С некоммутативными умножениями приходится встречаться так часто и в таких важных случаях, что в настоящее время под термином «кольцо» понимают обычно *некоммутативное кольцо* (точнее, не обязательно коммутативное кольцо, в смысле возможной некоммутативности умножения), называя тот частный тип колец, в которых требование III выполняется, *коммутативными кольцами*.

В последнее время повышается интерес и к кольцам с неассоциативным умножением и общая теория колец уже строится сейчас как теория неассоциативных (т. е. не обязательно ассоциативных) колец. Простейшим примером таких колец является множество векторов трехмерного евклидова пространства относительно операций сложения и (известного из курса аналитической геометрии) векторного умножения векторов.

§ 45. Поле

Подобно тому как среди числовых колец были выделены и названы числовыми полями те кольца, в которых можно выполнять деление (кроме деления на нуль), естественно сделать это и в общем случае. Заметим сначала, что *ни в каком кольце невозможно деление на нуль* ввиду доказанного выше свойства нуля по отношению к умножению: разделить элемент a на нуль означает найти в кольце такой элемент x, что $0 \cdot x = a$, что при $a \neq 0$ невозможно, так как левая часть равна нулю.

Введем следующее определение:

Кольцо P называется *полем*, если оно состоит не только из одного нуля и если в нем деление выполнимо, притом однозначным образом, во всех случаях, кроме случая деления на нуль, т. е. если для любых элементов a и b из P, из которых b отлично от нуля, существует в P такой элемент q, притом лишь единственный, который удовлетворяет равенству $bq = a$. Элемент q называется *частным* элементов a и b и обозначается символом $q = \frac{a}{b}$ [1]).

Примерами полей служат, понятно, все числовые поля. Кольцо многочленов от неизвестного x с действительными коэффициентами или вообще с коэффициентами из некоторого числового поля не является полем — существующее для многочленов деление с остатком отличается, конечно, от деления «нацело», предполагающегося в определении поля. С другой стороны, легко видеть, что *совокупность всех дробно-рациональных функций с действительными коэффициентами* (см. § 25) *будет полем*, содержащим кольцо многочленов, подобно тому как поле рациональных чисел содержит кольцо целых чисел.

Среди колец функций можно указать некоторые другие примеры полей; мы не будем, однако, на них останавливаться и перейдем к примерам совсем иного рода.

---

[1]) Единственность деления в поле, как и предполагавшаяся в определении кольца единственность вычитания, в действительности без труда могут быть доказаны при помощи других требований, входящих в определение поля или, соответственно, кольца.

Все числовые кольца и вообще кольца, которые мы до сих пор рассматривали, содержат бесконечно много элементов. Существуют, однако, кольца и даже поля, состоящие лишь из конечного числа элементов. Простейшие примеры *конечных колец* и *конечных полей*, существенно используемые в особой ветви математики — теории чисел, строятся следующим образом.

Берем любое натуральное число n, отличное от 1. Целые числа a и b называются *сравнимыми по модулю* n,

$$a \equiv b \pmod{n},$$

если эти числа дают при делении на n один и тот же остаток, т. е. если их разность нацело делится на n. Все кольцо целых чисел распадается на n непересекающихся классов,

$$C_0,\ C_1,\ \ldots,\ C_{n-1}, \tag{1}$$

сравнимых между собой по модулю n чисел, причем класс C_k, $k=0,\ 1,\ \ldots,\ n-1$, состоит из чисел, дающих при делении на n в остатке k. Оказывается, что можно вполне естественным способом определить сложение и умножение этих классов.

Возьмем с этой целью любые (притом не обязательно различные) классы C_k и C_l из системы (1). Складывая любое число из класса C_k с любым числом из класса C_l, мы будем получать числа, лежащие в одном вполне определенном классе, а именно в классе C_{k+l}, если $k+l<n$, или в классе C_{k+l-n}, если $k+l \geqslant n$. Это приводит к такому определению *сложения классов*:

$$\begin{aligned} C_k + C_l &= C_{k+l} \quad \text{при} \quad k+l<n, \\ C_k + C_l &= C_{k+l-n} \quad \text{при} \quad k+l \geqslant n. \end{aligned} \tag{2}$$

С другой стороны, умножая любое число класса C_k на любое число класса C_l, мы будем получать числа, снова лежащие во вполне определенном классе, а именно в классе C_r, где r — остаток при делении произведения kl на n. Мы принимаем поэтому такое определение *умножения классов*:

$$C_k \cdot C_l = C_r, \text{ где } kl = nq + r,\ 0 \leqslant r < n. \tag{3}$$

Система (1) *классов целых чисел, сравнимых между собой по модулю* n, *будет кольцом по отношению к операциям, определенным условиями* (2) *и* (3). В самом деле, справедливость требований I—V из определения кольца без труда устанавливается непосредственной проверкой, но вытекает также из справедливости этих требований в кольце целых чисел и той связи между операциями над целыми числами и операциями над классами, которая указана выше. Роль нуля играет, очевидно, класс C_0, состоящий из чисел, нацело делящихся на n. Противоположным для класса C_k, $k=1,\ 2,\ \ldots,\ n-1$, будет класс C_{n-k}. В системе классов (1) можно

определить, следовательно, вычитание, т. е. эта система удовлетворяет всем требованиям, входящим в определение кольца. Условимся обозначать полученное кольцо через Z_n.

Если число n составное, то кольцо Z_n обладает делителями нуля и поэтому, как будет показано ниже, не может быть полем. В самом деле, если $n=kl$, где $1<k<n$, $1<l<n$, то классы C_k и C_l отличны от нулевого класса C_0, но на основании определения умножения классов (см. (3)) $C_k \cdot C_l = C_0$.

Если же число n простое, то кольцо Z_n будет полем.

В самом деле, пусть даны классы C_k и C_m, причем $C_k \neq C_0$, т. е. $1 \leqslant k \leqslant n-1$. Нужно показать, что можно разделить C_m на C_k, т. е. найти такой класс C_l, что $C_k \cdot C_l = C_m$. Если $C_m = C_0$, то и $C_l = C_0$. Если же $C_m \neq C_0$, то рассмотрим систему чисел

$$k,\ 2k,\ 3k,\ \ldots,\ (n-1)\,k. \tag{4}$$

Все эти числа лежат вне нулевого класса C_0, так как произведение двух натуральных чисел, меньших простого числа n, не может на n делиться. Далее, никакие два числа sk и tk из системы (4), $s<t$, не могут лежать в одном классе, так как тогда их разность

$$tk - sk = (t-s)\,k$$

делилась бы на n, что снова противоречит простоте числа n. Таким образом, в каждом ненулевом классе лежит ровно одно число из системы (4). В частности, в классе C_m лежит число lk, где $1 \leqslant l \leqslant n-1$, т. е. $C_l \cdot C_k = C_m$, а тогда класс C_l и будет искомым частным от деления C_m на C_k.

Мы получили, таким образом, бесконечно много различных конечных полей: поле Z_2, состоящее всего из двух элементов, а также поля Z_3, Z_5, Z_7, Z_{11} и т. д.

Переходим к рассмотрению некоторых свойств полей, вытекающих из существования деления. Эти свойства аналогичны свойствам колец, основанным на существовании вычитания, и доказываются такими же рассуждениями, поэтому проведение доказательств предоставляется читателю.

Всякое поле P обладает однозначно определенным элементом, произведение которого на любой элемент a этого поля равно a. Этот элемент, совпадающий с равными между собою частными $\frac{a}{a}$ для всех a, отличных от нуля, называется *единицей* поля P и обозначается символом 1. Таким образом,

$$a \cdot 1 = a \quad \text{для всех } a \text{ из } P.$$

Во всяком поле для любого элемента a, отличного от нуля, существует однозначно определенный обратный элемент a^{-1}, удовлетворяющий равенству

$$a \cdot a^{-1} = 1,$$

а именно, $a^{-1}=\frac{1}{a}$. Очевидно, что $(a^{-1})^{-1}=a$. Частное $\frac{b}{a}$ можно записать теперь в виде

$$\frac{b}{a}=b\cdot a^{-1}.$$

Для любого элемента a, отличного от нуля, и любого целого положительного числа n имеет место равенство

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

Обозначая эти равные между собою элементы через a^{-n}, мы приходим к *отрицательным степеням* элемента поля, для которых сохраняются обычные правила оперирования. Положим, наконец, $a^0=1$ для всех a.

Существование единицы не является характерным свойством полей: единицей обладает, например, кольцо целых чисел. Вместе с тем, пример кольца четных чисел показывает, что не все кольца обладают единицей. С другой стороны, *всякое кольцо, обладающее единицей и содержащее обратный элемент для любого элемента, отличного от нуля, будет полем.* Действительно, в этом случае частным $\frac{b}{a}$, $a\neq 0$, будет служить произведение ba^{-1}. Единственность этого частного доказывается без затруднений.

Заметим, что *никакое поле не содержит делителей нуля.* Действительно, пусть $ab=0$, но $a\neq 0$. Умножая обе части равенства на элемент a^{-1}, мы получим слева $(a^{-1}a)b=1\cdot b=b$, а справа $a^{-1}\cdot 0=0$, т. е. $b=0$. Отсюда следует, что *во всяком поле любое равенство можно сократить на общий множитель, отличный от нуля.* В самом деле, если $ac=bc$ и $c\neq 0$, то $(a-b)c=0$, откуда $a-b=0$, т. е. $a=b$.

Из определения частного $\frac{a}{b}$ (где $b\neq 0$) и доказанной выше возможности записывать его в виде произведения ab^{-1} без труда может быть выведено, что *во всяком поле сохраняются все обычные правила обращения с дробями,* а именно:

$$\frac{a}{b}=\frac{c}{d} \text{ тогда и только тогда, если } ad=bc;$$

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

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd};$$

$$\frac{-a}{b}=-\frac{a}{b}.$$

Характеристика поля. Не все свойства числовых полей сохраняются в случае произвольного поля. Так, складывая число 1 само с собою несколько раз, т. е. беря любое целое положительное

кратное единицы, мы никогда не получим нуля, и вообще все эти кратные, т. е. все натуральные числа, отличны друг от друга. Если же мы будем брать целые кратные единицы в каком-либо конечном поле, то среди них непременно будут равные, так как это поле обладает лишь конечным числом различных элементов. Если все целые кратные единицы поля P являются различными элементами поля P, т. е. $k\cdot 1 \neq l\cdot 1$ при $k \neq l$, то говорят, что поле P имеет *характеристику нуль*; таковы, например, все числовые поля. Если же существуют такие целые числа k и l, что $k > l$, но в P имеет место равенство $k\cdot 1 = l\cdot 1$, то $(k-l)\cdot 1 = 0$, т. е. в P существует такое положительное кратное единицы, которое оказывается равным нулю. В этом случае P называется полем *конечной характеристики*, а именно *характеристики* p, если p есть тот первый положительный коэффициент, с которым единица поля P обращается в нуль. Примерами полей конечной характеристики служат все конечные поля; существуют, впрочем, и бесконечные поля, имеющие конечную характеристику.

Если поле P имеет характеристику p, то число p будет простым.

Действительно, из равенства $p = st$, где $s < p$, $t < p$, вытекало бы равенство $(s\cdot 1)(t\cdot 1) = p\cdot 1 = 0$, т. е., так как в поле не может быть делителей нуля, или $s\cdot 1 = 0$, или $t\cdot 1 = 0$, что, однако, противоречит определению характеристики как наименьшего положительного коэффициента, обращающего единицу поля в нуль.

Если характеристика поля P равна p, то для любого элемента a из этого поля имеет место равенство $pa = 0$. Если же характеристика поля P равна 0 и a — элемент этого поля, n — целое число, то из $a \neq 0$ и $n \neq 0$ следует $na \neq 0$.

Действительно, в первом случае элемент pa, т. е. сумму p слагаемых, равных a, можно, вынося a за скобки, представить в виде

$$pa = a(p\cdot 1) = a\cdot 0 = 0.$$

Во втором случае из равенства $na = 0$, т. е. $a(n\cdot 1) = 0$, следовало бы при $a \neq 0$ равенство $n\cdot 1 = 0$, т. е., так как характеристика поля равна нулю, $n = 0$.

Подполя, расширения. Пусть в поле P некоторая часть его элементов, составляющая множество P', сама оказывается полем по отношению к тем операциям, которые определены в поле P, т. е. для любых двух элементов a, b из P' содержащиеся в поле P элементы $a+b$, ab, $a-b$ и, при $b \neq 0$, $\frac{a}{b}$ принадлежат к P' (законы I—V, выполняясь в P, будут, конечно, выполняться и в P'). Тогда P' называется *подполем* поля P, а P — *расширением* поля P'. Понятно, что нуль и единица поля P будут содержаться также в P' и служить для P' нулем и единицей. Так, поле рациональных чисел

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