далее имеем

$$U_p U_p \subset U_{p^2}.$$

Из этого следует условие b) определения 3.

Далее имеем

$$-U_n = U_n.$$

Из этого следует условие c) определения 3.

Далее, если a — произвольный элемент тела K и $x \in U_p$, то

$$|ax| = |a| \cdot |x| < |a| \frac{1}{p}.$$

Следовательно, при p, больших $n|a|$, выполняется условие e) из определения 3.

Пусть x — произвольный элемент окрестностей U_n (см. (2)). Тогда множество

$$(e+U_n)^{-1}$$

состоит из всех элементов вида

$$(e+x)^{-1}.$$

Но мы имеем

$$(e+x)^{-1} = e - x + x^2 - x^3 + \dots . \qquad (11)$$

Эта формула, известная для действительных и комплексных чисел, верна также и для кватернионов, так как все кватернионы, входящие в нее, перестановочны между собой при перемножении. Формула (11) может быть переписана в виде

$$(e+x)^{-1} = e + y,$$

где

$$y = -x + x^2 - x^3 + \dots,$$

так что

$$|y| \leqslant \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + \dots = \frac{1}{n-1}.$$

Таким образом,

$$(e+U_n)^{-1} \in e + U_{n-1}.$$

Из этого вытекает условие d) определения 3. ■

§ 19. Топологические понятия в топологическом теле L

Здесь в топологическом теле L будут введены топологические понятия, общепринятые в топологии, знание которых, однако, в этой книге не предполагается.

А)

Пусть M — некоторое множество элементов пространства L. Точку $a \in L$ будем называть предельной для множества M, если в множестве M найдется последовательность

$$a_1, a_2, \ldots, a_n, \ldots$$

попарно различных элементов, сходящихся к элементу a.

• **Предельная точка множества**

Множество M называется замкнутым, если все его предельные точки принадлежат ему.

• **Замкнутое множество**

Присоединяя к произвольному множеству M все его предельные точки, мы получим замыкание множества M, которое обозначают через $\overline{M}$. Если множество M вообще не имеет предельных точек, то через $\overline{M}$ обозначается оно само.

• **Замыкание множества**

Множество M называется замкнутым, если $M = \overline{M}$. Оказывается, что

замыкание $\overline{M}$ любого множества M замкнуто, т. е.

$$\boxed{\overline{\overline{M}} = \overline{M}.} \qquad (12)$$

Доказательство этого соотношения просто, но оно громоздко. Поэтому я дам только некоторые указания, как его провести.

Доказательство. Пусть

$$b_1, b_2, \ldots, b_n, \ldots \qquad (13)$$

— последовательность попарно различных точек из $\overline{M}$, сходящаяся к некоторой точке b. Требуется доказать, что $b \in \overline{M}$. Без нарушения общности мы можем считать, что все точки последовательности (13) не принадлежат M. К каждой точке b_n сходится некоторая последовательность B_n попарно различных точек из M.

В последовательности B_n выберем некоторую точку достаточно высокого номера в этой последовательности и обозначим ее через c_n. Тогда мы получим последовательность

$$c_1, c_2, \ldots, c_n, \ldots$$

попарно различных точек множества M, сходящуюся к b. Таким образом, b есть предельная точка для M, и соотношение (12) доказано. Так устанавливается, что множество $\overline{M}$ замкнуто. ■

B)

Множество Q пространства L называется компактным, если каждое бесконечное подмножество M множества Q имеет хотя бы одну предельную точку, принадлежащую Q.

• **Компактное множество**

C)

Топологическое тело L называется локально компактным, если существует окрестность нуля U_n последовательности (3) пространства L, замыкание которой $\overline{U}_n$ компактно.

• **Локально компактное множество**

D)

Замкнутое бесконечное множество M из L называется связным, если его нельзя представить как объединение двух непустых замкнутых подмножеств M_1 и M_2, не имеющих общих точек.

• **Связное множество**

Это значит, что M нельзя разбить на сумму двух замкнутых непересекающихся подмножеств M_1 и M_2.

E) Оказывается, что

все три рассмотренных нами до сих пор тела K, т. е. поле действительных чисел, поле комплексных чисел и тело кватернионов, локально компактны и связны.

Так как все три тела K являются евклидовыми пространствами, то мы предпошлем доказательству предложения Е) рассмотрение n-мерного евклидова пространства A^n, состоящего из векторов

$$x = (x^1, x^2, \ldots, x^n).$$

Доказательство. Мы примем без доказательства, что множество действительных чисел

$$-1 \leqslant t \leqslant 1$$

является множеством связным и компактным.

В пространстве A^n рассмотрим куб Q, определяемый условиями

$$-1 \leqslant x^i \leqslant 1, \quad i = 1, 2, \ldots, n,$$

и докажем, что куб этот является компактным множеством. В кубе Q рассмотрим бесконечную последовательность попарно различных точек

$$x_1, x_2, \ldots, x_p, \ldots . \tag{14}$$

Пусть

$$x_1^i, x_2^i, \ldots, x_p^i, \ldots, \quad i = 1, \ldots, n, \tag{15}$$

— последовательность i-х координат точек (14). Заметим, что все числа этой последовательности принадлежат отрезку $-1 \leqslant t \leqslant 1$, который компактен. Поэтому из последовательности чисел (15) при $i = 1$ можно выбрать сходящуюся

подпоследовательность X^1, которая, вообще говоря, не состоит из попарно различных чисел.

Последовательность X^1 соответствует подпоследовательности Y^1 векторов (14). Вторые координаты последовательности Y^1 составляют последовательность чисел, принадлежащих отрезку $-1 \leqslant t \leqslant 1$. Из последовательности этих вторых координат выберем сходящуюся подпоследовательность, которой соответствует подпоследовательность Y^2 последовательности векторов (14). Продолжая так, получим подпоследовательность Y^n последовательности векторов (14), сходящуюся к некоторой точке y. Таким образом, установлено, что из последовательности попарно различных векторов (14) можно выбрать подпоследовательность Y^n, сходящуюся к некоторому вектору y, принадлежащему кубу Q. Из этого непосредственно вытекает, что куб Q компактен. В самом деле, если M — некоторое бесконечное множество точек куба Q, то из M можно выбрать некоторую последовательность (14) попарно различных векторов. Последовательность эта сходится к вектору y и потому является предельной точкой для множества M, а это и означает компактность куба Q.

В каждом из трех евклидовых пространств K, соответствующих трем рассмотренным телам K, куб Q является компактным множеством. Любая окрестность вида U_p (см. (2)) принадлежит кубу Q, а потому замыкание ее $\overline{U}_p$ ком-

пактно. Таким образом, все три рассмотренных тела K локально компактны.

Докажем теперь, что евклидово пространство A^n связно. Допустим противоположное, т. е. что его можно разбить на два замкнутых непересекающихся множества M_1 и M_2. Рассмотрим теперь в пространстве A^n прямолинейный отрезок

$$x(t) = \left(\frac{1}{2} - \frac{1}{2}t\right)x_{-1} + \left(\frac{1}{2} + \frac{1}{2}t\right)x_1, \qquad -1 \leqslant t \leqslant 1, \tag{16}$$

такой, что начальная точка отрезка $x(-1) = x_{-1}$ принадлежит M_1, а конец отрезка $x(1) = x_1$ принадлежит M_2. Пересечение рассматриваемого отрезка (16) с M_1 обозначим через M_1', а пересечение этого отрезка с множеством M_2 обозначим через M_2'. Множества M_1' и M_2' являются замкнутыми подмножествами отрезка (16). Так как пространство A^n распадается в сумму замкнутых непересекающихся множеств M_1 и M_2, то отрезок (16) распался в сумму замкнутых непересекающихся множеств M_1' и M_2', а это противоречит предположению о том, что отрезок этот есть связное множество.

Итак, доказано, что любое евклидово векторное пространство A^n связно. Следовательно, и все три рассмотренные нами тела K связны.

Итак, утверждение Е) доказано. ■

F)

• **Последовательность Коши**

Последовательность

$$a_1, a_2, \ldots, a_n, \ldots \qquad (17)$$

элементов топологического тела L называется последовательностью Коши, если для всякого натурального числа n можно найти настолько большое натуральное число r, что при $p > r$, $q > r$ имеем

$$(a_p - a_q) \in U_n.$$

Огюстен-Луи Коши (1789–1857)

Оказывается, что

если последовательность (17) *сходится в топологическом теле* L, *то она является последовательностью Коши. Однако последовательность Коши не всегда сходится. Но если какая-нибудь ее бесконечная подпоследовательность сходится, то сама последовательность Коши тоже сходится.*

Докажем, что

если последовательность (17) *сходится, то она является последовательностью Коши.*

Доказательство. Если

$$\lim_{n\to\infty} a_n = a,$$

то из этого следует, что для всякого натурального числа s найдется такое натуральное число r, что

при $p > r$, $q > r$ имеем

$$(a_p - a) \in U_s, \quad (a_q - a) \in U_s$$

(см. В) § 18). Отсюда

$$a_p - a_q = (a_p - a) - (a_q - a) \in U_s - U_s.$$

Но тогда в силу условий а) и с) определения 3 при достаточно большом s имеем

$$(U_s - U_s) \subset U_n,$$

где n — произвольно большое натуральное число.

Таким образом, доказано, что последовательность (17), сходящаяся к элементу a, является последовательностью Коши. ■

Докажем теперь, что

если последовательность (17) *есть последовательность Коши, а некоторая ее бесконечная подпоследовательность сходится к элементу* a, *то сама последовательность* (17) *сходится к этому элементу.*

Доказательство. Так как некоторая бесконечная подпоследовательность последовательности (17) сходится к a, то в последовательности (17) существуют элементы с произвольно большими номерами p такие, что

$$(a_p - a) \in U_s,$$

где s — произвольно большое натуральное число. Так как последовательность (17) является

последовательностью Коши, то для натурального числа s существует настолько большое натуральное число r, что при $p > r$, $q > r$ имеем

$$(a_p - a_q) \in U_s.$$

Так как

$$(a_p - a) \in U_s,$$

то

$$a_q - a = (a_q - a_p) + (a_p - a) \in -U_s + U_s.$$

Таким образом,

$$(a_q - a) \in U_n,$$

и последовательность (17) сходится к a. ■

G)

Топологическое тело L называется полным, если всякая последовательность Коши в нем сходится.

• **Полное топологическое пространство**

Оказывается, что

всякое локально компактное тело L является полным.

Доказательство. Пусть

$$a_1, a_2, \ldots, a_p, \ldots \qquad (18)$$

— некоторая последовательность Коши тела L. Тогда согласно определению последовательности

Коши (см. F)) разность $a_p - a_q$ при достаточно больших p и q принадлежит некоторой окрестности U_n нуля тела L, причем n можно выбрать так, чтобы $\overline{U}_n$ было компактным. Отсюда вытекает, что из элементов последовательности (18) достаточно высокого номера можно выбрать такой элемент c, что при достаточно больших p и q имеем

$$(a_p - c) \in U_n, \quad (a_q - c) \in U_n.$$

Так как $\overline{U}_n$ компактно, то из последовательности

$$(a_1 - c),\ (a_2 - c),\ \ldots,\ (a_p - c),\ \ldots \qquad (19)$$

можно выбрать подпоследовательность, сходящуюся к некоторому элементу $b \in \overline{U}_n$. Из того, что последовательность (18) есть последовательность Коши, непосредственно следует, что последовательность (19) также является последовательностью Коши. А так как некоторая ее бесконечная подпоследовательность сходится к элементу $b \in \overline{U}_n$, то сама последовательность (19) сходится к b. Отсюда следует, что последовательность (18) сходится к элементу $b + c$. ■

Из предложения G) следует, что все три рассмотренные нами тела K являются полными (см. E)).

Пример. Приведем теперь пример неполного топологического тела. Таким примером является совокупность R всех рациональных чисел с системой окрестностей нуля (2). Причем U_n состоит

из всех рациональных чисел x, удовлетворяющих условию $|x| < 1/n$. Это те же самые условия, которыми определены окрестности U_n в поле D действительных чисел. В этом смысле топологическое поле R рациональных чисел является подполем поля D действительных чисел. Если теперь

$$a_1, a_2, \ldots, a_n, \ldots \qquad (20)$$

— некоторая последовательность рациональных чисел, удовлетворяющая условию Коши, то как совокупность элементов тела D она сходится к числу a. Если a не является рациональным числом, то последовательность (20) не сходится в топологическом теле R и, следовательно, топологическое тело R не является полным. Топологическое тело D, содержащее в себе топологическое тело R, является пополнением R до полного тела D в том смысле, что каждый элемент тела D является предельным для некоторой последовательности Коши из тела R.

В § 21 будет дана другая топология в теле рациональных чисел R, приводящая к другому пополнению тела R до полного тела, отличного от тела действительных чисел.

§ 20. Теорема единственности

Действительные и комплексные числа возникли в математике в результате длительного развития понятия числа в основном из-за потребностей

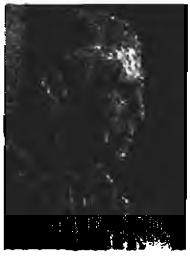
практики, а частично в результате логики развития самой математики. Необходимость считать предметы вызвала появление натуральных, т. е. положительных целых чисел. Дроби появились при торговых расчетах и при измерениях величин. Развитие геометрии привело к выяснению того факта, что диагональ квадрата со стороной единица не может быть измерена точно рациональным числом, хотя может быть измерена им с произвольной точностью. Таким образом, внутреннее развитие математики привело к появлению длин, неизмеримых при помощи рациональных чисел. Следовательно, из внутренних потребностей математики возникли нерациональные числа, которые стали называть иррациональными.

Вначале появилась потребность лишь в небольшом количестве иррациональных чисел, но требование логической стройности математики привело к построению всех действительных чисел. В частности, для стройности математической теории было очень важно, чтобы всякая последовательность Коши сходилась. Но для рациональных чисел это неверно. Последовательность Коши рациональных чисел может не сходиться к рациональному числу, она сходится к действительному числу. Таким образом, поле рациональных чисел нужно было дополнить до поля действительных чисел. Отрицательные числа появились в основном из внутренних математи-

ческих соображений для того, чтобы вычитание всегда было возможно, хотя отрицательные числа имели и практическое толкование. Можно было толковать отрицательное число как долг. Комплексные числа возникли из внутренних математических соображений, так как при некоторых вычислениях появилась необходимость извлекать квадратные корни из отрицательных чисел. Комплексные числа оправдывались в значительной степени еще и тем, что всякий многочлен с действительными коэффициентами всегда имеет корень, быть может, не действительный, а комплексный. Комплексные числа позволили очень сильно упростить некоторые вычисления и дали новую теорию комплексных функций комплексного переменного, играющую важную практическую и теоретическую роль. Таким образом, действительные и комплексные числа являются продуктом исторического развития математики. Кватернионы были построены из обобщательских соображений. Это была попытка обобщить комплексные числа, но она не дала ценных результатов, так как отсутствие коммутативности не дает возможности развить теорию кватернионных функций. По сравнению с тем значением, которое имеют действительные и комплексные числа в математике, роль кватернионов ничтожна.

Так как действительные и комплексные числа появились в математике в результате опреде-

ленного пути развития, который мог бы оказаться и другим, то возникает естественный вопрос: не мог ли этот другой путь развития привести к другим числам, аналогичным действительным и комплексным, но все же к другим? Для того чтобы решить этот вопрос, нужно точно сформулировать те требования, какие следует предъявить к объектам, которые могли бы играть роль чисел, и выяснить, существуют ли другие системы объектов, удовлетворяющие этим требованиям. Нетрудно прийти к убеждению, что система объектов, удовлетворяющая требованиям, предъявляемым к числам, должна представлять собой топологическое тело. Если наложить на это тело еще дополнительные требования о локальной компактности и связности, что довольно естественно, то оказывается, что имеет место следующая теорема, которая была доказана мною в 1931 году.



Лев Семенович Понтрягин (1908–1988)

Теорема Понтрягина

Теорема 5. *Всякое локально компактное связное топологическое тело является либо полем действительных чисел, либо полем комплексных чисел, либо телом кватернионов.*

Теорема эта показывает, в частности, что действительные и комплексные числа являются не случайным продуктом исторического развития, а по необходимости возникли в математике как единственные объекты, пригодные к употреблению в роли чисел.

§ 21. *p*-адические числа

Совокупность R всех рациональных чисел составляет поле в силу тех правил сложения и умножения, которые в нем определены. При этом нулем сложения является число нуль, а единицей умножения — число единица. p-адические числа появляются в результате введения в поле R своеобразной топологии, зависящей от заданного простого числа p. Интуитивный смысл этой топологии заключается в том, что рациональное число r считается тем меньше, чем лучше оно делится на заданное простое число p. Запишем число r в форме

$$r = \frac{a}{b} p^n. \tag{21}$$

Здесь b — натуральное число, не делящееся на p, а a — произвольное целое число. Число n может быть положительным, отрицательным или нулем. Если число a делится на p, то показатель n можно увеличить, вынеся множитель из a. Рациональное число r считается тем меньше, чем больше целое число n. Формально это осуществляется введением в поле R системы окрестностей нуля, удовлетворяющих определению 3.

• **p-топология в поле рациональных чисел**

А) Последовательность

$$U_1, U_2, \ldots, U_n, \ldots, \tag{22}$$

фигурирующая в определении 3, задается следующим образом. Окрестность U_n считается состоящей из всех чисел вида (21) с заданным n. Непосредственно видно, что последовательность (22) убывающая и что нуль является единственной общей точкой всех множеств (22). Оказывается, что

для последовательности (22) *выполнены все условия определения* 3.

Доказательство. Пусть r_1 и r_2 — два числа из окрестности U_n, так что они могут быть записаны в виде

$$r_1 = \frac{a_1}{b_1}p^n, \quad r_2 = \frac{a_2}{b_2}p^n.$$

Мы имеем

$$r_1 + r_2 = \frac{a_1b_2 + b_1a_2}{b_1b_2}p^n.$$

Из этой формулы следует

$$U_n + U_n \subset U_n.$$

Но так как $0 \in U_n$, то вместо предыдущего включения имеет место равенство

$$U_n + U_n = U_n.$$

Из этого следует, что условие а) определения 3 выполнено.

Далее, мы имеем

$$r_1r_2 = \frac{a_1a_2}{b_1b_2}p^{2n}.$$

Таким образом, получаем

$$U_n U_n \subset U_{2n}.$$

Таким образом, условие b) определения 3 выполнено. Из записи (21) числа r следует, что если $r \in U_n$, то $-r \in U_n$. Таким образом, мы имеем

$$-U_n = U_n.$$

Это значит, что условие c) определения 3 выполнено.

Докажем теперь, что и условие d) определения 3 выполнено.

Если r есть произвольный элемент множества U_n, то множество $(1+U_n)^{-1}$ состоит из всех элементов вида $\dfrac{1}{1+r}$. Эту дробь нам нужно записать в виде

$$\frac{1}{1+r} = 1 + s.$$

Из последней формулы получаем

$$s = \frac{-a}{b + ap^n} p^n.$$

Отсюда следует, что $s \in U_n$, и потому

$$(1+U_n)^{-1} \subset 1 + U_n.$$

Следовательно, условие d) определения 3 выполнено.

Пусть r — произвольное число из R. В силу соотношения (21) его можно записать в виде

$$r = \frac{a}{b} p^k.$$

Здесь b не делится на p, а k — произвольное целое число. Умножая окрестность U_n на число r, заданное последней формулой, получаем, очевидно,

$$rU_n \subset U_{n+k}.$$

Из этого видно, что условие е) определения 3 выполнено. ■

При построении p-адических чисел используется аналог разложения целого неотрицательного числа в сумму степеней числа p. Разложение это аналогично тому, которое мы употребляем при десятичной записи целых неотрицательных чисел, но там вместо p фигурирует число 10. Возможность такой записи почти очевидна, но мы все-таки ее сформулируем и докажем.

Построение p-адических чисел

В) *Каждое целое неотрицательное число x может быть записано в виде*

$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_n p^n, \qquad (23)$$

где коэффициенты $x_0, x_1, \ldots, x_n$ — целые числа, удовлетворяющие неравенствам

$$0 \leqslant x_i \leqslant p-1, \quad i = 0, 1, \ldots, n.$$

Доказательство. При $x = 0$ в разложении (23) все коэффициенты равны нулю и оно имеет место. При $x > 0$ доказательство будем вести индуктивно, именно, мы будем считать, что для всякого числа $x' < x$ разложение (23) имеет место.

Рассмотрим бесконечную геометрическую прогрессию

$$1, p, p^2, \ldots, p^n, p^{n+1}, \ldots .$$

Каждое натуральное число x непременно попадет в один из промежутков между двумя соседними членами этой прогрессии. Допустим, что имеют место неравенства:

$$p^n \leqslant x < p^{n+1}.$$

Разделим теперь число x на число p^n. Тогда мы получим равенство

$$x = x_n p^n + x'. \qquad (24)$$

Здесь

$$x' < p^n, \quad 0 \leqslant x_n \leqslant p - 1,$$

так как если бы x_n было больше или равно p, то x было бы больше или равно p^{n+1}, что противоречит предположению. Так как число $x' < p^n \leqslant x$, то оно разлагается в сумму, аналогичную (23), причем в ней присутствует не более чем $(n-1)$-я степень p. Из этого и из равенства (24) вытекает разложение (23). ■

Мы записали в форме (23) каждое целое неотрицательное число из R. Но отрицательное целое число нельзя записать в форме (23). Точно так же рациональное число вида (21) не всегда можно записать в форме (23). Кроме того,

поле R с заданной в нем при помощи A) топологией не является полным.

Поэтому мы будем рассматривать величины, несколько обобщив выражение (23). Именно, мы будем рассматривать бесконечные ряды по степеням p, включающие, быть может, конечное число отрицательных степеней, и определим алгебраические действия над ними.

Поле K_0^p • p-адических чисел

С) Обозначим через K_0^p совокупность всех рядов вида

$$x = \sum_{i=k}^{\infty} x_i p^i; \tag{25}$$

здесь коэффициенты x_i суть целые числа, удовлетворяющие неравенствам

$$0 \leqslant x_i \leqslant p-1, \quad i = k, k+1, \ldots . \tag{26}$$

В множестве K_0^p мы введем операции сложения и умножения так, что K_0^p превратится в поле, а также топологию — так, что поле K_0^p станет топологическим полем. Будет установлено, что поле R с топологией, введенной в нем в А), содержится в топологическом поле K_0^p и что каждый элемент топологического поля K_0^p является предельным для содержащегося в нем поля R.

Операция • исправления коэффициентов

При построении алгебраических операций в поле K_0^p мы будем производить операцию исправления коэффициентов, которую опишем сперва в общем виде.

Операция эта соответствует принятой в арифметике фразе «7 пишем, 2 в уме», кото-

рая произносится при сложении и умножении целых чисел, взятых в десятичной записи.

D) Пусть

$$w = \sum_{i=k}^{\infty} w_i p^i, \tag{27}$$

где коэффициенты w_i могут уже не удовлетворять неравенствам типа (26). Если w_k не удовлетворяет неравенствам

$$0 \leqslant w_k \leqslant p - 1,$$

то существует целое число z_k, удовлетворяющее неравенствам

$$0 \leqslant z_k \leqslant p - 1$$

и сравнимое с w_k по модулю p, т. е. такое, что

$$w_k = z_k + u_{k+1} p.$$

Подставим это значение w_k в сумму (27). Тогда получим следующее выражение для w:

$$w = z_k p^k + (u_{k+1} + w_{k+1}) p^{k+1} + \sum_{i=k+2}^{\infty} w_i p^i. \tag{28}$$

Если не выполнены неравенства

$$0 \leqslant u_{k+1} + w_{k+1} \leqslant p - 1,$$

то существует число z_{k+1}, удовлетворяющее неравенствам

$$0 \leqslant z_{k+1} \leqslant p - 1$$

и сравнимое с числом $u_{k+1}+w_{k+1}$ по модулю p, т. е. такое, что

$$u_{k+1}+w_{k+1}=z_{k+1}+u_{k+2}p.$$

Подставляя это значение в ряд (28), получим

$$w=z_kp^k+z_{k+1}p^{k+1}+(u_{k+2}+w_{k+2})p^{k+2}+\sum_{i=k+3}^{\infty}w_ip^i.$$

Продолжая этот процесс далее, получим для w вместо ряда (27) ряд

$$w=\sum_{i=k}^{\infty}z_ip^i$$

уже «нормального» вида, т. е. такой, что коэффициенты удовлетворяют неравенствам

$$0\leqslant z_i\leqslant p-1,\quad i=k,k+1,\ldots.$$

Алгебраические операции в K_0^p.

Определим теперь алгебраические операции в K_0^p.

Е) Пусть

$$y=\sum_{i=k}^{\infty}y_ip^i \tag{29}$$

есть произвольный элемент из множества K_0^p. Здесь k взято тем же, что и для ряда (25), но это не налагает никаких ограничений, так как некоторые коэффициенты в рядах (25) и (29) могут быть равны нулю. Складывая чисто формально

ряды (25) и (29), получим

$$x + y = \sum_{i=k}^{\infty} (x_i + y_i) p^i.$$

• **Сумма *p*-адических чисел**

Применяя к этому ряду операцию исправления коэффициентов, описанную в D), мы получим для суммы $x + y$ уже ряд в нормальной форме, т. е. элемент множества K_0^p, который и считается суммой $x + y$. Таким образом, сумма $x + y$ уже принадлежит множеству K_0^p. Разность $x - y$ определим сперва, произведя формально вычитание ряда (29) из ряда (25). Тогда получим

$$x - y = \sum_{i=k}^{\infty} (x_i - y_i) p^i.$$

• **Разность *p*-адических чисел**

Произведя исправление коэффициентов этого ряда по способу, указанному в D), мы получим для $x - y$ ряд «нормального» вида, т. е. элемент из K_0^p. Перемножая ряды x и y как степенные ряды по p, получим для произведения xy некоторый ряд по степеням p. Произведя исправление его коэффициентов по способу, указанному в D), мы получим для произведения xy ряд «нормального» вида, т. е. элемент из K_0^p. Итак, мы определили операции сложения, вычитания и умножения рядов вида (25). Для завершения построения

• **Произведение *p*-адических чисел**

алгебраических операций в поле K_0^p нам остается построить обратный элемент. Сделаем это.

Существование обратного элемента в K_0^p

F) Будем искать обратный элемент сперва для ряда

$$\widehat{x} = x_0 + x_1 p + x_2 p^2 + \dots, \qquad (30)$$

где $x_0 \neq 0$. Обратный элемент будем искать в виде ряда

$$y = y_0 + y_1 p + y_2 p^2 + \dots. \qquad (31)$$

Перемножая формально ряды $\widehat{x}, y$, мы получим

$$\widehat{x}y = w = w_0 + w_1 p + w_2 p^2 + \dots, \qquad (32)$$

где

$$w_i = x_0 y_i + x_1 y_{i-1} + \dots + x_i y_0.$$

Здесь ряд (31) должен быть подобран так, чтобы было выполнено соотношение $\widehat{x}y = 1$.

Таким образом, ряд (32) после поправки коэффициентов, описанной в D), должен получить вид

$$w = 1 + 0p + 0p^2 + \dots.$$

Согласно пункту D) исправленные коэффициенты ряда (32) записываются в виде

$$z_0 = w_0 - u_1 p;$$

$$z_i = w_i + u_i - u_{i+1} p =$$

$$= x_0 y_i + x_1 y_{i-1} + \dots + x_i y_0 + u_i - u_{i+1} p,$$

$$i = 1, 2, \dots.$$

Заметим прежде всего, что поскольку $x_0 \neq 0$, то существует обратный ему элемент из поля вычетов P^p по модулю p, т. е. такое число θ, что θx_0 сравнимо с единицей по модулю p.

Таким образом, первое из уравнений, которое нам нужно решить, а именно уравнение

$$z_0 = x_0 y_0 - u_1 p = 1,$$

имеет решение, именно, $y_0 = \theta$. При $i > 0$ нам нужно решать уравнения:

$$x_0 y_i + x_1 y_{i-1} + \ldots + x_i y_0 + u_i - u_{i+1} p = 0.$$

Уравнения эти можно решать последовательно с ростом i. Для уравнения с номером i появляется лишь одно новое неизвестное число y_i, которое стоит с коэффициентом x_0, потому уравнение это можно разрешить относительно y_i. Каждый раз мы можем выбирать решение y_i такое, чтобы были выполнены неравенства

$$0 \leqslant y_i \leqslant p - 1.$$

Таким образом, мы построим элемент y, обратный к элементу $\widehat{x}$ (см. (31)), причем $y_0 \neq 0$. Но каждый ряд вида (25), отличный от нуля, может быть записан как $p^l \widehat{x}$ (см. (30)) и обратный ему элемент (см. (31)):

$$(p^l \widehat{x})^{-1} = p^{-l} y.$$

В свою очередь каждый такой элемент может быть записан в виде (25) и потому принадлежит множеству K_0^p. Таким образом, для каждого

элемента множества K_0^p мы построили обратный элемент.

Для того чтобы доказать, что

K_0^p с введенными в нем операциями является полем,

нужно доказать еще ассоциативность сложения и умножения, а также дистрибутивность. Это не очевидно, так как после проведения каждой операции требуется править коэффициенты. Но доказательство этих фактов я проводить здесь не буду.

Введем теперь в поле K_0^p топологию при помощи окрестностей нуля, как это сделано в определении 3.

Полная система окрестностей нуля в поле K_0^p

G) Полную систему окрестностей нуля

$$U_1, U_2, \ldots, U_n, \ldots \tag{33}$$

в поле K_0^p определим, включив в окрестность U_n все ряды вида (25), в которых $k = n$, т. е. все ряды вида

$$x = x_n p^n + x_{n+1} p^{n+1} + \ldots . \tag{34}$$

Выпишем еще один ряд такого же вида

$$y = y_n p^n + y_{n+1} p^{n+1} + \ldots .$$

Каждый из этих рядов характеризуется тем, что первые n коэффициентов его равны нулю. Ока-

зывается, что

для системы множеств (33) *выполнены все условия определения* 3.

Доказательство. Очевидно, что последовательность (33) есть убывающая последовательность множеств, причем пересечение этих множеств содержит нуль и только нуль.

При формальном сложении x и y, входящих в U_n, мы получим ряд w, первые n коэффициентов которого равны нулю. При правке коэффициентов это обстоятельство не может быть нарушено. Таким образом, мы имеем

$$U_n + U_n \subset U_n.$$

Но так как U_n содержит нуль, то вместо последнего включения имеем равенство

$$U_n + U_n = U_n. \tag{35}$$

Таким образом, условие a) определения 3 выполнено.

При формальном перемножении рядов x и y мы получим ряд, низшей степенью p в котором будет $2n$, а предыдущие коэффициенты равны нулю. Это обстоятельство не может измениться при правке коэффициентов, так что

$$U_n U_n \subset U_{2n}.$$

Таким образом, условие b) определения 3 выполнено.

Преобразованием формального ряда $-x$ (см. (34)) мы получим ряд, первые n коэффициентов которого равны нулю. При правке коэффициентов это обстоятельство не может измениться. Таким образом, мы имеем

$$-U_n = U_n$$

Отсюда следует, что условие c) определения 3 выполнено.

Множество $(1 + U_n)^{-1}$ состоит из всех элементов вида $\dfrac{1}{1+x}$ (см. (34)). Представим этот элемент поля K_0^p в виде

$$\frac{1}{1+x} = 1 + y.$$

Отсюда $y = -\dfrac{x}{1+x}$. В силу F) элемент $(1+x)^{-1}$ есть элемент ряда (31), начинающийся с нулевой степени p. А так как ряд $-x$ начинается с n-й степени p, то мы получаем $y \in U_n$ и, следовательно,

$$(1 + U_n)^{-1} \subset 1 + U_n.$$

Таким образом, условие d) определения 3 выполнено.

Пусть x — ряд вида (25), т. е. произвольный элемент поля K_0^p. Ясно, что

$$xU_n \subset U_{n+k}.$$

Таким образом, условие e) определения 3 выполнено. ■

• **Вложение R в поле K_0^p**

Включим теперь поле R рациональных чисел в поле K_0^p с заданной в R p-адической топологией (см. А)). Элемент r (см. (21)), принадлежащий полю R, где b не делится на p, может быть записан в виде

$$ab^{-1}p^n.$$

Но элемент b^{-1} поля K_0^p записывается в виде

$$b^{-1} = y_0 + y_1 p + y_2 p^2 + \dots,$$

где $y_0 \neq 0$. Таким образом, элемент r включен в поле K_0^p. Причем окрестности (22), имеющиеся в R, переходят в окрестности (33) поля K_0^p. Таким образом, мы включили топологическое поле R в топологическое поле K_0^p с сохранением топологии. Для элемента x, заданного рядом (25), введем операцию $b_l(x)$ формулой

$$b_l(x) = \sum_{i=k}^{l-1} x_i p^i.$$

Ясно, что $b_l(x) \in R$.

Видно, что

$$x - b_l(x) \in U_l.$$

Отсюда следует, что

$$\lim_{n\to\infty} b_n(x) = x,$$

причем $b_n(x) \in R$. Таким образом,

каждый элемент поля K_0^p является пределом последовательности элементов вложенного в него поля R.

Пример. Для примера рассмотрим запись элемента -1 из поля K_0^p в форме (25), получающуюся после исправления коэффициентов (см. D)). Мы имеем

$$-1 = w = w_0 + w_1 p + w_2 p^2 + \ldots,$$

где $w_0 = -1$, $w_1 = 0$, $w_2 = 0$. Исправляя коэффициент w_0, мы получим $w_0 = z_0 + u_1 p$, где $z_0 = p - 1$; $u_1 = -1$.

Далее, $w_1 + u_1 = -1$. Поэтому в результате его исправления получаем $w_1 + u_1 = -1 = z_1 + u_2 p$, где $z_1 = p - 1$, $u_2 = -1$. Продолжая этот процесс дальше, мы получаем для $w = -1$ исправленный ряд

$$-1 = \sum_{i=0}^{\infty} (p-1)p^i,$$

иначе,

$$(p-1)(1 + p + p^2 + \ldots).$$

Бесконечный ряд, стоящий в скобках, сходится в топологическом поле K_0^p, так как p^i стремится к нулю с ростом i, и потому мы имеем

$$1 + p + p^2 + \ldots = \frac{1}{1-p}.$$

Таким образом, получаем

$$-1 = (p-1)\frac{1}{1-p} = -1,$$

что подтверждает правильность наших выкладок.

§ 22. Некоторые топологические свойства поля K_0^p p-адических чисел

А) *Пусть U_n — произвольная окрестность системы* (33). *Обозначим через θ_n совокупность всех точек из K_0^p, не входящих в U_n. Оказывается, что θ_n есть замкнутое множество.*

Доказательство. Допустим противоположное. Пусть

$$x^1, x^2, \ldots, x^q, \ldots \qquad (36)$$

— некоторая последовательность точек из θ_n, сходящаяся к точке $x \notin \theta_n$. Тогда $x \in U_n$. Так как последовательность (36) сходится к x, то согласно определению 4 это значит, в частности, что при достаточно большом q имеем

$$(x^q - x) \in U_n.$$

Тогда в силу (35) имеем:

$$x^q \in x + U_n \subset U_n.$$

И, следовательно, все элементы последовательности (36), начиная с достаточно большого номера, принадлежат U_n и не могут принадлежать θ_n. Таким образом, мы пришли к противоречию и, следовательно, предложение А) доказано. ■

Заметим, что p-адическое число x, заданное рядом (25), принадлежит окрестности U_n тогда и только тогда (см. (33)), когда $b_n(x) = 0$.

Наряду с p-адическим числом x, заданным рядом (25), рассмотрим произвольное p-адическое число y, заданное рядом (29).

B) *Разность $x - y$ p-адических чисел x и y (см. (25) и (29)) принадлежит окрестности U_n тогда и только тогда (см. (33)), когда имеет место равенство*

$$b_n(x) = b_n(y).$$

Доказательство. При построении разности $x - y$ мы сперва строим формальную разность между рядами (25) и (29), т. е. ряд

$$w = \sum_{i=k}^{\infty} w_i p^i = \sum_{i=k}^{\infty} (x_i - y_i) p^i. \qquad (37)$$

Пусть $x_l - y_l$ — первый из коэффициентов этого ряда, отличный от нуля. А это значит, что $x_l - y_l$ не сравнимо с нулем по модулю p. Таким образом, при правке коэффициентов ряда (37) первым отличным от нуля будет коэффициент z_l, и мы будем иметь

$$b_l(x) = b_l(y),$$

причем l — наибольшее число, удовлетворяющее этому условию. Отсюда вытекает правильность утверждения B). ■

C) *Для того чтобы последовательность*

$$x^1, x^2, \ldots, x^q, \ldots \qquad (38)$$

элементов топологического поля K_0^p *сходилась к элементу* x *этого поля, т. е. чтобы имело место равенство*

$$\lim_{q\to\infty} x^q = x, \tag{39}$$

необходимо и достаточно, чтобы для каждого натурального числа n *нашлось настолько большое натуральное число* r *такое, что при* $q > r$ *имеем:*

$$b_n(x^q) = b_n(x).$$

Доказательство. Согласно § 18 B) соотношение (39) выполняется тогда и только тогда, когда для произвольного натурального числа n найдется настолько большое натуральное число r, что при $q > r$ имеем

$$(x^q - x) \in U_n.$$

Но в силу предложения B) последнее включение имеет место тогда и только тогда, когда выполнено соотношение

$$b_n(x^q) = b_n(x).$$

Таким образом, утверждение C) доказано. ■

D) *Любая окрестность* U_ν (*см.* (33)) *замкнута и компактна.*

Доказательство. Докажем сперва замкнутость множества U_ν. Элементы окрестности U_ν характеризуются условием

$$b_\nu(x) = 0.$$

Если теперь предположить, что последовательность (38) целиком содержится в U_ν, то для всех достаточно больших натуральных чисел n имеет место равенство

$$b_n(x^q) = b_n(x) \tag{40}$$

(см. C)). Заметим теперь, что при $\nu < n$ для любого элемента y из K_0^p имеет место соотношение

$$b_\nu(b_n(y)) = b_\nu(y).$$

Если теперь имеет место равенство (40), то

$$b_\nu(x) = b_\nu(b_n(x)) = b_\nu(b_n(x^q)) = b_\nu(x^q) = 0.$$

Таким образом,

$$x \in U_\nu,$$

и, следовательно, U_ν замкнуто.

Докажем теперь компактность множества U_ν. В силу § 19 C) это означает локальную компактность топологического поля K_0^p и, следовательно, его полноту (см. § 19 G)).

Пусть M — бесконечное подмножество элементов из U_ν. Поскольку первый элемент разложения коэффициента x в ряд (25) может принимать лишь конечное число значений, а именно p, то в M можно выделить бесконечное множество M_k таких элементов из M, у которых коэффициенты x_k совпадают между собой в ряде (25). Точно так же в множестве M_k выделится бесконечное подмножество M_{k+1}, элементы x которого имеют одинаковые коэффициенты x_{k+1}.

И точно так же выделяется бесконечное подмножество M_{k+2} в множестве M_{k+1}, и мы получаем бесконечно убывающую последовательность подмножеств

$$M, M_k, M_{k+1}, M_{k+2}, \ldots,$$

причем для двух элементов x' и x'', принадлежащих M_l, имеем равенство

$$b_l(x') = b_l(x'').$$

Выберем теперь из множества M_l произвольный элемент x^l. Мы имеем (см. C))

$$\lim_{l\to\infty} x^l = x,$$

где x — некоторый элемент множества U_ν. Таким образом, компактность множества U_ν доказана.

Итак, предложение D) доказано. ■

Изучим теперь детальнее окрестность U_ν нуля поля K_0^p.

E) *Окрестность U_ν распадается в конечную сумму компактных замкнутых попарно непересекающихся множеств вида*

$$\boxed{x^\alpha + U_{\nu+l},} \qquad (41)$$

где x^α, $\alpha = 1, \ldots, p^l$, — различные элементы окрестности U_ν.

Доказательство. Пусть x — произвольный элемент из U_ν. Тогда

$$b_{\nu+l}(x) = x_\nu p^\nu + x_{\nu+1} p^{\nu+1} + \ldots + x_{\nu+l-1} p^{\nu+l-1} = x^\alpha$$

есть многочлен относительно p с l коэффициентами, каждый из которых может принимать p различных значений. Таким образом, последняя формула содержит ровно p^l различных многочленов. Эти многочлены мы обозначаем через x^α. Совокупность всех $x \in U_\nu$, для которых $b_{\nu+l}(x) = x^\alpha$, представляет собой сумму (41). Каждое из множеств (41) замкнуто и компактно. Далее, если $x^\alpha \neq x^\beta$, то соответствующие множества $x^\alpha + U_{\nu+l}$ и $x^\beta + U_{\nu+l}$ не пересекаются. Допустим противоположное, т. е. допустим, что имеется элемент y, принадлежащий этим двум множествам. Тогда мы получаем

$$b_{\nu+l}(y) = x^\alpha, \quad b_{\nu+l}(y) = x^\beta,$$

что невозможно, так как $x^\alpha \neq x^\beta$. Итак, предложение E) доказано. ∎

Оно показывает, что окрéстность U_ν разбита в сумму конéчного чúсла маленьких кусочков вида (41). Это может иметь место и для всего пространства K_0^p.

F) *В пространстве K_0^p нет связных замкнутых бесконечных подмножеств.*

Доказательство. Допустим, что M — связное замкнутое подмножество из K_0^p. Пусть y — какой-

нибудь его элемент. Тогда множество $M' = M - y$ связно и содержит нуль. Так как множество M' бесконечно, а окрестности U_n (см. (33)) пересекаются только по нулю, то найдется настолько большое натуральное число n, что окрестность U_n не содержит полностью всего множества M'.

Обозначим через M_1' пересечение $M' \cap U_n$, а через M_2' — пересечение $M' \cap \theta_n$ (см. A)). Множества M_1' и M_2' замкнуты и не пересекаются. Таким образом, множество M' не связно, а потому и не связно исходное множество M. Таким образом, мы пришли к противоречию, и утверждение F) доказано. ■

§ 23. Поле рядов над полем вычетов

• **Многочлен над полем вычетов**

Пусть P^p — поле вычетов по модулю заданного простого числа p (см. § 16). Выражение

$$a(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n, \quad (42)$$

где коэффициенты $a_0, a_1, \ldots, a_n$ суть вычеты по модулю p, называется многочленом над полем P^p.

Над многочленами вида (42) можно производить операции сложения, вычитания и умно-

жения, производя соответствующие действия как над элементами поля P^p.

Рациональное выражение над полем вычетов

Если $b(t)$ есть другой многочлен типа (42), то выражение

$$r = \frac{a(t)}{b(t)} \tag{43}$$

называется рациональным выражением над полем P^p.

Дроби вида (43) можно складывать, вычитать, умножать и делить по обычным правилам, так что совокупность всех этих дробей составляет поле P_t^p.

В поле P_t^p вводится топология, смысл которой заключается в том, что выражение (43) считается тем меньше, чем лучше оно делится на t.

Топология в поле рациональных выражений над полем вычетов

А) В поле P_t^p вводится топология при помощи последовательности окрестностей нуля:

$$U_1, U_2, \ldots, U_n, \ldots \tag{44}$$

(см. (33)), причем в окрестность U_n включаются все выражения вида

$$r = \frac{a(t)}{b(t)} t^n, \tag{45}$$

где предполагается, что многочлен $b(t)$ не делится на t, т. е. его свободный член $b_0 \neq 0$ в поле P^p. Прежде всего ясно, что последовательность (44)

есть убывающая последовательность, пересекающаяся только по нулю. Кроме того, оказывается, что

все пять условий определения 3 *для системы окрестностей нуля* (44) *выполнены.*

Доказательство. Если

$$r_1 = \frac{a_1(t)}{b_1(t)}t^n, \quad r_2 = \frac{a_2(t)}{b_2(t)}t^n$$

— два произвольных элемента из окрестности U_n, то ясно, что и их сумма есть элемент U_n. А так как $0 \in U_n$, то мы получаем следующее равенство:

$$U_n + U_n = U_n.$$

Из этого следует, что условие а) определения 3 выполнено.

Далее, мы имеем

$$r_1 r_2 = \frac{a_1(t)a_2(t)}{b_1(t)b_2(t)}t^{2n}.$$

При этом знаменатель дроби $b_1(t)b_2(t)$, очевидно, не делится на t. Таким образом, мы имеем

$$U_n U_n \subset U_{2n}.$$

Следовательно, условие в) определения 3 выполнено.

Далее, мы имеем (см. (45))

$$-r = -\frac{a(t)}{b(t)}t^n.$$

Отсюда получаем

$$-U_n = U_n,$$

и условие c) определения 3 выполнено.

Элемент (45) есть произвольный элемент окрестности U_n. Таким образом, произвольный элемент множества $(1+U_n)^{-1}$ записывается в виде $(1+r)^{-1}$. Если предположить, что

$$\frac{1}{1+r} = 1+s,$$

то для s мы получаем выражение

$$s = -\frac{a(t)}{b(t)+a(t)t^n}t^n.$$

Таким образом,

$$(1+U_n)^{-1} \subset 1+U_n,$$

и потому условие d) определения 3 выполнено.

Пусть

$$s = \frac{a(t)}{b(t)}t^k$$

— произвольный элемент поля P_t^p. Тогда мы получаем, очевидно,

$$sU_n \subset U_{n+k},$$

откуда следует, что условие e) определения 3 выполнено. ■

Итак, последовательность (44) является системой окрестностей нуля в теле P_t^p, в силу чего P_t^p становится топологическим полем. Оказывается, однако, что поле это не является локально

компактным. Для того чтобы включить его в локально компактное полное поле, мы рассмотрим всевозможные ряды относительно t с коэффициентами из P^p, включающие, быть может, конечное число отрицательных степеней t.

В)

• **Поле K_t^p**

Множество всех рядов вида

$$x = \sum_{i=k}^{\infty} x_i t^i, \qquad (46)$$

где коэффициенты x_i суть элементы поля вычетов P^p, а k — целое число, быть может, и отрицательное, обозначим через K_t^p.

• **Построение обратного элемента в K_t^p**

В множестве K_t^p естественным образом определяются операции сложения, вычитания и умножения. Для построения обратного элемента найдем сперва обратный элемент для ряда

$$\widehat{x} = x_0 + x_1 t + x_2 t^2 + \dots, \qquad (47)$$

где $x_0 \neq 0$. Обратный элемент обозначим через y и запишем его в виде

$$y = y_0 + y_1 t + y_2 t^2 + \dots . \qquad (48)$$

Произведение $\widehat{x}y$ обозначим через w. Тогда мы будем иметь

$$w = \sum_{i=0}^{\infty} w_i t^i,$$

где

$$w_i = x_0 y_i + x_1 y_{i-1} + \ldots + x_i y_0.$$

Для того, чтобы y был обратным элементом к $\widehat{x}$, достаточно, чтобы были выполнены условия

$$w_0 = 1, \quad w_i = 0, \quad i = 1, 2, \ldots . \qquad (49)$$

Первое из этих уравнений дает нам соотношение

$$x_0 y_0 = 1.$$

Это уравнение разрешимо относительно y_0 в поле P^p, так как $x_0 \neq 0$. Следующее уравнение последовательности (49) имеет вид

$$x_0 y_1 + x_1 y_0 = 0.$$

Его мы должны разрешить относительно y_1, что возможно, так как коэффициент при y_1 не равен нулю. Каждое следующее уравнение из ряда (49) содержит лишь один новый неизвестный элемент, входящий с ненулевым коэффициентом. Таким образом, элемент y (см. (48)), обратный к $\widehat{x}$, вычисляется, причем $y_0 \neq 0$. Произвольный ряд (46), не равный нулю, может быть записан в виде

$$x = t^l \widehat{x}$$

(см. (47)), и мы получаем

$$x^{-1} = t^{-l} y,$$

и обратный элемент для $x \neq 0$ построен. Таким образом,

K_t^p является полем.

Введем в этом поле топологию по способу, указанному в определении 3.

C) Последовательность

$$U_1, U_2, \ldots, U_n, \ldots \tag{50}$$

окрестностей нуля поля K_t^p определим, включив в окрестность U_n все ряды (46), в которых $k = n$. Прежде всего ясно, что последовательность (50) есть убывающая последовательность множеств, пересекающихся по нулю.

• **Система окрестностей нуля и топология в поле K_t^p**

Далее оказывается, что

для нее выполнены все пять условий определения 3.

Доказательство. Непосредственно проверяется, что имеют место соотношения

$$U_n + U_n = U_n; \quad U_n U_n = U_{2n}; \quad -U_n = U_n.$$

Отсюда следует, что условия a), b) и c) определения 3 выполнены.

Проверим условие d). Множество $(1+U_n)^{-1}$ состоит из всех элементов вида $(1+x)^{-1}$, где в ряде для x (46) $k = n$, $n \geqslant 1$. Таким образом, обратный элемент для $(1+x)$ существует (см. B)) и начинается с единицы, а далее идут степени t, начиная с n-й. В результате получаем

$$(1+U_n)^{-1} \subset (1+U_n),$$

и условие d) определения 3 выполнено.

Если теперь x (см. (46)) — произвольный элемент поля K_t^p, то ясно, что

$$xU_n \subset U_{n+k}.$$

Таким образом, условие е) определения 3 выполнено. ■

Итак,

система окрестностей (50) *определяет топологию в поле* K_t^p.

Вложим теперь P_t^p в поле K_t^p.

D) Каждый элемент r поля P_t^p записывается в виде (см. (43))

$$r = \frac{a(t)}{b(t)} t^n.$$

Так как многочлен $b(t)$ не делится на t, то в поле K_t^p он имеет обратный элемент $b^{-1}(t)$ (см. В)), и элемент r поля K_t^p записывается теперь в виде

$$r = a(t)b^{-1}(t)t^n$$

и входит в K_t^p. Таким образом,

Вложение P_t^p в поле K_t^p •

топологическое поле P_t^p *включено в топологическое поле* K_t^p, *причем всякая окрестность* U_n *из последовательности* (44) *оказывается вложенной в окрестность* U_n *последовательности* (50).

Следовательно,

топологическое поле P_t^p *вложено в топологическое поле* K_t^p *с сохранением топологии.*

E) Каждой сумме x (см. (46)) поставим в соответствие конечную сумму:

$$b_l(x) = \sum_{i=k}^{l-1} x_i t^i.$$

Прежде всего ясно, что условие $b_l(x) = 0$ эквивалентно условию $x \in U_l$. Отсюда следует, что соотношение

$$\lim_{q\to\infty} x^q = x$$

имеет место тогда и только тогда, когда для произвольного натурального числа n можно найти такое натуральное число r, что при $q > r$ имеем:

$$b_n(x^q) = b_n(x). \qquad (51)$$

Из этого условия непосредственно вытекает, что

$$\lim_{n\to\infty} b_n(x) = x,$$

но $b_n(x)$ есть элемент поля P_t^p. Итак,

поле P_t^p, вложенное в поле K_t^p, имеет своим замыканием все поле K_t^p.

• **Поле K_t^p не содержит связных множеств**

F) Построим теперь взаимно однозначное отображение f пространства K_t^p на пространство K_0^p p-адических чисел. Для построения отображения f в ряде (46) заменим каждый вычет x_i содержащимся в нем числом x_i, удовлетворяющим неравенству $0 \leqslant x_i \leqslant p-1$, а букву t — простым числом p. Тогда ряд (46) превратится

в p-адическое число $f(x)$. При этом отображении алгебраические операции не сохраняются, так как в поле p-адических чисел имеет место правка коэффициентов. Но сходимость сохраняется (см. (51), (40)). Именно, если

$$\lim_{q\to\infty} x^q = x, \tag{52}$$

то

$$\lim_{q\to\infty} f(x^q) = f(x).$$

Наоборот, из последнего соотношения следует (52). Из предложения F) следует, что

поле K_t^p не содержит связных множеств.

§ 24. О структуре несвязных локально компактных топологических тел

В то время как локально компактные связные тела полностью изучены, о несвязных локально компактных телах я могу привести здесь теорему Ковальского, доказанную им в 1953 году.

Теорема о разрывности локально компактного несвязного тела

Теорема 6. *Локально компактное несвязное тело L непременно всюду разрывно, то есть не содержит связных подмножеств, и могут иметься два взаимно исключающих случая:*

a) *тело L имеет характеристику нуль, и тогда в нем содержится поле $K_0^p = K$ p-адических чисел;*

b) *тело L имеет характеристику p, и тогда в нем содержится поле $K_t^p = K$ рядов относительно некоторого t.*

В обоих случаях элементы поля K перестановочны по умножению с элементами тела L и имеется конечный линейный базис тела L над полем K. Именно, такая система элементов

$$l_0 = e,\ l_1, \ldots,\ l_\nu,$$

что каждый элемент $x \in L$ записывается в виде

$$x = x_0 l_0 + x_1 l_1 + \ldots + x_\nu l_\nu,$$

где коэффициенты $x_i \in K$.

* * *

В этой книге мы рассмотрели системы величин с алгебраическими операциями и предельным переходом, которые являются логически возможными обобщениями чисел. В частности, налагая на эту систему весьма общие ограничения, мы пришли к результату, что никаких других логических возможностей для построения приемлемых в математике величин, аналогичных действительным и комплексным числам, кроме

действительных и комплексных чисел, не существует. Это показывает, что действительные и комплексные числа сложились в математике не в результате случайного процесса исторического развития, а как единственные логически возможные величины, удовлетворяющие тем требованиям, которые естественно предъявить к числам.

Об авторе

Лев Семенович Понтрягин
(1908–1988)

Выдающийся российский математик, академик АН СССР, Герой Социалистического Труда (1969). Родился 3 сентября 1908 г. в Москве. В 14 лет потерял зрение от несчастного случая. Окончил Московский государственный университет им. М. В. Ломоносова (1929). С 1930 г. работал в Московском университете, где в 1935 г. получил ученое звание профессора, и одновременно с 1939 г. занимал должность заведующего отделом Математического института им. В. А. Стеклова АН СССР.

Основные работы Л. С. Понтрягина относятся к теории дифференциальных уравнений, топологии, теории колебаний, теории управления, вариационному исчислению, алгебре. В топологии он открыл общий закон двойственности и в связи с этим построил теорию характеров непрерывных групп; получил ряд результатов в теории гомотопий (классы Понтрягина). В теории колебаний главные результаты работ Л. С. Понтрягина относятся к асимптотике релаксационных колебаний. В теории управления он выступил как создатель математической теории оптимальных процессов, в основе которой лежит так называемый принцип максимума Понтрягина. Ему принадлежат также существенные результаты в области вариационного исчисления, дифференциальных игр, теории размерности, теории регулирования. Работы школы Л. С. Понтрягина оказали большое влияние на развитие теории управления и вариационного исчисления во всем мире.

В книге представлен популярный рассказ о возможных обобщениях понятия числа. Сначала подробно рассмотрены обобщения действительных чисел, именно комплексные числа и кватернионы. Доказано, что других логически возможных величин, аналогичных действительным и комплексным числам и пригодных к употреблению в математике в роли чисел, кроме действительных и комплексных чисел, не существует. Затем рассматриваются другие обобщения понятия числа, уже не содержащие действительных чисел.

1795 ID 11629
9 785354 002597

ИЗДАТЕЛЬСТВО УРСС
НАУЧНОЙ И УЧЕБНОЙ ЛИТЕРАТУРЫ
E-mail: URSS@URSS.ru
Каталог изданий
в *Internet:* http://URSS.ru
Тел./факс: 7 (095) 135–44–23
Тел./факс: 7 (095) 135–42–46