§2. Коммутативные кольца и поля

2.1. Определения и примеры. Говоря вольно, поле представляет собою числовую область, где определены четыре стандартные арифметических 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 2.1
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: $$a + b = b + a \quad \forall\, a, b \in \mathbb{F} \tag{2-1}$$

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

наличие нуля: $$\exists\, 0 \in \mathbb{F} : \quad a + 0 = a \quad \forall\, a \in \mathbb{F} \tag{2-3}$$

наличие противоположных: $$\forall\, a \in \mathbb{F} \quad \exists\, (-a) \in \mathbb{F} : \quad a + (-a) = 0 \tag{2-4}$$

свойства умножения

коммутативность: $$ab = ba \quad \forall\, a, b \in \mathbb{F} \tag{2-5}$$

ассоциативность: $$a\,(bc) = (ab)\,c \quad \forall\, a, b, c \in \mathbb{F} \tag{2-6}$$

наличие единицы: $$\exists\, 1 \in \mathbb{F} : \quad 1\,a = a \quad \forall\, a \in \mathbb{F} \tag{2-7}$$

наличие обратных: $$\forall\, a \in \mathbb{F} \smallsetminus 0 \quad \exists\, a^{-1} \in \mathbb{F} : \quad aa^{-1} = 1 \tag{2-8}$$

свойства, связывающие сложение с умножением

дистрибутивность: $$a(b + c) = ab + ac \quad \forall\, a, b, c \in \mathbb{F} \tag{2-9}$$

нетривиальность: $$0 \neq 1 \tag{2-10}$$

Пример 2.1 (поле из двух элементов)
Простейший объект, удовлетворяющий всем аксиомам из опр. 2.1 — это поле $\mathbb{F}_2$, состоящее только из двух элементов 0 и 1, таких что $0+1 = 1\cdot 1 = 1$, а все остальные суммы и произведения равны нулю.

Упражнение 2.1. Проверьте, что $\mathbb{F}_2$ действительно является полем.

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, а операции сложения и умножения — как операции сложения и умножения классов вычетов, определённые формулами (1-20) – (1-21) на стр. 12. 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 2.2. 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: $0 + 1 = 1 + 0 = 1$, но $0 + 0 = 1 + 1 = 0$.

[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 2.2 (рациональные числа)
Напомним, 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, содержащим все отождествления

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

(см. n° 1.4.1). Сложение и умножение дробей определяется формулами

$$\frac{a}{b} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{ad + bc}{bd}\,, \qquad \frac{a}{b} \cdot \frac{c}{d} \stackrel{\text{def}}{=} \frac{ac}{bd}\,. \tag{2-11}$$

Упражнение 2.3. Проверьте, что эти операции определены корректно (результат не зависит от выбора представителей в классах) и удовлетворяют аксиомам поля.

Пример 2.3 (вещественные числа)
Множество вещественных чисел $\mathbb{R}$ определяется в курсе анализа несколькими различными способами: как множество классов эквивалентности десятичных[2] 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. Какое бы описание множества $\mathbb{R}$ ни использовалось, задание на нём сложения и умножения и проверка аксиом из опр. 2.1 требуют некоторой умственной работы, традиционно проделываемой в курсе анализа.

2.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти эти операции обладают всеми свойствами из опр. 2.1 на стр. 20 за исключением свойства (2-8) существования мультипликативно обратного элемента.

Если, кроме существования обратного, из списка аксиом поля исключаются требование существования единицы (2-7) и условие $0 \neq 1$, 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.

2.1.2. Абелевы группы. Множество A *с одной* операцией $A \times A \to A$, удовлетворяющей первым четырём аксиомам сложения из опр. 2.1, 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]Или привязанных к какой-либо другой позиционной системе счисления, например, двоичных.

Пример 2.4 (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. 2◇1 и рис. 2◇2.

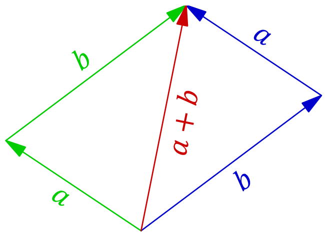

Рис. 2◇1. Правило параллелограмма.

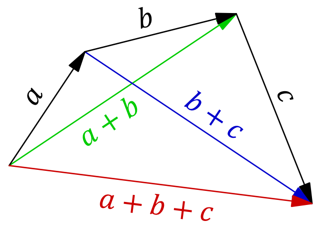

Рис. 2◇2. Правило четырёхугольника.

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

Пример 2.5 (мультипликативная группа поля)

Четыре аксиомы умножения из опр. 2.1 на стр. 20 утверждают, то множество

$$\mathbb{F}^* \stackrel{\text{def}}{=} \mathbb{F} \smallsetminus 0$$

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 $\mathbb{F}^*$ исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Лемма 2.1

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 2.2

В любом коммутативном кольце с единицей для любого элемента a выполняются равенства $0 \cdot a = 0$ и $(-1) \cdot a = -a$.

Доказательство. Пусть $a \cdot 0 = b$. Тогда $b + a = a \cdot 0 + a \cdot 1 = a(0+1) = a \cdot 1 = a$. Прибавляя к обеим частям этого равенства $(-a)$, получаем $b = 0$. Второе утверждение проверяется выкладкой $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$. □

Замечание 2.1. Аксиома нетривиальности (2-10) в определении поля равносильна требованию $\mathbb{F} \neq 0$, поскольку при $0 = 1$ для каждого $a \in \mathbb{F}$ получалось бы $a = a \cdot 1 = a \cdot 0 = 0$. Образование, состоящее из одного нуля, согласно предыдущим определениям является коммутативным кольцом (без единицы), но не полем.

2.1.3. Вычитание и деление. Из лем. 2.1 вытекает, что в любой абелевой группе корректно определена *разность* любых двух элементов

$$a - b \stackrel{\text{def}}{=} a + (-b)\,. \tag{2-12}$$

В частности, операция вычитания имеется в абелевой 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 (2-12) имеется операция *деления* на любые ненулевые элементы

$$a/b \stackrel{\text{def}}{=} ab^{-1}\,, \quad b \neq 0\,. \tag{2-13}$$

2.2. 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 только ненулевые константы (многочлены степени нуль).

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 $a \mathrel{\vdots} b$ (читается «a делится на b»). Отношение делимости тесно связано с решением линейных уравнений.

2.2.1. Уравнение $ax + by = k$ и НОД в кольце $\mathbb{Z}$. Зафиксируем какие-нибудь целые числа a и b и обозначим через

$$(a, b) \stackrel{\text{def}}{=} \{ax + by \mid x, y \in \mathbb{Z}\} \tag{2-14}$$

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 $z - kd$, а z и $-kd$ лежат в (a, b) при любом k. 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 $\text{нод}(a, b)$.

Упражнение 2.4. Обобщите предыдущее рассуждение: для любого конечного набора чисел $a_1, \dots, a_m \in \mathbb{Z}$ укажите число $d \in \mathbb{Z}$, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + \dots + a_mx_m$ с целыми x_i. Покажите, что уравнение $n = a_1x_1 + \dots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ если и только если $d|n$.

2.2.2. Алгоритм Евклида позволяет явно найти нод(a, b) для данных $a, b \in \mathbb{Z}$ и представить его в виде нод$(a, b) = ax + by$ с целыми x, y. Пусть $a \geqslant b$. Положим

$$E_0 = a\,,\ E_1 = b\,,\ E_k = \text{остатку от деления } E_{k-2} \text{ на } E_{k-1} \text{ при } k \geqslant 2. \tag{2-15}$$

Числа E_k строго убывают до тех пор, пока очередное число E_r не разделит нацело предыдущее число E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой элемент E_r последовательности E_k и будет наибольшим общим общим делителем нод(a, b).

Упражнение 2.5. Докажите это.

Чтобы получить представление $E_r = x \cdot E_0 + y \cdot E_1$ на каждом шаге вычисления надо представлять очередное E_k в виде $E_k = x \cdot E_0 + y \cdot E_1$. Например, для чисел $n = 10\,203$ и $m = 4\,687$ вычисление состоит из восьми шагов:

$$\begin{array}{rrrrr}
E_0 = & 10\,203 & = & +1\,E_0 & +0\,E_1 \\
E_1 = & 4\,687 & = & +0\,E_0 & +1\,E_1 \\
E_2 = & 829 = & E_0 - 2\,E_1 = & +1\,E_0 & -2\,E_1 \\
E_3 = & 542 = & E_1 - 5\,E_2 = & -5\,E_0 & +11\,E_1 \\
E_4 = & 287 = & E_2 - E_3 = & +6\,E_0 & -13\,E_1 \\
E_5 = & 255 = & E_3 - E_4 = & -11\,E_0 & +24\,E_1 \\
E_6 = & 32 = & E_4 - E_5 = & +17\,E_0 & -37\,E_1 \\
E_7 = & 31 = & E_5 - 7\,E_6 = & -130\,E_0 & +283\,E_1 \\
E_8 = & 1 = & E_6 - E_7 = & +147\,E_0 & -320\,E_1 \\
\left[E_9 = \right. & 0 = & E_7 - 31\,E_8 = & -4\,687\,E_0 & \left. +10\,203\,E_1\right]
\end{array} \tag{2-16}$$

(взятая в скобки последняя строка служит для проверки). Таким образом,

$$\text{нод}(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687\,.$$

Упражнение 2.6. Докажите, что в возникающем на последнем шаге работы алгоритма Евклида представлении нуля в виде $0 = E_{r+1} = q_0 E_0 + q_1 E_1$ число $|q_0 E_0| = |q_1 E_1|$ рано *наименьшему общему кратному* нок(a, b) чисел a и b.

Замечание 2.2. С вычислительной точки зрения отыскание нод(a, b) при помощи алгоритма Евклида *несопоставимо* быстрее разложения чисел a и b на простые множители. Читателю предлагается убедиться в этом, попытавшись вручную разложить на простые множители исходные числа $n = 10\,203$ и $m = 4\,687$ из проделанного выше вручную вычисления (2-16). Если задано произведение двух *очень* больших простых чисел, то найти по нему сами эти числа за разумное время не под силу даже мощным компьютерам. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

2.3. Взаимная простота. В кольце целых чисел $\mathbb{Z}$ условие нод$(a, b) = 1$ равносильно разрешимости в целых числах уравнения $ax+by = 1$, и числа a, b, обладающие этими свойствами, 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 многочленов от двух переменных $\mathbb{Q}[x, y]$ 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 2.7. Объясните почему.

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

Определение 2.2

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 2.3

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 и 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 $b_1 \dots b_m$.

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 2.8. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое целое число z является произведением конечного числа простых чисел[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 2.3. (нод в произвольном коммутативном кольце) Если коммутативное кольцо K произвольно, то *наибольшим общим делителем* элементов $a, b \in K$ принято называть любой элемент $d \in K$, который делит a и b и делится на любой общий делитель чисел a и b. Это определение не гарантирует ни существования, ни единственности наибольшего общего делителя, ни его представимости в виде $d = ax + by$.

[1] Напомним, что целое число называется *простым*, если оно не раскладывается в произведение двух чисел, каждое из которых отлично от ± 1.

2.4. Кольцо вычетов $\mathbb{Z}/(n)$. Напомним, 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[1] 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:

$$[a] + [b] \stackrel{\text{def}}{=} [a + b]\,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\,. \tag{2-17}$$

Согласно упр. 1.10 на стр. 12, эти операции определены корректно[2]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (2-17) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы выполнены.

2.4.1. 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 $[2]^3 = [8] = [0]$.

В произвольном кольце K элемент $a \in K$ называется *делителем нуля*, если $a \neq 0$ и $ab = 0$ для некоторого ненулевого $b \in K$. Обратимый элемент $a \in K$ не может быть делителем нуля, поскольку, умножая обе части равенства $ab = 0$ на a^{-1}, мы получаем $b = 0$. Поэтому кольцо с делителями нуля не может быть полем. Кольцо с единицей без делителей нуля называется *целостным*.

Ненулевой элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Всякий нильпотент автоматически является делителем нуля. Кольцо с единицей без нильпотентов называется *приведённым*. Всякое целостное кольцо автоматически приведено.

2.4.2. 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 кольце $\mathbb{Z}/(n)$ если и только если нод$(m, n) = 1$ в кольце $\mathbb{Z}$.

Проверить, обратим ли данный класс $[m]_n$, и если да, то вычислить $[m]_n^{-1}$, можно при помощи алгоритма Евклида[3]. Так, проделанное в форм. (2-16) на стр. 24 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 $4\,687^{-1} = -320 \pmod{10\,203}$.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют мультипликативную абелеву группу. Она называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Порядок этой группы равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается через $\varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}/(n)^*\right|$ и называется *функцией Эйлера* числа $n \in \mathbb{Z}$.

2.4.3. Поля вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из предыдущего 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 $[m], [k] \in \mathbb{Z}/(n)$ будут делителями нуля и не могут быть

[1] См. n° 1.4 на стр. 10.

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

[3] См. n° 2.2.2 на стр. 24.

обратимы. Напротив, если p простое число, то 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 2.6 (бином Ньютона по модулю p)
В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ раз}} = 0\,. \tag{2-18}$$

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

$$(a + b)^p = a^p + b^p\,. \tag{2-19}$$

В самом деле, раскрывая скобки в биноме $(a + b)^p$, мы для каждого k получим $\binom{p}{k}$ одночленов $a^k b^{p-k}$, сумма которых равна $a^k b^{p-k} \cdot (1 + 1 + \cdots + 1)$, где в скобках стоит сумма $\binom{p}{k}$ единиц, равная нулю при $0 < k < p$.

Лемма 2.4
При простом p и любом 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. 2.3 взаимно просто с произведением $k!(p-k)!$. Поскольку $p!$ делится на $k!(p-k)!$, из той же лем. 2.3 следует, что $(p - 1)!$ делится на $k!(p - k)!$, а значит, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 2.1 (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 (2-19), имеем

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

□

Упражнение 2.9. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod{p}$ для простого $p \nmid m$.

2.5. Прямые произведения. Прямое произведение

$$\prod_\nu A_\nu = A_1 \times \ldots \times A_\nu = \{(a_1, \ldots, a_m) \mid a_\nu \in A_\nu\ \forall\, \nu\} \tag{2-20}$$

абелевых групп $A_1, \ldots, A_m$ состоит из упорядоченных наборов $(a_1, \ldots, a_m)$ элементов $a_\nu \in A_\nu$ и обладает естественной структурой абелевой группы относительно покомпонентных операций:

$$(a_1, \ldots, a_m) + (b_1, \ldots, b_m) \stackrel{\text{def}}{=} (a_1 + b_1, \ldots, a_m + b_m)\,. \tag{2-21}$$

Упражнение 2.10. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, 0, \ldots, 0)$, а противоположным к набору $(a_1, \ldots, a_m)$ является набор $(-a_1, \ldots, -a_m)$.

Абелева группа (2-20) называется *прямым произведением* абелевых групп A_i. Если все группы A_i конечны, прямое произведение (2-20) тоже конечно и имеет порядок

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

Прямые произведения имеют смысл не только для конечных, но и для любых семейств абелевых групп A_x, занумерованных элементами $x \in X$ произвольного множества X. Соответствующее произведение обозначается в этом случае через $\prod\limits_{x\in X} A_x$.

Аналогичным образом, для любого семейства коммутативных колец $\{K_x\}_{x\in X}$ определено прямое произведение $\prod K_x$, представляющее собою множество семейств элементов $(a_x)_{x\in X}$, в которых каждый элемент a_x лежит в своём кольце K_x. Операции сложения и умножения также определяются покомпонентно:

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

Упражнение 2.11. Убедитесь, что $\prod K_x$ является кольцом, причём если все K_x были кольцами с единицей, то $\prod K_x$ также будет кольцом с единицей $(1, 1, \dots, 1)$.

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 $\prod\limits_{x\in\mathbb{R}} \mathbb{R}_x$ канонически изоморфно кольцу функций $f : \mathbb{R} \to \mathbb{R}$ с обычными операциями поточечного сложения и умножения значений функций. Этот изоморфизм переводит семейство вещественных чисел $(f_x) \in \prod\limits_{x\in\mathbb{R}} \mathbb{R}_x$, 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, $(0, 1, \dots, 1)$ является делителем нуля, так как $(0, 1, \dots, 1)(1, 0, \dots, 0) = (0, 0, \dots, 0) = 0$. Поэтому произведение нескольких колец никогда не является полем. Например, в произведении $\mathbb{F}_p \times \mathbb{F}_q$ конечных полей $\mathbb{F}_p$ и $\mathbb{F}_q$, состоящих из p и q элементов соответственно, имеется ровно $(p-1)(q-1)$ обратимых элементов (a, b), образующих мультипликативную группу $\mathbb{F}_p^* \times \mathbb{F}_q^*$, и $p+q-2$ делителя нуля, имеющих вид $(a, 0)$ и $(0, b)$ с $a, b \neq 0$.

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:

$$\left(\prod K_\nu\right)^* = \prod K_\nu^* \tag{2-22}$$

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

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)\,. \tag{2-23}$$

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

Упражнение 2.12. Убедитесь, что композиция гомоморфизмов — это тоже гомоморфизм.

Любой гомоморфизм $\varphi\colon A \to B$ 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 $0 = \varphi(0)$. Равенства

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

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

2.6.1. Ядро гомоморфизма. Полный прообраз нулевого элемента группы B при гомоморфизме $\varphi\colon A \to B$ 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

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

Предложение 2.1

Слой любого гомоморфизма абелевых групп $\varphi\colon A \to B$ над произвольной точкой $b \in B$ либо пуст, либо равен $a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$, где $a \in A$ — произвольно выбранный элемент, переходящий в b. В частности, все непустые слои находятся в биекции с $\ker\varphi$, 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 $a_1 - a_2 \in \ker(\varphi)$. □

2.6.2. 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:

$$\varphi_1 + \varphi_2\colon a \mapsto \varphi_1(a) + \varphi_2(a)\,.$$

Нулевым элементом группы $\operatorname{Hom}(A, B)$ является *нулевой гомоморфизм*, отображающий все элементы A в нулевой элемент B.

2.6.3. 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:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{2-24}$$

Поскольку гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми свойствами гомоморфизмов абелевых групп. В частности, $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, 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 $\varphi\colon A \to B$ очевидно является подкольцом в B, однако он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$.

Упражнение 2.13. Убедитесь, что отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[0] \mapsto [0]$, $[1] \mapsto [3]$, является гомоморфизмом колец.

Предложение 2.2
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 равенство

$$\varphi(1)\big(1 - \varphi(1)\big) = 0\,.$$

В целостном кольце такое возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\forall\, a \in A \;\; \varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$. □

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

Предложение 2.3
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. □

2.7. 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 $z \pmod{n_i}$:

$$\begin{aligned} \varphi : \mathbb{Z}/(n) &\to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m) \\ [z]_n &\mapsto \left([z]_{n_1}, \dots, [z]_{n_m}\right), \end{aligned} \tag{2-25}$$

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:

$$\begin{gathered} \varphi\big([z]_n + [w]_n\big) = \varphi\big([z+w]_n\big) = \big([z+w]_{n_1}, \dots, [z+w]_{n_m}\big) = \big([z]_{n_1} + [w]_{n_1}, \dots, [z]_{n_m} + [w]_{n_m}\big) = \\ = \big([z]_{n_1}, \dots, [z]_{n_m}\big) + \big([w]_{n_1}, \dots, [w]_{n_m}\big) = \varphi\big([z]_n\big) + \varphi\big([w]_n\big) \end{gathered}$$

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. 2.3 на стр. 25, 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 (2-25) 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 следующим образом. Из взаимной простоты числа n_i с остальными числами n_ν

[1] Напомню, что *целостным* называется кольцо с единицей без делителей нуля, см. n° 2.4.1 на стр. 26.

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 $z = r_1 b_1 + \cdots + r_m b_m$ решает задачу.

Пример 2.7
Для демонстрации эффективности предыдущего алгоритма 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 к $E_0 = 57$ и $E_1 = 13$, 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

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

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

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

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

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

$$\varkappa(\pm n) = \pm(\underbrace{1 + 1 + \cdots + 1}_{n})\,, \quad \text{где} \quad n \in \mathbb{N}\,. \tag{2-26}$$

Образ $\operatorname{im}\varkappa$ является наименьшим 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

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

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

$$\varkappa_p : \mathbb{Z}/(p) \to K\,, \quad a \pmod{p} \mapsto \varkappa(a)\,. \tag{2-27}$$

[1] По всё той же лем. 2.3 на стр. 25.

По предл. 2.3 гомоморфизм (2-27) 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 $\operatorname{char} K$.

2.8.1. 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 (2-26). 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 2.14. 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 2.8 (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 $\varphi(x_1) < \varphi(x_2)$, так как $\varphi(x_2) - \varphi(x_1) = \varphi(x_2 - x_1) = \varphi(a^2) = \varphi(a)^2 > 0$. Таким образом, φ является строго монотонной функцией, совпадающей с тождественным отображением $\varphi(x) = x$ на простом подполе $\mathbb{Q} \subset \mathbb{R}$.

Упражнение 2.15 (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.

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

$$F_p : \mathbb{F} \to \mathbb{F}, \quad x \mapsto x^p, \tag{2-28}$$

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. 2.6 и лем. 2.4 на стр. 27). Гомоморфизм (2-28) называется *гомоморфизмом Фробениуса*. Как и всякий ненулевой гомоморфизм из поля в себя, он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$, ср. со сл. 2.1 на стр. 27.

Ответы и указания к некоторым упражнениям

Упр. 2.2. Ответы: $1+x$ и $xy+x+y$.

Упр. 2.3. При умножении числителя и знаменателя любой из дробей в левых частях равенств форм. (2-11) на стр. 21 на одно и то же число c, числитель и знаменатель дроби в правой части соответствующего равенства также умножатся на c. Отсюда следует корректность. Проверка выполнения аксиом бесхитростна.

Упр. 2.5. Возрастающая индукция по k, начинающаяся с $k=0$, показывает, что все числа E_k лежат в (a,b), в частности, делятся на нод(a,b). С другой стороны, убывающая индукция по k, начинающаяся с $k=r+1$, показывает, что все числа E_k (в том числе $E_0=a$ и $E_1=b$) делятся на E_r. Поэтому и нод$(a,b)=ax+by$ делится E_r.

Упр. 2.8. Существование. 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. Для любого простого числа p и любого целого числа z выполняется следующая 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 $p_1p_2\cdots p_k=q_1q_2\cdots q_m$ все сомножители просты. Поскольку $\prod q_i$ делится на p_1, число p_1, в силу лем. 2.3, не может быть взаимно просто с каждым q_i. Согласно упомянутой выше альтернативе, хотя бы один из множителей q_i (можно считать, что q_1) делится на p_1. Поскольку q_1 прост, $q_1=\pm p_1$. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.9. 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. (2-19) на стр. 27, 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. 2.14. 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. 2.15. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

[1] См. n° 2.6.4 на стр. 30.