§1. Поля, коммутативные кольца и абелевы группы

1.1. Определения и примеры. Говоря вольно, поле представляет собою числовую область, где определены четыре стандартные арифметические операции: сложение, вычитание, умножение и деление, которые обладают теми же свойствами, что и соответствующие действия над рациональными числами. Точный перечень этих свойств идёт ниже.

Определение 1.1
Множество $\mathbb{F}$ с двумя операциями $\mathbb{F}\times\mathbb{F}\to\mathbb{F}$: *сложением* $(a,b)\mapsto a+b$ и *умножением* $(a,b)\mapsto ab$ называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

коммутативность: $a+b=b+a \quad \forall\, a,b\in\mathbb{F}$ (1-1)

ассоциативность: $a+(b+c)=(a+b)+c \quad \forall\, a,b,c\in\mathbb{F}$ (1-2)

наличие нуля: $\exists\, 0\in\mathbb{F}:\quad a+0=a \quad \forall\, a\in\mathbb{F}$ (1-3)

наличие противоположных: $\forall\, a\in\mathbb{F} \quad \exists\,(-a)\in\mathbb{F}:\quad a+(-a)=0$ (1-4)

свойства умножения

коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$ (1-5)

ассоциативность: $a\,(bc)=(ab)\,c \quad \forall\, a,b,c\in\mathbb{F}$ (1-6)

наличие единицы: $\exists\, 1\in\mathbb{F}:\quad 1\,a=a \quad \forall\, a\in\mathbb{F}$ (1-7)

наличие обратных: $\forall\, a\in\mathbb{F}\smallsetminus 0 \quad \exists\, a^{-1}\in\mathbb{F}:\quad aa^{-1}=1$ (1-8)

свойства, связывающие сложение с умножением

дистрибутивность: $a(b+c)=ab+ac \quad \forall\, a,b,c\in\mathbb{F}$ (1-9)

нетривиальность: $0\neq 1$ (1-10)

Пример 1.1 (поле из двух элементов)
Простейший объект, удовлетворяющий всем аксиомам из опр. 1.1 — это поле $\mathbb{F}_2$, состоящее только из двух таких элементов 0 и 1, что $0+1=1\cdot 1=1$, а все остальные суммы и произведения равны нулю.

Упражнение 1.1. Проверьте, что $\mathbb{F}_2$ действительно является полем.

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, т. е. «чётное» $=0$ и «нечётное» $=1$, со сложением и умножением, заданными формулами (0-19) – (0-20) на стр. 11. С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как «ложь» $=0$ и «истина» $=1$, сложение — как логическое «исключающее или»[1], а умножение — как логическое «и»[2]. При такой интерпретации алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

Упражнение 1.2. Напишите многочлен от x с коэффициентами из поля $\mathbb{F}_2$, равный «не x», а

[1] Т. е. высказывание $A+B$ истинно тогда и только тогда, когда истинно *ровно одно* из высказываний A, B. На языке формул: $0+1=1+0=1$, а $0+0=1+1=0$.

[2] Т. е. высказывание $A\cdot B$ истинно если и только если истинны *оба* высказывания A и B : $1\cdot 1=1$, но $0\cdot 1=1\cdot 0=0\cdot 0=0$.

также многочлен от x и y, равный «x или[1] y».

Пример 1.2 (рациональные числа)
Напомню[2], что поле рациональных чисел $\mathbb{Q}$ можно определить как множество дробей a/b, где под «дробью» понимается класс эквивалентности упорядоченной пары (a,b) с $a, b \in \mathbb{Z}$ и $b \neq 0$ по отношению $(a_1, b_1) \sim (a_2, b_2)$ при $a_1 b_2 = a_2 b_1$, которое является минимальным отношением эквивалентности[3], содержащим все отождествления

$$\frac{a}{b} = \frac{ac}{bc} \quad \forall\, c \neq 0\,.$$

Сложение и умножение дробей определяется формулами

$$\frac{a}{b} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{ad+bc}{bd}\,, \quad \frac{a}{b} \cdot \frac{c}{d} \stackrel{\text{def}}{=} \frac{ac}{bd}\,. \tag{1-11}$$

Упражнение 1.3. Проверьте, что эти операции определены корректно (результат не зависит от выбора представителей в классах) и удовлетворяют аксиомам поля.

Пример 1.3 (вещественные числа)
Множество вещественных чисел $\mathbb{R}$ определяется в курсе анализа несколькими различными способами: как множество классов эквивалентности десятичных[4] дробей, как множество дедекиндовых сечений упорядоченного множества $\mathbb{Q}$, или как множество классов эквивалентности рациональных последовательностей Коши. Мы полагаем, что читатель знаком с этими определениями и понимает, как они связаны друг с другом, либо скоро узнает об этом из курса анализа. Какое бы описание множества $\mathbb{R}$ не использовалось, задание на нём сложения и умножения, равно как и проверка аксиом из опр. 1.1, требуют определённой умственной работы, также традиционно проделываемой в курсе анализа.

1.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти операции обладают всеми свойствами из опр. 1.1 на стр. 21 за исключением свойства (1-8) существования мультипликативно обратных элементов и условия $0 \neq 1$. Если, кроме этих двух аксиом из списка аксиом поля исключается требование наличия единицы (1-7), то множество K с двумя операциями, удовлетворяющими оставшимся аксиомам, называется просто *коммутативным кольцом*. Примерами отличных от полей колец с единицами являются кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные целые числа, многочлены с чётными целыми коэффициентами, многочлены без свободного члена с коэффициентами в любом коммутативном кольце и т. п.

1.1.2. Абелевы группы. Множество A *с одной* операцией $A \times A \to A$, удовлетворяющей первым четырём аксиомам сложения из опр. 1.1, называется *абелевой группой*. Таким образом, всякое коммутативное кольцо K является абелевой группой относительно операции сложения. Эта группа называется *аддитивной группой кольца*. Пример абелевой группы, не являющейся кольцом, доставляют *векторы*.

[1] Здесь имеется в виду обычное, не исключающее «или»: многочлен должен принимать значение 1 тогда и только тогда, когда *хотя бы одна* из переменных равна 1.

[2] См. прим. 0.5 на стр. 12.

[3] См. n° 0.4.1 на стр. 12.

[4] Или привязанных к какой-либо другой позиционной системе счисления, например, двоичных.

Пример 1.4 (геометрические векторы)
Будем называть *геометрическим вектором* класс направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему между собой все отрезки, которые получающиеся друг из друга параллельным переносом. Нулевым вектором назовём класс эквивалентности точки — это единственный вектор, имеющий нулевую длину и не имеющий направления. Сложение векторов определяется стандартным образом: надо выбрать представителей векторов a и b так, чтобы конец a совпал с началом b, и объявить $a + b$ равным вектору с началом в начале a и концом в конце b. Коммутативность и ассоциативность этой операции видны из рис. 1⋄1 и рис. 1⋄2.

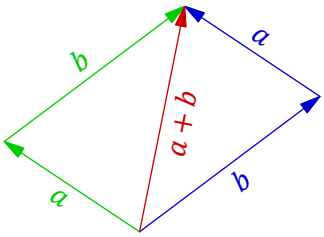

Рис. 1⋄1. Правило параллелограмма.

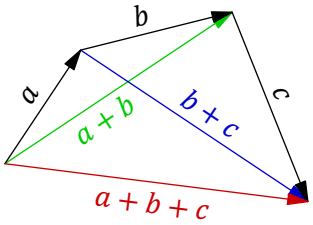

Рис. 1⋄2. Правило четырёхугольника.

Нулевым элементом является нулевой вектор. Вектор $-a$, противоположный вектору a, получается из вектора a изменением его направления на противоположное.

Пример 1.5 (мультипликативная группа поля)
Четыре аксиомы умножения из опр. 1.1 на стр. 21 утверждают, то множество $\mathbb{F}^\times \stackrel{\text{def}}{=} \mathbb{F} \setminus 0$ всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно операции умножения. Эту группу называют *мультипликативной группой поля*. Роль нуля из аддитивной группы $\mathbb{F}$ в мультипликативной группе $\mathbb{F}^\times$ исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Лемма 1.1
В любой абелевой группе A нейтральный элемент единствен, и для каждого $a \in A$ противоположный к a элемент $-a$ определяется по a однозначно. В частности, $-(-a) = a$.

Доказательство. Будем записывать операцию в A аддитивно. Если есть два нулевых элемента 0_1 и 0_2, то $0_1 = 0_1 + 0_2 = 0_2$ (первое равенство выплнено, так как 0_2 является нулевым элементом, второе — поскольку нулевым элементом является 0_1). Если есть два элемента $-a$ и $-a'$, противоположных к a, то $-a = (-a) + 0 = (-a) + \big(a + (-a')\big) = \big((-a) + a\big) + (-a') = 0 + (-a') = -a'$. □

Лемма 1.2
В любом коммутативном кольце для любого элемента a выполняется равенство $0 \cdot a = 0$, а в любом коммутативном кольце с единицей — равенство $(-1) \cdot a = -a$.

Доказательство. Так как $a \cdot 0 = a\,(0 + 0) = a \cdot 0 + a \cdot 0$, прибавляя к обеим частям элемент, противоположный к $a \cdot 0$, получаем $0 = a \cdot 0$. Второе утверждение проверяется выкладкой $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$. □

Замечание 1.1. Если в коммутативном кольце K с единицей выполняется равенство $0 = 1$, то K состоит из одного нуля, так как для каждого $a \in K$ имеем $a = a \cdot 1 = a \cdot 0 = 0$. Образование, состоящее из одного нуля, согласно предыдущим определениям, является коммутативным кольцом с единицей, но не полем.

1.1.3. Вычитание и деление. Из лем. 1.1 вытекает, что в любой абелевой группе корректно определена *разность* любых двух элементов

$$a - b \stackrel{\text{def}}{=} a + (-b)\,. \tag{1-12}$$

В частности, операция вычитания имеется в аддитивной группе любого коммутативного кольца. В поле ненулевые элементы образуют абелеву группу по умножению. Поэтому в любом поле имеется ровно один единичный элемент, и для любого ненулевого элемента a обратный к нему элемент a^{-1} однозначно определяется по a. Тем самым, в любом поле помимо сложения, умножения и вычитания (1-12) имеется операция *деления* на любые ненулевые элементы

$$a/b \stackrel{\text{def}}{=} ab^{-1}\,, \quad b \neq 0\,. \tag{1-13}$$

1.2. Делимость в кольце целых чисел. Основным отличием коммутативных колец с единицей от полей является отсутствие обратных элементов к некоторым ненулевым элементам кольца. Элемент a коммутативного кольца K с единицей называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*. Например, в кольце $\mathbb{Z}$ обратимыми элементами являются только 1 и -1. В кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами обратимыми элементами являются ненулевые константы (многочлены степени нуль) и только они.

Говорят, что элемент a *делится* на элемент b, если в кольце существует такой элемент q, что $a = bq$. Это записывается как $b|a$ (читается «b делит a») или как $a \vdots b$ (читается «a делится на b»). Отношение делимости тесно связано с решением линейных уравнений.

1.2.1. Уравнение $ax + by = k$, НОД и НОК. Зафиксируем какие-нибудь целые числа a и b и обозначим через

$$(a, b) \stackrel{\text{def}}{=} \{ax + by \mid x, y \in \mathbb{Z}\} \tag{1-14}$$

множество всех целых чисел, представимых в виде $ax + by$ с целыми x, y. Это множество замкнуто относительно сложения и вместе с каждым своим элементом содержит все его целые кратные. Кроме того, все числа из (a, b) нацело делятся на каждый общий делитель чисел a и b, а сами a и b тоже входят в (a, b). Обозначим через d наименьшее положительное число в (a, b). Остаток от деления любого числа $z \in (a, b)$ на d лежит в (a, b), поскольку представляется в виде $z - kd$, где и z и $-kd$ лежат в (a, b). Так как этот остаток строго меньше d, он равен нулю. Следовательно, (a, b) совпадает с множеством всех чисел, кратных d.

Таким образом, число d является общим делителем чисел $a, b \in (a, b)$, представляется в виде $d = ax + by$ и делится на любой общий делитель чисел a и b. При этом произвольное число $k \in \mathbb{Z}$ представляется в виде $k = ax + by$ если и только если оно делится на d. Число d называется *наибольшим общим делителем* чисел $a, b \in \mathbb{Z}$ и обозначается нод(a, b).

Упражнение 1.4. Обобщите проделанные только что рассуждения: для любого конечного набора чисел $a_1, \ldots, a_m \in \mathbb{Z}$ укажите число $d \in \mathbb{Z}$, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + \cdots + a_mx_m$ с целыми x_i. Покажите также, что уравнение $n = a_1x_1 + \cdots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ если и только если $n \vdots d$.

Записывая числа a и b как $a = \alpha d$, $b = \beta d$, где $d = \text{нод}(a, b)$, мы заключаем, что число

$$c = \alpha\beta d = \beta a = \alpha b \tag{1-15}$$

делится на a и на b. Покажем, что c делит все общие кратные чисел a и b. Пусть $m = ka = \ell b$. Так как $\text{нод}(\alpha, \beta) = 1$, существуют такие $x, y \in \mathbb{Z}$, что $\alpha x + \beta y = 1$. Умножая обе части этого равенства на m, мы заключаем, что $m = m\alpha x + m\beta y = \ell b\alpha x + ka\beta y = c(\ell x + ky)$, как и утверждалось. Число c называется *наименьшим общим кратным* чисел a и b и обозначается $\text{нок}(a, b)$.

Упражнение 1.5. Убедитесь, что все целые решения (x, y) уравнения $ax + by = k$ имеют вид $x = x_0 + n\beta$, $y = y_0 - n\alpha$, где α и β те же, что и выше, (x_0, y_0) — какое-то одно решение, а $n \in \mathbb{Z}$ — любое.

1.2.2. Алгоритм Евклида – Гаусса. Найти $\text{нод}(a, b)$ для данных $a, b \in \mathbb{Z}$ и представить его в виде $\text{нод}(a, b) = ax + by$ с целыми x, y можно следующим образом. Составим таблицу

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \tag{1-16}$$

и будем преобразовывать её строки, поэлементно прибавляя к одной строке другую, умноженную на подходящее целое число так, чтобы один из элементов первого столбца каждый раз строго уменьшался по абсолютной величине. Это возможно до тех пор, пока один из элементов в первом столбце не обнулится. После этого, меняя при необходимости строки местами и/или меняя знак у всех элементов одной из строк, можем переписать полученную таблицу в виде

$$\begin{pmatrix} d & x & y \\ 0 & k & \ell \end{pmatrix}, \tag{1-17}$$

где $x, y, k, \ell \in \mathbb{Z}$ и $d \in \mathbb{N}$. Это означает, что $\text{нод}(a, b) = d = ax + by$, а $\text{нок}(a, b) = |ka| = |\ell b|$, причём $\text{нод}(k, \ell) = 1$. Например, для чисел $a = 5\,073$ и $b = 1\,064$ получаем[1]:

$$\begin{pmatrix} 5\,073 & 1 & 0 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (1) \mapsto (1) - 5 \cdot (2)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 76 & 4 & -19 \end{pmatrix} \qquad (1) \mapsto (1) + 3 \cdot (2)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 76 & 4 & -19 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 0 & 56 & -267 \end{pmatrix} \qquad (1) \mapsto -(1)$$

$$\begin{pmatrix} 19 & -13 & 62 \\ 0 & 56 & -267 \end{pmatrix}.$$

Тем самым, $\text{нод}(5\,073,\ 1\,064) = 19 = -13 \cdot 5\,073 + 62 \cdot 1\,064$, $\text{нок}(5\,073,\ 1\,064) = 5\,073 \cdot 56 = 1\,064 \cdot 267$.

[1] Запись вроде $(1) \mapsto (1) - 5 \cdot (2)$ означает, что к 1-й строке прибавляется 2-я, умноженная на -5.

Упражнение 1.6. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$$

кроме, может быть, итоговой (полученной перестановкой строк и/или сменой знака в одной из строк) выполняются равенства $m = ax + by$, $n = as + bt$ и $xt - ys = 1$.

Из упражнения вытекает, что элементы возникающей в конце вычисления таблицы вида

$$\begin{pmatrix} d' & x & y \\ 0 & s & t \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & s & t \\ d' & x & y \end{pmatrix}$$

(где $d' \in \mathbb{Z}$ может отличаться от итогового $d \in \mathbb{N}$ лишь знаком) удовлетворяют равенствам

$$d' = ax + by\,, \quad sa = -tb\,, \quad tx - sy = 1\,. \tag{1-18}$$

Из первого следует, что d' делится на все общие делители чисел a и b. Умножая последнее равенство на a и на b и пользуясь первыми двумя равенствами, заключаем, что

$$a = atx - asy = atx + bty = td' \quad \text{и} \quad b = btx - bsy = -asx - bsy = -sd'$$

оба делятся на d', откуда $d = |d'| = \text{нод}(a, b)$. Второе равенство (1-18) показывает, что число $c' = sa = -tb$ является общим кратным a и b. Умножая третье равенство (1-18) на любое общее кратное $m = ka = \ell b$ чисел a и b, убеждаемся, что $m = mtx - msy = \ell btx - kasy = -c'(\ell x + ky)$ делится на c', откуда $c = |c'| = \text{нок}(a, b)$.

Замечание 1.2. С вычислительной точки зрения отыскание $\text{нод}(a, b)$ и $\text{нок}(a, b)$ по алгоритму Евклида – Гаусса *несопоставимо* быстрее разложения чисел a и b на простые множители. Читателю предлагается убедиться в этом, попробовав вручную разложить на простые множители числа 10 203 и 4 687. Вычисление по алгоритму Евклида – Гаусса занимает 6 строк:

$$\begin{aligned}
&\begin{pmatrix} 10\,203 & 1 & 0 \\ 4\,687 & 0 & 1 \end{pmatrix} && (1) \mapsto (1) - 2 \cdot (2) \\
&\begin{pmatrix} 829 & 1 & -2 \\ 4\,687 & 0 & 1 \end{pmatrix} && (2) \mapsto (2) - 6 \cdot (1) \\
&\begin{pmatrix} 829 & 1 & -2 \\ -287 & -6 & 13 \end{pmatrix} && (1) \mapsto (1) + 3 \cdot (2) \\
&\begin{pmatrix} -32 & -17 & 37 \\ -287 & -6 & 13 \end{pmatrix} && (2) \mapsto (2) - 9 \cdot (1) \\
&\begin{pmatrix} -32 & -17 & 37 \\ 1 & 147 & -320 \end{pmatrix} && (1) \mapsto (1) + 32 \cdot (2) \\
&\begin{pmatrix} 0 & 4\,687 & 10\,203 \\ 1 & 147 & -320 \end{pmatrix}, &&
\end{aligned} \tag{1-19}$$

откуда $\text{нод}(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687$, $\text{нок}(10\,203, 4\,687) = 10\,203 \cdot 4\,687$. Если известно произведение двух *очень* больших простых чисел, то извлечь из него сами эти числа за разумное время не под силу даже мощным компьютерам. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

1.3. Взаимная простота. Выше мы видели, что в кольце $\mathbb{Z}$ условие нод$(a, b) = 1$ равносильно разрешимости в целых числах уравнения $ax + by = 1$. Числа a, b, обладающие этим свойством, называются *взаимно простыми*. В произвольном коммутативном кольце K с единицей из разрешимости уравнения $ax + by = 1$ также вытекает отсутствие у элементов a и b необратимых общих делителей: если $a = d\alpha$, $b = d\beta$, и $ax + by = 1$, то $d(\alpha + \beta) = 1$ и d обратим. Однако, отсутствие у a и b необратимых общих делителей, вообще говоря, не гарантирует разрешимости уравнения $ax + by = 1$. Например, в кольце $\mathbb{Q}[x, y]$ многочленов с рациональными коэффициентами от двух переменных x, y одночлены x и y не имеют общих делителей, отличных от констант, однако равенство $f(x, y) \cdot x + g(x, y) \cdot y = 1$ невозможно ни при каких $f, g \in \mathbb{Q}[x, y]$.

Упражнение 1.7. Объясните почему.

Оказывается, что именно разрешимость уравнения $ax + by = 1$ влечёт за собою наличие у элементов a, b многих приятных свойств, которыми обладают взаимно простые целые числа.

Определение 1.2
Элементы a и b произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если уравнение $ax + by = 1$ разрешимо в K относительно x и y.

Лемма 1.3
В произвольном коммутативном кольце K с единицей для любого $c \in K$ и любых взаимно простых $a, b \in K$ справедливы импликации:

(1) если ac делится на b, то c делится на b

(2) если c делится и на a, и на b, то c делится на ab.

Кроме того, если $a \in K$ взаимно прост с каждым из элементов $b_1, \dots, b_n$, то он взаимно прост и с их произведением $b_1 \dots b_n$.

Доказательство. Умножая обе части равенства $ax + by = 1$ на c, получаем соотношение

$$c = acx + bcy\,,$$

из которого вытекают обе импликации (1), (2). Если $\forall\, i\ \exists\, x_i, y_i \in K :\ ax_i + b_i y_i = 1$, то перемножая все эти равенства и раскрывая скобки, получим в левой части сумму, в которой все слагаемые, кроме $(b_1 \dots b_n) \cdot (y_1 \dots y_n)$, делятся на a. Вынося a за скобку, приходим к соотношению $a \cdot X + (b_1 \dots b_n) \cdot (y_1 \dots y_n) = 1$. □

Упражнение 1.8. Пользуясь лем. 1.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое необратимое целое число $z \neq 0$ является произведением конечного числа простых[1], причём любые два таких представления

$$p_1 \dots p_k = z = q_1 \dots q_m$$

имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $p_i = \pm q_i$ для всех i.

Замечание 1.3. (нод и нок в произвольном кольце) В произвольном коммутативном кольце K принято называть *наибольшим общим делителем* элементов $a, b \in K$ любой элемент $d \in K$,

[1]Напомним, что ненулевое необратимое целое число называется *простым*, если оно не раскладывается в произведение двух необратимых целых чисел.

который делит a и b и делится на все их общие делители. Это определение не гарантирует ни существования, ни единственности наибольшего общего делителя, ни его представимости в виде $d = ax + by$. Аналогично, *наименьшим общим кратным* элементов $a, b \in K$ называется любой элемент $c \in K$, который делится на a и b и делит все их общие кратные. Такого элемента тоже может не быть, а если он есть, то не обязательно единствен.

1.4. Кольцо вычетов $\mathbb{Z}/(n)$. Напомню[1], что числа $a, b \in \mathbb{Z}$ называются *сравнимыми* по модулю n, что записывается как $a \equiv b \pmod{n}$, если их разность $a - b$ делится на n. Сравнимость по модулю n является отношением эквивалентности[2] и разбивает множество целых чисел на непересекающиеся классы сравнимых по модулю n чисел. Эти классы называются *классами вычетов по модулю* n, а их совокупность обозначается через $\mathbb{Z}/(n)$. Мы будем писать $[a]_n \in \mathbb{Z}/(n)$ для обозначения класса, содержащего число $a \in \mathbb{Z}$. Такое обозначение не однозначно: разные числа $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$ задают один и тот же класс $[x]_n = [y]_n$ если и только если $x = y + dn$ для некоторого $d \in \mathbb{Z}$. Всего в $\mathbb{Z}/(n)$ имеется n различных классов: $[0]_n$, $[1]_n$, … , $[(n-1)]_n$. Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a + b]\,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\,. \tag{1-20}$$

Согласно упр. 0.9 на стр. 11, эти операции определены корректно[3]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (1-20) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы выполнены.

1.4.1. Делители нуля и нильпотенты. В $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(8)$ ненулевой класс $[2]$ имеет нулевой куб $[2]^3 = [8] = [0]$. Элемент a произвольного коммутативного кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Тривиальным делителем нуля является нуль. Обратимый элемент $a \in K$ не может быть делителем нуля, поскольку, умножая обе части равенства $ab = 0$ на a^{-1}, мы получаем $b = 0$. Тем самым, кольцо с ненулевыми делителями нуля не может быть полем. Кольцо с единицей без ненулевых делителей нуля называется *целостным*.

Элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Тривиальным нильпотентом является нуль. Всякий нильпотент автоматически делит нуль. Кольцо с единицей без ненулевых нильпотентов называется *приведённым*. Например, каждое целостное кольцо приведено.

1.4.2. Обратимые элементы кольца вычетов. Обратимость класса $[m]_n \in \mathbb{Z}/(n)$ означает существование такого класса $[x]_n$, что $[m]_n[x]_n = [mx]_n = [1]_n$. Последнее равенство равносильно наличию таких $x, y \in \mathbb{Z}$, что $mx + ny = 1$ в $\mathbb{Z}$. Тем самым, класс $[m]_n$ обратим в $\mathbb{Z}/(n)$ если и только если нод$(m, n) = 1$ в кольце $\mathbb{Z}$.

Проверить, обратим ли данный класс $[m]_n$, и если да, вычислить $[m]_n^{-1}$, можно при помощи алгоритма Евклида – Гаусса[4]. Так, проделанное в форм. (1-19) на стр. 26 вычисление показывает, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и $10\,203^{-1} = 147 \pmod{4\,687}$, а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $4\,687^{-1} = -320 \pmod{10\,203}$.

[1] См. прим. 0.4 на стр. 11.

[2] См. n° 0.4 на стр. 10.

[3] Т. е. не зависят от способа записи классов или, что то же самое — от выбора представителей $a \in [a]$ и $b \in [b]$.

[4] См. n° 1.2.2 на стр. 25.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют мультипликативную абелеву группу. Она называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^\times$. Порядок этой группы равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается

$$\varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}/(n)^\times\right|$$

и называется *функцией Эйлера* числа $n \in \mathbb{Z}$.

Пример 1.6 (теорема Эйлера и порядок обратимого вычета)
Умножение на фиксированный обратимый вычет $[a] \in \mathbb{Z}/(n)^\times$ задаёт биекцию[1]

$$a:\ \mathbb{Z}/(n)^\times \xrightarrow{\sim} \mathbb{Z}/(n)^\times, \quad [x] \mapsto [ax], \tag{1-21}$$

обратной к которой является умножение на вычет $[a]^{-1}$. Последовательно применяя отображение (1-21) к произвольному элементу $[z] \in \mathbb{Z}/(n)^\times$, получаем цепочку его образов

$$[z] \overset{a}{\mapsto} [az] \overset{a}{\mapsto} [a^2z] \overset{a}{\mapsto} [a^3z] \overset{a}{\mapsto} \dots, \tag{1-22}$$

которые начнут повторяться, ибо множество вычетов конечно. В силу биективности отображения (1-21), самым первым повторно встретившимся элементом цепочки (1-22) станет её начальный элемент $[z]$, т. е. цепочка (1-22) является циклом. В силу всё той же биективности отображения (1-21) два таких цикла, проходящие через классы $[x]$ и $[y]$, либо не пересекаются, либо полностью совпадают. Кроме того, все циклы имеют одинаковую длину.

Упражнение 1.9. Убедитесь, что отображения умножения на $[x]^{-1}[y]$ и на $[y]^{-1}[x]$ суть взаимно обратные биекции между циклами, проходящими через классы $[x]$ и $[y]$.

Мы заключаем, что $\mathbb{Z}/(n)^\times$ распадается в объединение непересекающихся циклов (1-22) *одинаковой длины* m, которая таким образом является делителем числа $\varphi(n) = |\mathbb{Z}/(n)^\times|$. Умножая обе части равенства $[z] = [a]^m[z]$ на $[z]^{-1}$, получаем $[a^m] = [1]$, откуда и $[a^{\varphi(n)}] = [1]$. Иными словами, для любых взаимно простых целых чисел a и n выполняется сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$. Этот факт известен как *теорема Эйлера*. Число m однозначно характеризуется как наименьшее такое $k \in \mathbb{N}$, что $[a]^k = 1$, и называется *порядком* обратимого вычета $[a] \in \mathbb{Z}/(n)^\times$. Как мы видели, порядок каждого обратимого вычета в $\mathbb{Z}/(n)^\times$ делит $\varphi(n)$.

1.4.3. Поля вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из сказанного в начале n° 1.4.2 вытекает, что кольцо вычетов $\mathbb{Z}/(n)$ является полем тогда и только тогда, когда n является *простым числом*. В самом деле, если $n = mk$ составное, ненулевые классы $[m], [k] \in \mathbb{Z}/(n)$ делят нуль и не могут быть обратимы. Напротив, если p простое, то $\text{нод}(m, p) = 1$ для всех m, не кратных p, и значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим. Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$.

Пример 1.7 (бином Ньютона по модулю p)
В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ раз}} = 0\,. \tag{1-23}$$

Из него вытекает, что для любых $a, b \in \mathbb{F}_p$ выполняется равенство

$$(a + b)^p = a^p + b^p\,. \tag{1-24}$$

[1] См. n° 0.5.2 на стр. 15.

В самом деле, раскрывая скобки в биноме $(a+b)^p$, мы для каждого k получим $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ одночленов $a^k b^{p-k}$, сумма которых равна $(1+\ldots+1)\cdot a^k b^{p-k}$, где внутри скобок складываются $\binom{p}{k}$ единиц поля $\mathbb{F}_p$. Такая сумма равна нулю при $0 < k < p$ в силу следующей леммы.

Лемма 1.4
При простом p и любом натуральном k в пределах $1 \leqslant k \leqslant (p-1)$ биномиальный коэффициент $\binom{p}{k}$ делится на p.

Доказательство. Так как число p взаимно просто со всеми числами от 1 до $p-1$, оно по лем. 1.3 взаимно просто с произведением $k!(p-k)!$. Поскольку $p!$ делится на $k!(p-k)!$, из той же лем. 1.3 следует, что $(p-1)!$ делится на $k!(p-k)!$, а значит, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 1.1 (малая теорема Ферма)
Для любого $a \in \mathbb{Z}$ и любого простого $p \in \mathbb{N}$ выполняется сравнение $a^p \equiv a \pmod{p}$.

Доказательство. Надо показать, что $[a^p] = [a]$ в поле $\mathbb{F}_p$. Согласно (1-24)

$$[a]^p = \underbrace{\big([1]+\ldots+[1]\big)^p}_{a \text{ раз}} = \underbrace{[1]^p+\ldots+[1]^p}_{a \text{ раз}} = \underbrace{[1]+\ldots+[1]}_{a \text{ раз}} = [a]\,.$$

□

Упражнение 1.10. Выведите малую теорему Ферма из теоремы Эйлера[1].

Упражнение 1.11. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod{p}$ для всех $m, n \in \mathbb{N}$ и простых $p \nmid m$.

1.5. Гомоморфизмы. Отображение абелевых групп $\varphi : A \to B$ называется *гомоморфизмом*, если для любых $a_1, a_2 \in A$ в группе B выполнено соотношение

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)\,. \tag{1-25}$$

В частности, этим условиям удовлетворяет *нулевой* (или *тривиальный*) гомоморфизм, отображающий все элементы A в нулевой элемент B.

Упражнение 1.12. Убедитесь, что композиция[2] гомоморфизмов — это тоже гомоморфизм.

Любой гомоморфизм $\varphi : A \to B$ переводит нулевой элемент группы A в нулевой элемент группы B, так как из равенств $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$ вытекает, что $0 = \varphi(0)$. Выкладка

$$\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0$$

показывает, что $\varphi(-a) = -\varphi(a)$. Тем самым, *образ* $\operatorname{im}\varphi = \varphi(A) \subset B$ любого гомоморфизма $\varphi : A \to B$ является абелевой подгруппой в B.

1.5.1. Ядро. Полный прообраз нулевого элемента группы B при гомоморфизме $\varphi : A \to B$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi = \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}\,.$$

Ядро образует в A подгруппу, так как из равенств $\varphi(a_1) = 0$ и $\varphi(a_2) = 0$ вытекает равенство

$$\varphi(a_1 \pm a_2) = \varphi(a_1) \pm \varphi(a_2) = 0 \pm 0 = 0\,.$$

[1] См. прим. 1.6 на стр. 29.
[2] См. n° 0.5 на стр. 13.

Предложение 1.1
Каждый непустой слой[1] гомоморфизма абелевых групп $\varphi\colon A \to B$ является сдвигом его ядра:

$$\varphi^{-1}(\varphi(a)) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\} \text{ для всех } a \in A.$$

В частности, все непустые слои находятся в биекции друг с другом, и инъективность гомоморфизма φ равносильна равенству $\ker\varphi = \{0\}$.

Доказательство. Равенства $\varphi(a_1) = \varphi(a_2)$ и $\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = 0$ равносильны. Поэтому элементы $a_1, a_2 \in A$ переходят в один и тот же элемент из B тогда и только тогда, когда $a_1 - a_2 \in \ker(\varphi)$. □

Пример 1.8 (квадраты в поле $\mathbb{F}_p$)
Зафиксируем простое $p > 2$. Отображение $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$, является гомоморфизмом мультипликативной группы ненулевых элементов поля $\mathbb{F}_p$ в себя. Его ядро состоит из таких $x \in \mathbb{F}_p^\times$, что $x^2 = 1$. Поскольку в поле равенство $x^2 - 1 = (x+1)(x-1) = 0$ возможно только для $x = \pm 1$, мы заключаем, что $\ker\varphi = \{\pm 1\}$, и все непустые слои гомоморфизма φ состоят из двух элементов. Поэтому $|\operatorname{im}\varphi| = (p-1)/2$, т. е. ровно половина ненулевых элементов поля $\mathbb{F}_p$ является квадратами. Узнать, является ли квадратом заданное число $a \in \mathbb{F}_p^\times$ можно при помощи другого гомоморфизма $\psi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^{\frac{p-1}{2}}$. По малой теореме Ферма[2] все $(p-1)/2$ ненулевых квадратов лежат в его ядре. Поэтому $|\operatorname{im}\psi| \leqslant 2$.

Упражнение 1.13. Покажите, что ненулевой многочлен степени m с коэффициентами в произвольном поле $\Bbbk$ имеет в этом поле не более m различных корней.

Из упражнения вытекает, что равенство $x^{\frac{p-1}{2}} = 1$ не может выполняться сразу для всех $p-1$ элементов группы $\mathbb{F}_p^\times$. Поэтому $|\operatorname{im}\psi| = 2$ и $|\ker\psi| = (p-1)/2$. Мы заключаем, что $\ker\psi$ состоит в точности из ненулевых квадратов поля $\mathbb{F}_p$. Иными словами, $a \in \mathbb{F}_p^\times$ является квадратом если и только если $a^{\frac{p-1}{2}} = 1$. Например, -1 является квадратом в поле $\mathbb{F}_p$ если и только если $(p-1)/2$ чётно.

Упражнение 1.14. Покажите, что $\operatorname{im}\psi = \{\pm 1\}$.

1.5.2. Группа гомоморфизмов. Для абелевых групп A, B через $\operatorname{Hom}(A,B)$ мы обозначаем множество всех *гомоморфизмов* $A \to B$. Это множество является абелевой группой относительно операции поточечного сложения значений, т. е. $\varphi_1+\varphi_2\colon a \mapsto \varphi_1(a)+\varphi_2(a)$. Нулевым элементом группы $\operatorname{Hom}(A,B)$ является *нулевой гомоморфизм*, отображающий все элементы группы A в нулевой элемент группы B.

1.5.3. Гомоморфизмы колец. Отображение колец $\varphi\colon A \to B$ называется *гомоморфизмом колец*, если для любых $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{1-26}$$

Поскольку гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми свойствами гомоморфизмов абелевых групп. В частности, $\varphi(0) = 0$,

[1] Ср. с n° 0.3 на стр. 7.
[2] См. сл. 1.1 на стр. 30.

$\varphi(-a) = -\varphi(a)$, и все непустые слои φ являются сдвигами слоя над нулём: если $\varphi(a) = b$, то $\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$. Поэтому гомоморфизм φ инъективен тогда и только тогда, когда $\ker\varphi = \{0\}$. Ядро гомоморфизма колец $\varphi\colon A \to B$ вместе с каждым элементом $a \in \ker\varphi$ содержит и все кратные ему элементы aa', поскольку $\varphi(aa') = \varphi(a)\varphi(a') = 0$. В частности, ядро $\ker\varphi$ является подкольцом в A. Образ гомоморфизма колец $\varphi\colon A \to B$ является подкольцом в B, но он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$.

Упражнение 1.15. Убедитесь, что отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[0] \mapsto [0]$, $[1] \mapsto [3]$, является гомоморфизмом колец.

Предложение 1.2
Любой ненулевой гомоморфизм произвольного кольца с единицей в любое целостное[1] кольцо переводит единицу в единицу.

Доказательство. Из равенств $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ вытекает, что $\varphi(1)\big(1 - \varphi(1)\big) = 0$. В целостном кольце такое возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$ для всех $a \in A$. □

1.5.4. Гомоморфизмы полей. Если кольца A и B являются полями, то всякий ненулевой гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом мультипликативных групп этих полей. В частности, $\varphi(1) = 1$ и $\varphi(a/b) = \varphi(a)/\varphi(b)$ для всех a и всех $b \neq 0$.

Предложение 1.3
Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.

Доказательство. Если $\varphi(a) = 0$ для какого-нибудь $a \neq 0$, то для каждого b

$$\varphi(b) = \varphi\left(ba^{-1}a\right) = \varphi\left(ba^{-1}\right)\varphi(a) = 0\,.$$

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

1.5.5. Характеристика. Для любого кольца K с единицей имеется канонический гомоморфизм колец $\varkappa\colon \mathbb{Z} \to K$, заданный правилом

$$\varkappa(\pm n) = \pm\underbrace{(1 + \ldots + 1)}_{n}, \quad \text{где} \quad n \in \mathbb{N}\,. \tag{1-27}$$

Его образ $\operatorname{im}\varkappa$ является наименьшим по включению подкольцом в K с единицей, равной единице кольца K. Если гомоморфизм $\varkappa$ инъективен, то говорят, что кольцо K имеет *характеристику нуль*. В противном случае *характеристикой* $\operatorname{char}(K)$ кольца K называют наименьшее $m \in \mathbb{N}$, для которого $\underbrace{1 + 1 + \cdots + 1}_{m} = 0$. Равенство

$$\underbrace{1 + 1 + \cdots + 1}_{mn} = \underbrace{(1 + 1 + \cdots + 1)}_{m} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{n}$$

[1] Напомню, что *целостным* называется кольцо с единицей без ненулевых делителей нуля, см. n° 1.4.1 на стр. 28.

показывает, что характеристика целостного кольца либо равна нулю, либо является простым числом. Для целостного кольца K характеристики $p > 0$ гомоморфизм $\varkappa$ переводит все числа, кратные p, в нуль и корректно факторизуется до гомоморфизма поля вычетов

$$\varkappa_p : \mathbb{Z}/(p) \to K\,, \quad a \,(\mathrm{mod}\ p) \mapsto \varkappa(a)\,. \tag{1-28}$$

По предл. 1.3 гомоморфизм (1-28) инъективен, и значит, $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p \simeq \mathbb{F}_p$. Таким образом, наименьшее содержащее единицу подкольцо целостного кольца K положительной характеристики является полем, изоморфным полю вычетов $\mathbb{Z}/(p)$ по простому модулю $p \in \mathbb{N}$, равному характеристике $\operatorname{char} K$.

1.5.6. Простое подполе. Пусть теперь $K = \mathbb{F}$ является полем. Его наименьшее по включению подполе называется *простым подполем* в $\mathbb{F}$. В силу своего определения простое подполе содержит образ $\operatorname{im}(\varkappa)$ гомоморфизма (1-27). Если $\operatorname{char}(\mathbb{F}) = p > 0$, то простое подполе совпадает с $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p$ и изоморфно полю вычетов $\mathbb{Z}/(p)$. Если $\operatorname{char}(\mathbb{F}) = 0$, то гомоморфизм $\varkappa$ инъективно вкладывает $\mathbb{Z}$ в $\mathbb{F}$. Так как простое подполе содержит обратные ко всем элементам из $\operatorname{im}\varkappa$, правило $p/q \mapsto \varkappa(p)/\varkappa(q)$ продолжает $\varkappa$ до вложения полей $\varkappa : \mathbb{Q} \hookrightarrow \mathbb{F}$, образ которого совпадает с простым подполем. Тем самым, простое подполе поля характеристики нуль изоморфно полю рациональных чисел $\mathbb{Q}$.

Упражнение 1.16. Покажите, что а) каждый ненулевой гомоморфизм из поля в себя тождественно действует на простом подполе б) между полями разной характеристики не существует ненулевых гомоморфизмов.

Пример 1.9 (автоморфизмы поля $\mathbb{R}$)
Покажем, что каждый ненулевой гомоморфизм $\varphi : \mathbb{R} \to \mathbb{R}$ тождествен. Поскольку неравенство $x_1 < x_2$ равносильно тому, что $x_2 - x_1 = a^2$ для некоторого $a \neq 0$, мы заключаем, что для всех $x_1 < x_2$ выполняется неравенство $\varphi(x_1) < \varphi(x_2)$, ибо $\varphi(x_2) - \varphi(x_1) = \varphi(x_2 - x_1) = \varphi(a^2) = \varphi(a)^2 > 0$. Таким образом, φ является строго монотонной функцией, совпадающей с тождественным отображением $\varphi(x) = x$ на простом подполе $\mathbb{Q} \subset \mathbb{R}$.

Упражнение 1.17 (по анализу). Покажите, что строго монотонная функция $\mathbb{R} \to \mathbb{R}$, совпадающая с функцией $\varphi(x) = x$ на подмножестве $\mathbb{Q} \subset \mathbb{R}$, совпадает с нею всюду.

Пример 1.10 (гомоморфизм Фробениуса)
В поле $\mathbb{F}$ характеристики $\operatorname{char}(\mathbb{F}) = p > 0$ отображение возведения в p-тую степень

$$F_p : \mathbb{F} \to \mathbb{F}\,, \quad x \mapsto x^p\,, \tag{1-29}$$

является гомоморфизмом, поскольку $\forall\, a, b \in \mathbb{F}$ выполняются равенства $(ab)^p = a^p b^p$ и

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \underbrace{(1 + 1 + \cdots + 1)}_{\binom{p}{k}} \cdot a^k b^{p-k} = a^p + b^p$$

(ср. с прим. 1.7 и лем. 1.4 на стр. 30). Гомоморфизм (1-29) называется *гомоморфизмом Фробениуса*. Как и всякий ненулевой гомоморфизм из поля в себя, он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$, что ещё раз доказывает малую теорему Ферма[1].

[1] См. сл. 1.1 на стр. 30.

1.6. Прямые произведения. Прямое произведение абелевых групп $A_1, \dots, A_m$

$$\prod_\nu A_\nu = A_1 \times \dots \times A_\nu \stackrel{\text{def}}{=} \{(a_1, \dots, a_m) \mid a_\nu \in A_\nu \ \forall\, \nu\} \tag{1-30}$$

состоит из упорядоченных наборов $(a_1, \dots, a_m)$ элементов $a_\nu \in A_\nu$ и наделяется структурой абелевой группы посредством покомпонентных операций:

$$(a_1, \dots, a_m) + (b_1, \dots, b_m) \stackrel{\text{def}}{=} (a_1 + b_1, \dots, a_m + b_m)\,. \tag{1-31}$$

Упражнение 1.18. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, \dots, 0)$, а противоположным к набору $(a_1, \dots, a_m)$ является набор $(-a_1, \dots, -a_m)$.

Абелева группа (1-30) называется *прямым произведением* абелевых групп A_i. Если все группы A_i конечны, прямое произведение (1-30) тоже конечно и имеет порядок

$$\left|\prod A_i\right| = \prod |A_i|\,.$$

Прямое произведение имеет смысл не только для конечного набора, но и для произвольного семейства абелевых групп A_x, занумерованных элементами $x \in X$ какого-нибудь множества X. Такое произведение обозначается через $\prod_{x\in X} A_x$.

Аналогичным образом, для любого семейства коммутативных колец $\{K_x\}_{x\in X}$ определено прямое произведение $\prod K_x$, элементами которого являются семейства $(a_x)_{x\in X}$, где каждый элемент a_x лежит в своём кольце K_x. Операции сложения и умножения определяются также покомпонентно:

$$(a_x)_{x\in X} + (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x + b_x)_{x\in X}\ , \qquad (a_x)_{x\in X} \cdot (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x \cdot b_x)_{x\in X}\ .$$

Упражнение 1.19. Убедитесь, что $\prod K_x$ является кольцом, причём если все кольца K_x имеют единицы, то $\prod K_x$ тоже имеет единицу $(1, \dots, 1)$.

Например, если $X = \mathbb{R}$ и все $K_x = \mathbb{R}$, т. е. перемножается континуальное семейство одинаковых экземпляров поля $\mathbb{R}$, занумерованных действительными числами $x \in \mathbb{R}$, то прямое произведение $\prod_{x\in\mathbb{R}} \mathbb{R}_x$ изоморфно кольцу функций $f : \mathbb{R} \to \mathbb{R}$ с обычными операциями поточечного сложения и умножения значений функций. Этот изоморфизм переводит семейство вещественных чисел $(f_x) \in \prod_{x\in\mathbb{R}} \mathbb{R}_x$, занумерованное вещественным числом x, в функцию $f : \mathbb{R} \to \mathbb{R}$, значение которой в точке $x \in \mathbb{R}$ равно x-тому элементу семейства: $f(x) = f_x$.

В прямом произведении колец любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0, 1, \dots, 1)$ делит нуль:

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

Поэтому произведение нескольких колец никогда не является полем. Например, произведение $\mathbb{F}_p \times \mathbb{F}_q$ конечных полей $\mathbb{F}_p$ и $\mathbb{F}_q$ из p и q элементов состоит из $(p-1)(q-1)$ обратимых пар (a, b), образующих мультипликативную группу $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$, и $p + q - 1$ делителей нуля вида $(a, 0)$ или $(0, b)$.

В общем случае элемент $a = (a_1, \dots, a_m) \in K_1 \times \dots \times K_m$ обратим если и только если каждая его компонента $a_\nu \in K_\nu$ обратима в своём кольце K_ν. Поэтому группа обратимых элементов кольца $\prod K_\nu$ является прямым произведением групп обратимых элементов колец K_ν:

$$\left(\prod K_\nu\right)^\times = \prod K_\nu^\times \tag{1-32}$$

1.7. Китайская теорема об остатках. Пусть целое число $n = n_1 \dots n_m$ является произведением попарно взаимно простых чисел $n_1, \dots, n_m \in \mathbb{Z}$. Отображение, переводящее вычет $z \pmod n$ в набор вычетов $z \pmod{n_i}$:

$$\varphi : \mathbb{Z}/(n) \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m), \quad [z]_n \mapsto \bigl([z]_{n_1}, \dots, [z]_{n_m}\bigr), \tag{1-33}$$

корректно определено, поскольку при выборе другого представителя $z_1 \equiv z_2 \pmod n$ разность $z_1 - z_2$ делится на произведение $n = n_1 \dots n_m$, и $[z_1]_{n_i} = [z_2]_{n_i}$ при всех i. Легко видеть, что φ перестановочно со сложением:

$$\begin{aligned}\varphi\bigl([z]_n + [w]_n\bigr) = \varphi\bigl([z+w]_n\bigr) = \bigl([z+w]_{n_1}, \dots, [z+w]_{n_m}\bigr) = \\ = \bigl([z]_{n_1} + [w]_{n_1}, \dots, [z]_{n_m} + [w]_{n_m}\bigr) = \\ = \bigl([z]_{n_1}, \dots, [z]_{n_m}\bigr) + \bigl([w]_{n_1}, \dots, [w]_{n_m}\bigr) = \varphi\bigl([z]_n\bigr) + \varphi\bigl([w]_n\bigr).\end{aligned}$$

Аналогично проверяется, что φ перестановочно с умножением, т. е. является гомоморфизмом колец. Если $[z]_n \in \ker\varphi$, то z делится на каждое n_i, а значит, по лем. 1.3 на стр. 27, делится и на их произведение $n = n_1 \dots n_m$, откуда $[z]_n = 0$. Так как гомоморфизм с нулевым ядром инъективен и в кольцах $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ одинаковое число элементов $n = n_1 \dots n_m$, отображение (1-33) биективно. Этот факт известен как *китайская теорема об остатках*.

На житейском языке он означает, что для любого набора остатков $r_1, \dots, r_m$ от деления на попарно взаимно простые числа $n_1, \dots, n_m$ всегда найдётся число z, имеющее остаток r_i от деления на n_i одновременно для всех i, причём любые два таких числа z_1, z_2 различаются на целое кратное числа $n = n_1 \dots n_k$. Практическое отыскание такого z осуществляется с помощью алгоритма Евклида – Гаусса следующим образом. Из взаимной простоты числа n_i с остальными числами n_ν вытекает[1], что n_i взаимно просто с произведением $m_i = \prod_{\nu \neq i} n_\nu$. Поэтому для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Число $b_i = m_i y_i$ даёт остаток 1 от деления на n_i и делится на все n_ν с $\nu \neq i$. Число $z = r_1 b_1 + \dots + r_m b_m$ решает задачу.

Пример 1.11

Найдём наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$. Сначала найдём число, обратное к $91 \cdot 179$ по модулю 57: замечаем, что $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, применяем алгоритм Евклида – Гаусса[2] к $a = 57$ и $b = 13$ и приходим к равенству $22 \cdot 13 - 5 \cdot 57 = 1$. Таким образом, число

$$b_1 = -22 \cdot 91 \cdot 179 \quad (\equiv 22 \cdot 13 \pmod{57})$$

даёт при делении на 57, 91 и 179 остатки $(1,\ 0,\ 0)$. Аналогично находим числа

$$\begin{aligned} b_2 &= -33 \cdot 57 \cdot 179 \quad (\equiv 33 \cdot 11 \pmod{91}) \\ b_3 &= -45 \cdot 57 \cdot 91 \quad (\equiv 45 \cdot 4 \pmod{179}) \end{aligned}$$

дающие при делении на 57, 91 и 179 остатки $(0,\ 1,\ 0)$ и $(0,\ 0,\ 1)$ соответственно. Требуемые остатки $(2,\ 7,\ 43)$ имеет число

$$\begin{aligned} z = 2\,b_1 + 7\,b_2 + 43\,b_3 = -(2 \cdot 22 \cdot 91 \cdot 179 + 7 \cdot 33 \cdot 57 \cdot 179 + 43 \cdot 45 \cdot 57 \cdot 91) = \\ = -(716\,716 + 2\,356\,893 + 10\,036\,845) = -13\,110\,454, \end{aligned}$$

[1] По всё той же лем. 1.3 на стр. 27.

[2] См. n° 1.2.2 на стр. 25.

а также все числа, отличаются от него на целые кратные числа $n = 57 \cdot 91 \cdot 179 = 928\,473$. Наименьшим положительным среди них является $z + 15\,n = 816\,641$.

Ответы и указания к некоторым упражнениям

Упр. 1.2. Ответы: $1+x$ и $xy+x+y$.

Упр. 1.3. Если умножить числитель и знаменатель любой дроби в левой части равенств (1-11) на c, числитель и знаменатель правой части также умножится на c. Отсюда следует корректность. Проверка аксиом бесхитростна.

Упр. 1.5. Пусть $ax_0+by_0=k$. Тогда $a(x_0+n\beta)+b(y_0-n\alpha)=ax_0+by_0+n(a\beta-b\alpha)=k$ при всех $n\in\mathbb{Z}$. Если $ax+by=k$, то $a(x-x_0)=-b(y-y_0)$ делится на нок$(ab)=\alpha\beta d$. Тем самым, число $n=(x-x_0)/\beta=-(y-y_0)/\alpha\in\mathbb{Z}$, и $x=x_0+n\beta$, а $y=y_0-n\alpha$.

Упр. 1.6. Пусть числа таблицы $\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$ удовлетворяют равенствам $m=xa+by$, $n=as+bt$ и $xt-ys=1$. Прибавляя к 1-й строке 2-ю, умноженную на k, получаем таблицу $\begin{pmatrix} m' & x' & y' \\ n & s & t \end{pmatrix}$, в которой $m'=m+nk$, $x'=x+ks$, $y'=t+kt$. Тогда

$$m'=ax+by+k(as+bt)=ax'+by'$$
$$x't-y's=xt-ys+kst-kst=1\,.$$

Упр. 1.7. Подставьте в это равенство $x=y=0$.

Упр. 1.8. Существование разложения. Если число n простое, то оно само и будет своим разложением. Если n составное, представим его в виде произведения строго меньших по абсолютной величине чисел, каждое из которых в свою очередь или просто или является произведением строго меньших по абсолютной величине чисел и т. д. Поскольку модуль целого числа нельзя бесконечно долго уменьшать, мы в конце концов получим требуемое разложение.

Единственность разложения. Для любого простого числа p и любого целого z имеется альтернатива: либо нод$(z,p)=|p|$, и тогда z делится на p, либо нод$(z,p)=1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1\dots p_k=q_1\dots q_m$ все сомножители просты. Так как $\prod q_i$ делится на p_1, число p_1 не может быть взаимно просто с каждым q_i в силу лем. 1.3 на стр. 27. Согласно упомянутой альтернативе, хотя бы один из множителей q_i (будем считать, что q_1) делится на p_1. Поскольку q_1 прост, $q_1=\pm p_1$. Сокращаем первые множители и повторяем рассуждение.

Упр. 1.9. При любом $k\in\mathbb{N}$ умножение на класс $[x]^{-1}[y]$ переводит класс $[a^kx]$ в класс $[a^ky]$, а умножение на класс $[x][y]^{-1}$ переводит класс $[a^ky]$ назад в $[a^kx]$.

Упр. 1.11. Класс $\binom{mp^n}{p^n}\pmod p$ равен коэффициенту при x^{p^n}, возникающему после раскрытия скобок и приведения подобных слагаемых в биноме $(1+x)^{mp^n}$ над полем $\mathbb{F}_p$. Последовательно применяя формулу форм. (1-24) на стр. 29, получаем

$$(1+x)^{p^nm}=\left((1+x)^p\right)^{p^{n-1}m}=\left(1+x^p\right)^{p^{n-1}m}=\left((1+x^p)^p\right)^{p^{n-2}m}=\left(1+x^{p^2}\right)^{p^{n-2}m}=\ \cdots$$
$$\cdots\ =\left(1+x^{p^n}\right)^m=1+mx^{p^n}+\text{ старшие степени}$$

Упр. 1.13. Если число $\alpha\in\Bbbk$ является корнем многочлена $f(x)$, то $f(x)$ делится на $(x-\alpha)$ (разделите $f(x)$ на $(x-\alpha)$ с остатком и подставьте $x=\alpha$).

Упр. 1.14. По малой теореме Ферма[1] каждый элемент $x\in\operatorname{im}\psi$ удовлетворяет уравнению $x^2=1$.

[1] См. сл. 1.1 на стр. 30.

Упр. 1.16. Ненулевой гомоморфизм полей инъективен, переводит единицу в единицу и перестановочен со сложением, вычитанием, умножением и делением[1]. Простое подполе состоит из элементов вида $\pm(1 + \cdots + 1)/(1 + \cdots + 1)$, каждый из которых остаётся на месте. Если имеется ненулевой гомоморфизм $\Bbbk \to \mathbb{F}$, то равенство или неравенство нулю суммы некоторого количества единиц в поле $\Bbbk$ влечёт точно такое же равенство или неравенство в поле $\mathbb{F}$, откуда $\operatorname{char}\Bbbk = \operatorname{char}\mathbb{F}$.

Упр. 1.17. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

[1] См. n° 1.5.4 на стр. 32.