§2. Коммутативные кольца и поля

2.1. Определения и примеры. Говоря вольно, поле — это числовая область, в которой есть четыре обычных арифметических операции: сложение, вычитание, умножение и деление, обладающие привычными свойствами соответствующих действий над рациональными числами. Аксиоматизация этих свойств приводит к такому определению:

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

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

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

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

свойства умножения

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

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

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

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

свойства, связывающие сложение с умножением

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

нетривиальность: $0\neq 1$ (2-10)

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

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) и (1-21) из упр. 1.9 на стр. 10. 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.

[1]т. е. высказывание $A+B$ истинно тогда и только тогда, когда истинно *ровно одно* из высказываний A, B

[2]т. е. высказывание AB истинно , если и только если истинны *оба* высказывания A, B

Упражнение 2.2. Напишите над полем $\mathbb{F}_2$ многочлен от x, равный «не x», а 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

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

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 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. 15 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.

[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

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*.

Пример 2.4 (геометрические векторы)
Будем называть *геометрическим вектором* класс направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему отрезки, 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 демонстрируются на рис. 2◇1 и рис. 2◇2.

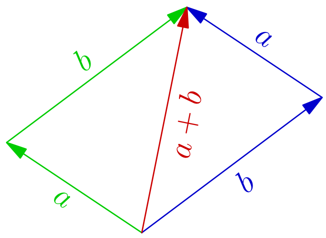

Рис. 2◇1. Правило параллелограмма.

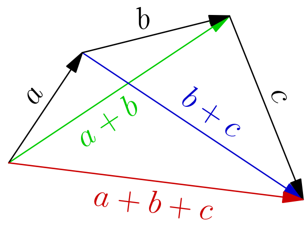

Рис. 2◇2. Правило четырёхугольника.

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. 15 утверждают, то множество

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

всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно 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 единственен, и для любого $a \in A$ элемент, противоположный к a, однозначно определяется по a (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, поскольку 0_2 является нулевым элементом, второе — в силу того, то 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 K для любого $a \in K$ выполняется равенство $0 \cdot a = 0$, и если в K имеется единица, то $(-1) \cdot a$ противоположен к a для любого $a \in A$.

Доказательство. Пусть $a \cdot 0 = b$. Тогда $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0+1) = a \cdot 1 = a$. 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 $a \in \mathbb{F}$ выполнялось бы равенство $a = a \cdot 1 = a \cdot 0 = 0$. 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 определяются по a. Тем самым, в любом поле помимо сложения, умножения и вычитания (2-12) имеется операциия *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 элемент q, такой 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.

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 образует в $\mathbb{Z}$ подкольцо, и вместе с каждым своим элементом содержит и все его кратные. Кроме того, все числа из (a, b) нацело делятся на каждый общий делитель чисел a и b, и 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 кольце (a, b), поскольку он представляется в виде

$z - kd$, а z и kd лежат в кольце (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. Произвольное число $k \in \mathbb{Z}$ представляется в виде $k = ax + by$ тогда и только тогда, когда 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 $a_1, a_2, \dots, a_m$ постройте число d, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + a_2x_2 + \dots + a_mx_m$ с целыми x_i. Покажите, что уравнение $n = a_1x_1 + a_2x_2 + \dots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ тогда и только тогда, когда n делится на d.

2.2.2. Алгоритм Евклида позволяет явно найти $\text{нод}(a, b)$ и представить его в виде $\text{нод}(a, b) = ax + by$. Пусть $a \geqslant b$. Положим

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

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 чисел (a, b), причём он автоматически получится представленным в виде $E_r = x \cdot E_0 + y \cdot E_1$, если при вычислении каждого E_k мы будем представлять его в виде $E_k = x \cdot E_0 + y \cdot E_1$.

Упражнение 2.5. Докажите это.

Например, для чисел $n = 10\,203$ и $m = 4\,687$ вычисление состоит из восьми шагов:

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

(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 $0 = E_{r+1} = q_0E_0 + q_1E_1$ число $|q_0E_0| = |q_1E_1|$ рано *наименьшему общему кратному* $\text{нок}(a, b)$.

Замечание 2.2. С вычислительной точки зрения алгоритм Евклида *несопоставимо* быстрее разложения на простые множители. Читателю предлагается убедиться в этом, попытавшись «вручную» разложить на простые множители числа $n = 10\,203$ и $m = 4\,687$ из абсолютно ручного вычисления (2-16). Найти два очень больших простых числа по заданному их произведению невозможно за разумное время даже на мощном компьютере. 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 $ax + by = 1$ вытекает отсутствие у элементов a и b необратимых общих делителей: если $a = d\alpha$, $b = d\beta$, и при этом $ax + by = 1$, 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.

В произвольном кольце 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 $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением $b_1 b_2 \ \dots \ b_m$.

Доказательство. Умножая обе части равенства $ax + by = 1$ на c, получаем $c = acx + bcy$, откуда сразу следуют обе импликации (1) и (2). Пусть для каждого i существуют такие $x_i, y_i \in K$, что $ax_i + b_i y_i = 1$. Перемножим все эти равенства и раскроем скобки в левой части. Получим сумму, где все слагаемые, кроме $(b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n)$, делятся на a. Вынося a за скобку, приходим к соотношению $a \cdot X + (b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) = 1$. □

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 $p_1 p_2 \cdots p_k = z = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\, i \ p_i = \pm q_i$.

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

2.3.1. Замечание о НОД. В произвольном коммутативном кольце K, элементы которого никак не упорядочены, *наибольший общий делитель* элементов $a, b \in K$ определяется как такой элемент $d \in K$, который делит a и b и делится на любой элемент с таким свойством. Это определение не гарантирует ни единственности наибольшего общего делителя (даже в кольце $\mathbb{Z}$ по этому определению мы получаем два наибольших общих делителя, различающиеся знаком) ни его представимости в виде $d = ax + by$.

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 (см. n° 1.4) 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 $a \in \mathbb{Z}$. Такая запись как обозначение для класса неоднозначна: числа $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$ задают один и тот же класс $[x]_n = [y]_n$ тогда и только тогда, когда $x = y + dn$ для некоторого $d \in \mathbb{Z}$.

Всего имеется n различных классов: $[0]_n, [1]_n, \dots, [(n-1)]_n$. Сложение и умножение классов вычетов задаётся правилами:

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

Согласно упр. 1.9 на стр. 10, эти операции определены корректно[1]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (2-17) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы кольца выполняются.

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.

Упражнение 2.9. Составьте таблицы сложения и умножения в кольцах $\mathbb{Z}/(n)$ для $n = 3, 4, 5, 6, 7, 8$. Найдите в этих кольцах все делители нуля, все нильпотенты, и все обратимые элементы. Для обратимых элементов составьте таблицу обратных. Какие из этих колец являются полями?

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 кольце $\mathbb{Z}$. Тем самым, класс $[m]_n$ обратим в кольце $\mathbb{Z}/(n)$ тогда и только тогда, когда нод$(m, n) = 1$ в $\mathbb{Z}$.

---

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

Проверить, обратим ли данный класс $[m]_n$ и вычислить $[m]_n^{-1}$ можно при помощи алгоритма Евклида из n° 2.2.2. К примеру, вычисление из формулы 2-16 на 19 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 абелеву группу относительно умножения. Она называется*группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Её порядок равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается через $\varphi(n)$ и называется *функцией Эйлера* числа n.

2.4.3. Поля вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из сказанного выше 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 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. Поскольку число p взаимно просто с каждым из чисел в пределах от 1 до $p - 1$, оно по лем. 2.3 взаимно просто с произведением $k!\,(p - k)!$. Поскольку $p!$ делится на $k!\,(p - k)!$, мы из того же лем. 2.3 заключаем, что $(p - 1)!$ делится на $k!\,(p - k)!$. Следовательно, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ 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

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

□

Упражнение 2.10. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod{p}$ при нод$(m, p) = 1$.

2.5. Прямые произведения. Прямое поизведение

$$\prod_{\nu} A_\nu = A_1 \times A_2 \times \cdots \times A_\nu = \{(a_1, a_2, \dots, a_m) \mid a_\nu \in A_\nu \ \forall \nu\} \tag{2-20}$$

абелевых групп $A_1, A_2, \dots, A_m$ состоит из упорядоченных наборов $(a_1, a_2, \dots, a_m)$ элементов $a_\nu \in A_\nu$ и обладает естественной структурой абелевой группы относительно покомпонентных операций:

$$(a_1, a_2, \dots, a_m) + (b_1, b_2, \dots, b_m) = (a_1 + b_1,\ a_2 + b_2,\ \cdots\ ,\ a_m + b_m)\,. \tag{2-21}$$

Упражнение 2.11. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, 0, \dots, 0)$, а противоположным к набору $(a_1, a_2, \dots, a_m)$ является набор $(-a_1, -a_2, \dots, -a_m)$.

Абелева группа (2-20) называется *прямым произведением* абелевых групп $A_1, A_2, \dots, A_m$. Если все группы A_i конечны, прямое произведение (2-20) тоже конечно и имеет порядок

$$\left|\prod A_\nu\right| = \prod |A_\nu|\,.$$

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

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

$$\left(a_x\right)_{x \in X} + \left(b_x\right)_{x \in X} = \left(a_x + b_x\right)_{x \in X}\ , \qquad \left(a_x\right)_{x \in X} \cdot \left(b_x\right)_{x \in X} = \left(a_x \cdot b_x\right)_{x \in X}$$

Упражнение 2.12. 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 $(1, 1, \dots, 1) \in \prod K_x$.

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 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, т. к. $(0,\ 1,\ \dots\ ,\ 1)(1,\ 0,\ \dots\ ,\ 0) = (0,\ 0,\ \dots\ ,\ 0) = 0$. Поэтому произведение нескольких[1] колец (в частности, произведение нескольких полей) никогда не является полем.

Если $\mathbb{F}_p$ и $\mathbb{F}_q$ — конечные поля, состоящие соответственно из p и q элементов, то в их произведении $\mathbb{F}_p \times \mathbb{F}_q$ будет ровно $(p-1)(q-1)$ обратимых элементов (a, b), составляющих

[1] т. е. как минимум двух

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 $a = (a_1, a_2, \dots, a_m) \in K_1 \times K_2 \times \dots \times K_m$ обратим тогда и только тогда, когда 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. Гомомрфизмы. Отображение абелевых групп $\varphi : A \to B$ называется *гомоморфизмом*, если для любой пары элементов $a_1, a_2 \in A$ в 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 2.13. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

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

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

показывают, что $\varphi(-a) = -\varphi(a)$. Таким образом, образ $\operatorname{im}\varphi = \varphi(A) \subset B$ любого гомоморфизма $\varphi : A \to B$ является абелевой подгруппой в B.

2.6.1. Ядро гомоморфизма. Полный прообраз нулевого элемента 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, т. к. 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 $\varphi : A \to B$ над произвольной точкой $b \in B$ либо пуст, либо равен $\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$, где $a \in A$ — какой-нибудь элемент, переходящий в b. В частности, 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, если и только если $a_1 - a_2 \in \ker(\varphi)$. □

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:

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

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 $\varphi : A \to B$ называется *гомоморфизмом колец*, если для любой пары элементов $a_1, a_2 \in A$ в 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 $\varphi : A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми перечисленными выше свойствами гомоморфизмов абелевых групп: $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, и все непустые слои φ представляют собою сдвиги слоя над нулём: если $\varphi(a) = b$, то

$$\varphi^{-1}(b) = a + \ker \varphi = \{a + a' \mid a' \in \ker \varphi\}$$

(в частности, φ инъективен тогда и только тогда, когда $\ker \varphi = \{0\}$).

Ядро гомоморфизма колец $\varphi : A \to B$ 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, $\ker \varphi$ является подкольцом в A.

Образ гомоморфизма колец $\varphi : A \to B$, очевидно, является подкольцом в B. Вообще говоря, он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$. Например, отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[z]_2 \mapsto [3z]_6$, является гомоморфизмом колец и посылает

$$[0]_2 \mapsto [0]_6 \qquad \text{и} \qquad [1]_2 \mapsto [3]_6 .$$

Предложение 2.2
Любой ненулевой гомоморфизм произвольного кольца с единицей в целостное кольцо переводит единицу в единицу.

Доказательство. Так как $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, мы имеем равенство $\varphi(1)(\varphi(1) - 1) = 0$, которое в целостном кольце возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\forall\, a \in A \;\; \varphi(a) = \varphi(1 \cdot a) = \varphi(1)\varphi(a) = 0$. □

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 ненулевых b.

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 $\forall\, b \in A$

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

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

2.7. Китайская теорема об остатках. Пусть числа $n_1, n_2, \dots, n_m \in \mathbb{Z}$ попарно взаимно просты и $n = n_1 n_2 \cdots n_m$. Отображение

$$\begin{aligned} \varphi : \mathbb{Z}/(n) &\to \left(\mathbb{Z}/(n_1)\right) \times \left(\mathbb{Z}/(n_2)\right) \times \cdots \times \left(\mathbb{Z}/(n_m)\right) \\ [z]_n &\mapsto \left([z]_{n_1}, [z]_{n_2}, \dots, [z]_{n_m}\right) , \end{aligned} \tag{2-25}$$

сопоставляющее вычету $z \pmod n$ набор вычетов $z_i \pmod{n_i}$, является корректно определённым гомоморфизмом колец. Действительно, при выборе различных представителей $z_1 \equiv z_2 \pmod n$ их разность $z_1 - z_2$ делится на $n = n_1 n_2 \cdots n_m$, а значит, и на каждое n_i, так что $[z_1]_{n_i} = [z_2]_{n_i}$ при всех i. Равенства

$$\begin{aligned}\varphi\big([z]_n + [w]_n\big) = \varphi\big([z+w]_n\big) = \big([z+w]_{n_1}, [z+w]_{n_2}, \dots, [z+w]_{n_m}\big) = \\ = \big([z]_{n_1} + [w]_{n_1}, [z]_{n_2} + [w]_{n_2}, \dots, [z]_{n_m} + [w]_{n_m}\big) = \\ = \big([z]_{n_1}, [z]_{n_2}, \dots, [z]_{n_m}\big) + \big([w]_{n_1}, [w]_{n_2}, \dots, [w]_{n_m}\big) = \varphi\big([z]_n\big) + \varphi\big([w]_n\big)\end{aligned}$$

показывают, что φ перестановочен со сложением. Перестановочность φ с умножением проверяется дословно такой же выкладкой.

Легко видеть, что $\ker \varphi = 0$: если вычет $[z]_n$ таков, что все вычеты $[z]_{n_i} = 0$, то z делится на каждое n_i, а значит, по лем. 2.3, и на их произведение $n = n_1 n_2 \dots n_m$, откуда $[z]_n = 0$. Поскольку гомоморфизм с нулевым ядром инъективен по предл. 2.1 и оба кольца $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ состоят из одинакового числа элементов $n = \prod n_i$, отображение (2-25) биективно.

Этот факт известен как *китайская теорема об остатках*. На житейском языке он означает, что для любого набора остатков $r_1, r_2, \dots, r_m$ от деления на попарно взаимно простые числа $n_1, n_2, \dots, n_m$ всегда найдётся целое число z, которое даёт остаток r_i от деления n_i *сразу для всех* i, причём любые два таких числа z_1, z_2 различаются на целое кратное числа $n = n_1 n_2 \cdots n_k$. Для практического отыскания z полезно установить сюрьективность гомоморфизма φ непосредственно, не прибегая к предл. 2.1.

Из взаимной простоты числа n_i с остальными n_ν вытекает, что n_i взаимно просто с их произведением $m_i = \prod_{\nu \neq i} n_\nu$ (см. лем. 2.3). 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 $\nu \neq i$. Поэтому число $z = r_1 b_1 + r_2 b_2 + \dots + r_m b_m$ решает задачу.

Для демонстрации эффективности этого алгоритма найдём, к примеру, 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. Так как $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, для этого достаточно применить алгоритм Евклида к $E_0 = 57$ и $E_1 = 13$. В результате получим $22 \cdot 13 - 5 \cdot 57 = 1$, откуда $-22 \cdot 91 \cdot 179 \equiv 1 \pmod{57}$. Число

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

даёт при делении на 57, 91 и 179 остатки $(1, 0, 0)$. Аналогичным образом 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

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

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. Простое подполе и характеристика. Для любого кольца с единицей K имеется канонический гомоморфизм $\varkappa : \mathbb{Z} \to K$, заданный правилом

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

Если гомоморфизм $\varkappa$ инъективен, то говорят, что кольцо K имеет *характеристику нуль*. В противном случае *характеристикой* называют наименьшее $m \in \mathbb{N}$, для которого

$$\underbrace{1 + 1 + \dots + 1}_{m} = 0 .$$

Характеристика кольца K обозначается через $\mathrm{char}(K)$.

Предложение 2.4
Характеристика целостного кольца либо равна нулю либо является простым числом.

Доказательство. При $m, n > 1$ левая часть равенства

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

обращается в нуль только тогда, когда зануляется один из сосстоящих из меньшего числа единиц сомножителей в правой части. □

2.8.1. Простое подполе. Пусть $K = \mathbb{F}$ является полем. Наименьшее по включению подполе в $\mathbb{F}$, содержащее 1 и 0, называется *простым подполем* в $\mathbb{F}$. В силу своего определения простое подполе содержит образ $\mathrm{im}\,(\varkappa)$ гомоморфизма (2-26).

Если $\mathrm{char}(\mathbb{F}) = p > 0$, простое подполе совпадает с $\mathrm{im}\,(\varkappa)$ и изоморфно полю $\mathbb{F}_p$. Действительно, в этом случае отображение $\mathbb{Z}/(p) \to \mathbb{F}$, переводящее $a \pmod p$ в $\varkappa(a)$, корректно определено и является гомоморфизмом, а его образ, очевидно, содержится в образе $\varkappa$, а тем самым и в простом подполе. По предл. 2.3 этот гомоморфизм инъективен, а значит его образ является полем. Стало быть, он и есть простое подполем.

Если $\mathrm{char}(\mathbb{F}) = 0$, то гомоморфизм $\varkappa$ вкладывает $\mathbb{Z}$ в $\mathbb{F}$. Простое подполе содержит обратные элементы ко всем элементам из $\mathrm{im}\,\varkappa$. Поэтому правило $p/q \mapsto \varkappa(p)/\varkappa(q)$ продолжает $\varkappa$ до вложения полей $\varkappa : \mathbb{Q} \hookrightarrow \mathbb{F}$, образ которого лежит в простом подполе, а значит, совпадает с ним. Тем самым, простое подполе поля характеристики нуль изоморфно полю рациональных чисел $\mathbb{Q}$.

Упражнение 2.14. Покажите, что любой автоморфизм поля оставляет на месте каждый элемент из его простого подполя.

Отметим, что из этого упражнения вытекает, что поле $\mathbb{Q}$ остаётся неподвижным при любом автоморфизме полей $\mathbb{R}$ и $\mathbb{C}$.

Упражнение 2.15. Покажите, что между полями разной характеристики нет никаких ненулевых гомоморфизмов.

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

$$F_p : \mathbb{F} \to \mathbb{F}, \quad x \mapsto x^p, \tag{2-27}$$

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

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

(см. прим. 2.6 и лем. 2.4 на стр. 22). Гомоморфизм (2-27) называется *гомоморфизмом Фробениуса*. В силу малой теоремы Ферма[1], он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$.

[1]см. сл. 2.1 на стр. 22

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. 16 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, которые в свою очередь или неприводимы или являются произведениями 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, найдётся q_i (можно считать, что q_1) который делится на p_1. Поскольку q_1 прост, $q_1=\pm p_1$. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.10. 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. 22, получаем

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

Упр. 2.14. Любой автоморфизм $\varphi:\mathbb{F}\to\mathbb{F}$ оставляет на месте каждый элемент из $\operatorname{im}\varkappa$, т. к.

$$\varphi(\underbrace{1+\cdots+1}_{p})=\underbrace{1+\cdots+1}_{p},$$

а простое подполе либо совпадает с $\operatorname{im}\varkappa$, либо состоит из элементов a/b с $a,b\in\operatorname{im}\varkappa$.

Упр. 2.15. Пусть $\operatorname{char}(\mathbb{F})=p$ и $\operatorname{char}(\Bbbk)=q$. При $q\neq p$ элемент $\underbrace{1+\cdots+1}_{p}\in\Bbbk$ отличен от нуля, но переводится в нуль любым гомоморфизмом $\varphi:\Bbbk\to\mathbb{F}$. Тем самым, φ не инъективен и по предл. 2.3 должен быть нулевым.