является подполем поля действительных чисел; все числовые поля будут подполями поля комплексных чисел.

Пусть в поле P даны подполе P' и элемент c, лежащий вне P', и пусть мы нашли минимальное подполе P'' поля P, содержащее и P', и c. Такое минимальное подполе может быть только одно, так как если бы P''' было еще одно подполе с этими свойствами, то пересечение подполей P'' и P''' (т. е. совокупность элементов, общих обоим подполям) содержало бы P' и элемент c и вместе с любыми двумя своими элементами содержало бы их сумму (эта сумма должна содержаться и в P'', и в P''', а потому и в их пересечении), а также их произведение, разность и частное; иными словами, это пересечение само было бы подполем, в противоречие с минимальностью подполя P''. Мы будем говорить, что поле P'' *получено присоединением к полю* P' *элемента* c, и употреблять запись $P''=P'(c)$.

Понятно, что поле $P'(c)$ содержит, помимо элемента c и всех элементов поля P', также все элементы, которые получаются из них при помощи сложения, умножения, вычитания и деления. В качестве примера укажем на рассматривавшееся в § 43 расширение поля рациональных чисел, состоящее из чисел вида $a+b\sqrt{2}$ с рациональными a, b: это расширение получается присоединением к полю рациональных чисел числа $\sqrt{2}$.

§ 46*. Изоморфизм колец (полей). Единственность поля комплексных чисел

В теории колец большую роль играет понятие изоморфизма. Именно, кольца L и L' называются *изоморфными*, если между ними можно установить такое взаимно однозначное соответствие, при котором для любых элементов a, b из L и соответствующих им элементов a', b' из L' сумме $a+b$ соответствует сумма $a'+b'$, а произведению ab соответствует произведение $a'b'$.

Пусть между кольцами L и L' установлено изоморфное соответствие. *При этом соответствии нулю* 0 *кольца* L *соответствует нуль* $0'$ *кольца* L'. Действительно, пусть элементу 0 соответствует элемент c' из L'. Берем произвольный элемент a из L и соответствующий ему элемент a' из L'. Тогда элементу $a+0$ должен соответствовать элемент $a'+c'$; но $a+0=a$, поэтому $a'+c'=a'$, откуда $c'=0'$. Далее, *элементу* $-a$ *соответствует элемент* $-a'$. Действительно, пусть элементу $-a$ соответствует элемент d'. Тогда элементу $a+(-a)=0$ должен соответствовать элемент $a'+d'$, т. е. $a'+d'=0'$, откуда $d'=-a'$. Отсюда следует, что *разности элементов из* L *соответствует разность соответствующих элементов в* L'. Аналогичными рассуждениями можно показать, что если кольцо L обладает единицей, то образ этого элемента (т. е. элемент, соответствующий ему в L' при рассматриваемом изоморфизме) будет единицей кольца L', и если элемент a из L

обладает обратным элементом a^{-1}, то образом элемента a^{-1} в L' будет элемент, обратный к a'.

Отсюда следует, что *кольцо, изоморфное полю, само будет полем.* Легко видеть также, что свойство кольца не иметь делителей нуля также сохраняется при изоморфном соответствии. Вообще, изоморфные кольца могут отличаться друг от друга природой своих элементов, но они тождественны по своим алгебраическим свойствам; всякая теорема, доказанная относительно некоторого кольца, будет справедливой для всех колец, с ним изоморфных, если только в доказательстве теоремы использовались лишь свойства операций, а не индивидуальные свойства элементов этого кольца. По этой причине *мы не будем считать изоморфные кольца или поля различными*; они будут для нас лишь разными экземплярами одного и того же кольца или поля.

Применим это понятие к вопросу о построении поля комплексных чисел. Изложенная в § 17 конструкция поля комплексных чисел, основанная на использовании точек плоскости, не является единственно возможной. Вместо точек можно было бы взять отрезки (векторы) на плоскости, выходящие из начала координат, и, задавая эти векторы их компонентами a, b на осях координат, определить сложение и умножение векторов при помощи тех же самых формул (2) и (3) из § 17, как и в случае точек плоскости. Можно было бы, далее, вообще отказаться от привлечения геометрического материала; замечая, что и точки плоскости, и векторы на плоскости задаются упорядоченными парами действительных чисел (a, b), можно просто взять совокупность всех таких пар и в ней ввести сложение и умножение по формулам (2) и (3) из указанного параграфа.

На самом деле все эти поля оказались бы по своим алгебраическим свойствам неразличимыми, как показывает следующая теорема:

Все расширения поля действительных чисел D, полученные присоединением к полю D корня уравнения

$$x^2+1=0, \tag{1}$$

изоморфны между собой.

Пусть, в самом деле, дано какое-либо поле P, являющееся расширением поля D и содержащее элемент, удовлетворяющий уравнению (1). Выбор обозначения для этого элемента находится в нашем распоряжении, и мы употребим для этой цели букву i. Таким образом, имеет место равенство $i^2+1=0$ (откуда $i^2=-1$), где возведение в степень и сложение нужно понимать в смысле операций, определенных в поле P. Мы хотим найти сейчас поле $D(i)$, получающееся присоединением к полю D элемента i, т. е. найти минимальное подполе поля P, содержащее и поле D, и элемент i.

Рассмотрим для этой цели все те элементы α поля P, которые можно записать в виде

$$\alpha=a+bi, \tag{2}$$

где a и b — произвольные действительные числа, а произведение числа b на элемент i и сумму числа a с этим произведением следует понимать в смысле операций, определенных в поле P. Никакой элемент α поля P не может обладать двумя различными записями такого вида: из

$$\alpha = a + bi = \bar{a} + \bar{b}i$$

и $b \neq \bar{b}$ следовало бы

$$i = \frac{\bar{a} - a}{b - \bar{b}},$$

т. е. i оказалось бы действительным числом; если же $b = \bar{b}$, то и $a = \bar{a}$. К числу элементов поля P, записываемых в виде (2), принадлежат, в частности, все действительные числа (случай $b = 0$), а также сам элемент i (случай $a = 0$, $b = 1$).

Покажем, что ***совокупность всех элементов вида*** (2) ***составляет подполе поля*** P; это и будет тогда искомым полем $D(i)$. Пусть нам даны элементы $\alpha = a + bi$ и $\beta = c + di$. Тогда, используя коммутативность и ассоциативность сложения и закон дистрибутивности, имеющие место в поле P, получаем:

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (bi + di),$$

откуда

$$\alpha + \beta = (a + c) + (b + d)\, i, \tag{3}$$

т. е. эта сумма снова принадлежит к рассматриваемому множеству элементов. Далее,

$$-\beta = (-c) + (-d)\, i,$$

так как, ввиду (3), тогда будет справедливо равенство $\beta + (-\beta) = 0 + 0i = 0$; поэтому

$$\alpha - \beta = \alpha + (-\beta) = (a - c) + (b - d)\, i, \tag{3'}$$

т. е. и вычитание не выводит нас за пределы рассматриваемого множества. Снова используя свойства I—V, имеющие место для операций в поле P (см. § 44), и опираясь на равенство $i^2 = -1$, мы получаем:

$$\alpha\beta = (a + bi)(c + di) = ac + adi + bci + bdi^2,$$

т. е.

$$\alpha\beta = (ac - bd) + (ad + bc)\, i; \tag{4}$$

таким образом, произведение двух любых элементов вида (2) снова будет элементом этого же вида. Предположим, наконец, что $\beta \neq 0$, т. е. хотя бы одно из чисел c, d отлично от нуля. Тогда будет также $c - di \neq 0$ и

$$(c + di)(c - di) = c^2 - (di)^2 = c^2 - d^2 i^2 = c^2 + d^2,$$

причем $c^2+d^2 \neq 0$. Поэтому, используя отмечавшееся в предшествующем параграфе утверждение, что во всяком поле сохраняются все обычные правила обращения с дробями, а поэтому, в частности, дробь не меняется от умножения ее числителя и знаменателя на один и тот же отличный от нуля элемент, получаем:

$$\frac{\alpha}{\beta}=\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2},$$

т. е. элемент

$$\frac{\alpha}{\beta}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i \tag{4'}$$

снова имеет вид (2).

Покажем теперь, что *полученное нами подполе $D(i)$ поля P изоморфно тому полю из точек плоскости, которое было построено в* § 17. Сопоставляя элементу $a+bi$ поля $D(i)$ точку (a, b), мы получим ввиду доказанной единственности записи вида (2) для элементов поля $D(i)$ взаимно однозначное соответствие между элементами этого поля и всеми точками плоскости. При этом соответствии действительному числу a соответствует точка $(a, 0)$ ввиду равенства $a=a+0i$, а элементу $i=0+1\cdot i$ сопоставляется точка $(0, 1)$. С другой стороны, сравнивая формулы (3) и (4) настоящего параграфа с формулами (2) и (3) из § 17, мы получаем, что сумме и произведению элементов α и β поля $D(i)$ сопоставляются точки, являющиеся суммой и соответственно произведением точек, сопоставленных элементам α и β.

Этим, так как все поля, изоморфные некоторому данному полю, изоморфны между собой, заканчивается доказательство теоремы. Мы видим, в частности, что выбор в § 17 формул (2) и (3) для определения операций над точками не был случайным и не может быть изменен.

Помимо способов построения поля комплексных чисел, рассматривавшихся выше, существуют и многие другие. Укажем один из них, использующий сложение и умножение матриц.

Рассмотрим некоммутативное кольцо матриц второго порядка над полем действительных чисел. Очевидно, что скалярные матрицы

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

составляют в этом кольце подполе, изоморфное полю действительных чисел. Оказывается, однако, что *в кольце матриц второго порядка над полем действительных чисел можно найти также подполе, изоморфное полю комплексных чисел.* В самом деле, поставим в соответствие всякому комплексному числу $a+bi$ *матрицу*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Этим путем все поле комплексных чисел отображается, притом взаимно однозначно, на часть кольца матриц второго порядка, причем из равенств

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

вытекает, что это отображение изоморфное, так как матрицы, стоящие в правых частях равенств, соответствуют комплексным числам $(a+c)+(b+d)\,i=(a+bi)+(c+di)$ и $(ac-bd)+(ad+bc)\,i=(a+bi)\,(c+di)$. В частности, роль мнимой единицы i играет матрица

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Полученный нами результат указывает на еще один возможный способ построения поля комплексных чисел, столь же удовлетворительный, как и те, которые рассматривались выше.

§ 47. Линейная алгебра и алгебра многочленов над произвольным полем

В тех из предшествующих глав книги, которые посвящены линейной алгебре, роль основного поля играло обычно поле действительных чисел. Без труда проверяется, однако, что очень многое из этих глав дословно переносится на случай произвольного основного поля.

Так, *для произвольного основного поля P остаются справедливыми изложенные в гл. 1 метод Гаусса для решения систем линейных уравнений, теория определителей и правило Крамера.* Лишь замечание о кососимметрических определителях, приведенное в конце § 4, требует предположения, что характеристика поля P отлична от двух. Впрочем, доказательство свойства 4 из этого же параграфа также теряет силу, если характеристика поля P равна двум, хотя само это свойство остается справедливым.

Полезно отметить также, что неоднократно высказывавшееся в гл. 1 утверждение о существовании у неопределенной системы линейных уравнений бесконечного множества различных решений сохраняет силу в случае любого бесконечного основного поля P, но перестает быть справедливым, если поле P конечно.

Далее, *полностью переносятся на случай произвольного основного поля изложенные в гл. 2 теория линейной зависимости векторов, теория ранга матрицы и общая теория систем линейных уравнений, а также алгебра матриц из гл. 3.*

Общая теория квадратичных форм, построенная в § 26, *переносится на случай любого основного поля P, характеристика которого отлична от двух.* Без этого ограничения, как легко показать, основная теорема этого параграфа уже перестает быть справедливой.