А. Л. Городенцев*

А Л Г Е Б Р А

1-й курс

Факультет математики НИУ ВШЭ
2022/23 уч. год

* ВШЭ, ИТЭФ, НМУ, e-mail:gorod@itep.ru , http://gorod.bogomolov-lab.ru/

Оглавление

О множествах и отображениях

В этом разделе собраны некоторые факты о множествах и отображениях, которые будут использоваться в нашем курсе. Я надеюсь, что многие их них знакомы читателю из школы, ну а те, что не знакомы, будут в самое ближайшее время изучены в параллельном нашему курсе теории множеств и топологии. Нет нужды «учить» данный раздел *перед* тем, как браться за курс алгебры. Но к нему стоит выборочно обращаться всякий раз, когда Вы почувствуете себя неуверенно в тех или иных рассуждениях, использующих множества, отображения и отношения или незнакомую Вам комбинаторику.

0.1. Множества. В наши цели не входит построение логически строгой теории множеств. Для понимания этого курса достаточно школьного интуитивного представления о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множеств мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

Множество X задано, как только про любой объект можно сказать, является он элементом множества X или нет. Принадлежность точки x множеству X записывается как $x \in X$. Два множества *равны*, если они состоят из одних и тех же элементов. Существует единственное множество, не содержащее ни одного элемента. Оно называется *пустым* и обозначается $\varnothing$. Если множество X конечно, то мы обозначаем через $|X|$ количество точек в нём.

Множество X называется *подмножеством* множества Y, если каждый его элемент $x \in X$ лежит также и в Y. В этом случае пишут $X \subset Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Подмножества, отличные от всего множества, называются *собственными*. В частности, пустое подмножество собственное. Если надо указать, что X является собственным подмножеством в Y используется обозначение $X \subsetneq Y$.

Упражнение 0.1. Сколько всего подмножеств (включая пустое и несобственное) имеется у множества, состоящего из n элементов?

Для заданных множеств X, Y их *объединение* $X \cup Y$ состоит из всех элементов, принадлежащих хотя бы одному из множеств X, Y; *пересечение* $X \cap Y$ состоит из всех элементов, принадлежащих одновременно каждому из множеств X, Y; *разность* $X \smallsetminus Y$ состоит из всех элементов множества X, которые не содержатся в Y.

Упражнение 0.2. Проверьте, что операция пересечения выражается через разность по формуле $X \cap Y = X \smallsetminus (X \smallsetminus Y)$. Можно ли выразить разность через пересечение и объединение?

Если множество X является объединением непересекающихся подмножеств Y и Z, то говорят, что X является *дизъюнктным объединением* Y и Z и пишут $X = Y \sqcup Z$.

Множество $X \times Y$, элементами которого являются, по определению, всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

0.2. Отображения. Отображение $f : X \to Y$ из множества X в множество Y есть правило, однозначно сопоставляющее каждой точке $x \in X$ некоторую точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f. Множество всех таких точек $x \in X$, образ которых равен заданной точке $y \in Y$, называется *полным прообразом* точки y (или *слоем* отображения f над y) и обозначается

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}\,.$$

Полные прообразы различных точек не пересекаются и могут быть как пустыми, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, называется *образом отображения* $f : X \to Y$ и обозначается

$$\mathrm{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \varnothing\} = \{y \in Y \mid \exists\, x \in X : f(x) = y\}\,.$$

Два отображения $f : X \to Y$ и $g : X \to Y$ *равны*, если $f(x) = g(x)$ для всех $x \in X$. Множество всех отображений из множества X в множество Y обозначается $\mathrm{Hom}(X, Y)$.

Отображение $f : X \to Y$ называется *наложением* (а также *сюрьекцией* или *эпиморфизмом*), если $\mathrm{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюрьективные отображения стрелками $X \twoheadrightarrow Y$. Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$, т. е. когда прообраз каждой точки $y \in Y$ содержит не более одного элемента. Инъективные отображения изображаются стрелками $X \hookrightarrow Y$.

Упражнение 0.3. Перечислите все отображения $\{0, 1, 2\} \to \{0, 1\}$ и $\{0, 1\} \to \{0, 1, 2\}$. Сколько среди них вложений и сколько наложений?

Отображение $f : X \to Y$, которое является одновременно и вложением и наложением, называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*). Биективность отображения f означает, что для каждого $y \in Y$ существует единственный $x \in X$, такой что $f(x) = y$. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$.

Упражнение 0.4. Из отображений: а) $\mathbb{N} \to \mathbb{N} : x \mapsto x^2$ б) $\mathbb{Z} \to \mathbb{Z} : x \mapsto x^2$ в) $\mathbb{Z} \to \mathbb{Z} : x \mapsto 7x$ г) $\mathbb{Q} \to \mathbb{Q} : x \mapsto 7x$ выделите все инъекции, все сюрьекции и все биекции.

Отображения $X \to X$ из множества X в себя обычно называют *эндоморфизмами* множества X. Множество всех эндоморфизмов обозначается $\mathrm{End}(X) \stackrel{\text{def}}{=} \mathrm{Hom}(X, X)$.

Упражнение 0.5 (принцип Дирихле). Покажите, что следующие три условия на множество X равносильны: а) X бесконечно б) существует вложение $X \hookrightarrow X$, не являющееся наложением в) существует наложение $X \twoheadrightarrow X$, не являющееся вложением.

Взаимно однозначные эндоморфизмы $X \xrightarrow{\sim} X$ называются *автоморфизмами* X. Множество всех автоморфизмов обозначается через $\mathrm{Aut}(X)$. Автоморфизмы можно воспринимать как *перестановки* элементов множества X. У всякого множества X имеется *тождественный автоморфизм* $\mathrm{Id}_X : X \to X$, который переводит каждый элемент в самого себя: $\forall\, x \in X\ \mathrm{Id}_X(x) = x$.

Упражнение 0.6. Счётно[1] ли множество $\mathrm{Aut}(\mathbb{N})$?

[1] Множество M называется *счётным* если существует биекция $\mathbb{N} \xrightarrow{\sim} M$.

Пример 0.1 (запись отображений словами)
Рассмотрим множества $X = \{1, 2, \dots, n\}$ и $Y = \{1, 2, \dots, m\}$, сопоставим каждому отображению $f : X \to Y$ последовательность его значений:

$$w(f) \overset{\text{def}}{=} \big(f(x_1), f(x_2), \dots, f(x_n)\big) \tag{0-1}$$

и будем воспринимать её как n-буквенное слово, написанное при помощи m-буквенного алфавита Y. Так, отображениям $f : \{1, 2\} \to \{1, 2, 3\}$ и $g : \{1, 2, 3\} \to \{1, 2, 3\}$, действующим по правилам $f(1) = 3$, $f(2) = 2$ и $g(1) = 1$, $g(2) = 2$, $g(3) = 2$, сопоставятся слова $w(f) = (3, 2)$ и $w(g) = (1, 2, 2)$, составленные из букв алфавита $\{1, 2, 3\}$. Запись отображения словом задаёт биекцию

$$w : \operatorname{Hom}(X, Y) ⥲ \{\text{слова из } |X| \text{ букв в алфавите } Y\}, \quad f \mapsto w(f). \tag{0-2}$$

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюрьективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых каждая буква алфавита Y встречается ровно один раз.

0.3. Слои отображений. Задание отображения $f : X \to Y$ равносильно указанию подмножества $\operatorname{im}(f) \subset Y$ и разбиению множества X в дизъюнктное объединение непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \operatorname{im}(f)$:

$$X = \bigsqcup_{y \in \operatorname{im}(f)} f^{-1}(y). \tag{0-3}$$

Такой взгляд на отображения часто оказывается полезным при подсчёте количества элементов в том или ином множестве. Например, когда все непустые слои отображения $f : X \to Y$ состоят из одного и того же числа точек $m = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X соотношением

$$|X| = m \cdot |\operatorname{im} f|, \tag{0-4}$$

которое при всей своей простоте имеет много разнообразных применений.

Предложение 0.1
Если множества X и Y конечны, то $|\operatorname{Hom}(X, Y)| = |Y|^{|X|}$.

Доказательство. Зафиксируем какую-нибудь точку $x \in X$ и рассмотрим *отображение вычисления*[1]

$$\operatorname{ev}_x : \operatorname{Hom}(X, Y) \to Y, \quad f \mapsto f(x), \tag{0-5}$$

сопоставляющее каждому отображению $f : X \to Y$ его значение в точке x. Его слой $\operatorname{ev}_x^{-1}(y)$ над точкой $y \in Y$ состоит из всех отображений $f : X \to Y$, у которых $f(x) = y$. Сопоставляя такому отображению f его ограничение на подмножество $X \smallsetminus \{x\}$, мы

[1] Обозначение «ev» является сокращением слова *evaluation*.

получаем биекцию $\mathrm{ev}_x^{-1}(y) \xrightarrow{\sim} \mathrm{Hom}(X \smallsetminus \{x\}, Y)$. Таким образом, все слои отображения (0-5) состоят из одинакового числа элементов, равного количеству всех отображений из $(n-1)$-элементного множества $X \smallsetminus \{x\}$ в Y. По формуле (0-4) $|\mathrm{Hom}(X,Y)| = |\mathrm{Hom}(X \smallsetminus \{x\}, Y)| \cdot |Y|$, т. е. при добавлении к X одной точки число отображений $X \to Y$ увеличивается в $|Y|$ раз. □

Замечание 0.1. В виду предл. 0.1 множество $\mathrm{Hom}(X,Y)$ всех отображений $X \to Y$ часто обозначают через Y^X. В терминах прим. 0.1 отображение $X \to Y$ представляет собою слово, в котором места расположения букв отвечают точкам множества X, а сами буквы независимо выбираются из алфавита Y. Отображение вычисления ev_x сопоставляет слову его x-ю букву.

Замечание 0.2. В доказательстве предл. 0.1 мы молчаливо предполагали, что оба множества непусты. Если $X = \varnothing$, то для любого множества Y множество $\mathrm{Hom}(\varnothing, Y)$ по определению состоит из единственного элемента — вложения $\varnothing$ в Y в качестве пустого подмножества или, что то же самое, пустого слова в алфавите Y. Вычисление (0-5) в этом случае не определено, но предл. 0.1 остаётся в силе: $1 = |Y|^0$. В частности, $\mathrm{Hom}(\varnothing,\varnothing)$ тоже состоит из одного элемента[1] — тождественного автоморфизма $\mathrm{Id}_\varnothing$. Если $Y = \varnothing$, а $X \neq \varnothing$, то $\mathrm{Hom}(X,\varnothing) = \varnothing$, что тоже согласуется с предл. 0.1: $0^{|X|} = 0$ при $|X| > 0$.

Предложение 0.2
Если $|X| = n$, то $|\mathrm{Aut}(X)| = n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 1$.

Доказательство. Положим $Y = X$ в доказательстве предл. 0.1 и ограничим отображение вычисления (0-5) на подмножество биекций $\mathrm{Aut}(X) \subset \mathrm{Hom}(X,X)$. Получим отображение $\mathrm{ev}_x : \mathrm{Aut}(X) \to X$, $f \mapsto f(x)$, слой которого $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X$ состоит из всех биекций $X \xrightarrow{\sim} X$, переводящих x в x'.

Упражнение 0.7. Постройте взаимно однозначное отображение между биекциями $X \xrightarrow{\sim} X$, переводящими x в x', и биекциями $X \xrightarrow{\sim} X$, оставляющими точку x на месте.

Таким образом, слои $\mathrm{ev}_x^{-1}(x')$ над всеми точками $x' \in X$ непусты и состоят из одного и того же числа элементов, равного количеству автоморфизмов $(n-1)$-элементного множества $X \smallsetminus \{x\}$. По формуле (0-4), $|\mathrm{Aut}(X)| = |\mathrm{Aut}(X \smallsetminus \{x\})| \cdot |X|$, т. е. при добавлении n-той точки к $(n-1)$-элементному множеству количество автоморфизмов увеличивается в n раз. Поэтому $|\mathrm{Aut}(X)| = n \cdot (n-1) \cdot \ldots \cdot 1 = n!$. □

Замечание 0.3. Число $n! = n \cdot (n-1) \cdot \ldots \cdot 1$ называется *n-факториал*. Так как $|\mathrm{Aut}(\varnothing)| = |\{\mathrm{Id}_\varnothing\}| = 1$, мы полагаем $0! \stackrel{\text{def}}{=} 1$.

Замечание 0.4. В терминах прим. 0.1 автоморфизм n-элементного множества X представляет собою n-буквенное слово без повторяющихся букв в алфавите X, т. е. перестановку элементов множества X, и предл. 0.2 утверждает, что имеется ровно $n!$ различных слов, которые можно получить, переставляя буквы в заданном n-буквенном слове без повторяющихся букв.

[1] Т. е. 0^0 в этом контексте считается равным 1.

Пример 0.2 (мультиномиальные коэффициенты)
При раскрытии скобок в выражении $(a_1 + \dots + a_m)^n$ получится сумма одночленов вида $a_1^{k_1} \cdots a_m^{k_m}$, где каждый показатель k_i заключён в пределах $0 \leqslant k_i \leqslant n$, а общая степень $k_1 + \dots + k_m = n$. Коэффициент, возникающий при таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{k_1 \dots k_m}$. Таким образом,

$$(a_1 + \dots + a_m)^n = \sum_{\substack{k_1+\dots+k_m=n \\ \forall i \; 0\leqslant k_i \leqslant n}} \binom{n}{k_1 \dots k_m} \cdot a_1^{k_1} \cdots a_m^{k_m}, \tag{0-6}$$

Чтобы явно выразить $\binom{n}{k_1 \dots k_m}$ через $k_1, \dots, k_m$, заметим, что раскрытие n скобок

$$(a_1 + \dots + a_m)(a_1 + \dots + a_m) \dots (a_1 + \dots + a_m)$$

заключается в выборе внутри каждой из скобок какой-нибудь одной буквы и выписывании их слева направо друг за другом в одно n-буквенное слово. Это надо сделать всеми возможными способами и сложить все полученные слова. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$, суть слова, состоящие ровно из k_1 букв a_1, k_2 букв a_2, … , k_m букв a_m. Количество таких слов легко подсчитать по формуле (0-4). А именно, сделаем на время k_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с k_2 буквами a_2, k_3 буквами a_3 и т. д. В результате получим $n = k_1 + \dots + k_m$ попарно разных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \dots, a_1^{(k_1)}}_{k_1 \text{ меченых букв } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \dots, a_2^{(k_2)}}_{k_2 \text{ меченых букв } a_2}, \dots \dots \dots, \underbrace{a_m^{(1)}, a_m^{(2)}, \dots, a_m^{(k_m)}}_{k_m \text{ меченых букв } a_m}.$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n различными буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, $|X| = n!$. В качестве Y возьмём интересующее нас множество слов из k_1 одинаковых букв a_1, k_2 одинаковых букв a_2, и т. д. и рассмотрим отображение $f : X \to Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1! \cdot k_2! \cdot \,\cdots\, \cdot k_m!$ слов, которые получаются из y всевозможными расстановками k_1 верхних индексов у букв a_1, k_2 верхних индексов у букв a_2, и т. д. По формуле (0-4)

$$\binom{n}{k_1 \dots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \,\cdots\, \cdot k_m!}. \tag{0-7}$$

Тем самым, разложение (0-6) имеет вид

$$(a_1 + \dots + a_m)^n = \sum_{\substack{k_1+\dots+k_m=n \\ \forall i \; 0\leqslant k_i \leqslant n}} \frac{n! \cdot a_1^{k_1} \dots a_m^{k_m}}{k_1! \cdot \dots \cdot k_m!}. \tag{0-8}$$

Упражнение 0.8. Сколько всего слагаемых в правой части формулы (0-8) ?

В частности, при $m = 2$ мы получаем известную формулу для раскрытия бинома с натуральным показателем[1]:

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}\, a^k b^{n-k}\,. \tag{0-9}$$

При $m = 2$ мультиномиальный коэффициент $\binom{n}{k,n-k}$ принято обозначать $\binom{n}{k}$ или C_n^k и называть k-тым *биномиальным коэффициентом* степени n или *числом сочетаний* из n по k. Он равен

$$\binom{n}{k} = C_n^k = \frac{n\cdot(n-1)\cdot\,\cdots\,\cdot(n-k+1)}{k\cdot(k-1)\cdot\,\cdots\,\cdot 1}$$

(сверху и снизу стоит по k последовательно убывающих сомножителей).

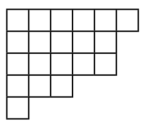
Пример 0.3 (диаграммы Юнга)
Разбиение конечного множества $X = \{1, 2, \dots, n\}$ в объединение непересекающихся подмножеств

$$X = X_1 \sqcup X_2 \sqcup \dots \sqcup X_k \tag{0-10}$$

можно кодировать следующим образом. Занумеруем подмножества в порядке нестрогого убывания их размера и обозначим количество элементов в i-том подмножестве через $\lambda_i = |X_i|$. Получим невозрастающую последовательность чисел

$$\lambda = (\lambda_1, \dots, \lambda_k)\,, \quad \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k\,,$$

которая называется *формой* разбиения (0-10). Форму разбиения удобно изображать *диаграммой Юнга* — картинкой вида



, (0-11)

составленной из выровненных по левому краю горизонтальных клетчатых полосок, занумерованных сверху вниз, так что в i-той сверху полоске λ_i клеток. Общее число клеток в диаграмме λ называется её *весом* и обозначается $|\lambda|$, а количество строк называется *длиной* и обозначается $\ell(\lambda)$. Так, диаграмма Юнга (0-11) отвечает разбиению формы $\lambda = (6, 5, 5, 3, 1)$, имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 0.9. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток (включая пустую диаграмму и сам прямоугольник).

Будем называть *заполнением* диаграммы λ множеством X из $|X| = |\lambda|$ элементов произвольную расстановку этих элементов в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всякая диаграмма λ веса n имеет $n!$ различных заполнений заданным n-элементным множеством X.

[1] Это частный случай *формулы Ньютона*, которую в полной общности мы обсудим чуть позже, когда будем заниматься степенными рядами.

Объединяя элементы, стоящие в i-той строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств $X_1, \dots, X_k$. Поскольку любое разбиение (0-10) заданной формы λ можно получить таким образом, возникает сюрьективное отображение из множества заполнений диаграммы λ в множество разбиений множества X формы λ. Покажем, что все слои этого отображения состоят из одного и того же числа элементов. Два заполнения приводят к одинаковым разбиениям тогда и только тогда, когда они получаются друг из друга перестановками элементов внутри строк и перестановками строк одинаковой длины между собою как единого целого. Если обозначить через $m_i = m_i(\lambda)$ число строк длины[1] i в диаграмме λ, то перестановок первого типа будет $\prod \lambda_i! = \prod\limits_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod\limits_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod\limits_{i=1}^{n} (i!)^{m_i} m_i!$ элементов. Из формулы (0-4) вытекает

Предложение 0.3
Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, … , m_n n-элементных подмножеств равно

$$\frac{n!}{\prod\limits_{i=1}^{n} m_i! \cdot (i!)^{m_i}} . \tag{0-12}$$

0.4. Классы эквивалентности. Альтернативный способ разбить заданное множество X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так. Назовём *бинарным отношением* на множестве X любое подмножество

$$R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\} .$$

Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$.

Например, на множестве целых чисел $X = \mathbb{Z}$ имеются бинарные отношения

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{0-13}$$

$$\text{неравенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{0-14}$$

$$\text{делимость} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 | x_2 \tag{0-15}$$

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \pmod{n} \tag{0-16}$$

[1] Отметим, что многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \cdots + nm_n$

(последнее условие $x_1 \equiv x_2 \pmod n$ читается как «x_1 сравнимо с x_2 по модулю n» и по определению означает, что $x_1 - x_2$ делится на n).

Определение 0.1

Бинарное отношение $\underset{R}{\sim}$ называется *эквивалентностью*, если оно обладает следующими тремя свойствами:

$$\begin{aligned}
\textit{рефлексивность}: &\quad \forall\, x \in X \; x \underset{R}{\sim} x \\
\textit{транзитивность}: &\quad \forall\, x_1, x_2, x_3 \in X \text{ из } x_1 \underset{R}{\sim} x_2 \text{ и } x_2 \underset{R}{\sim} x_3 \text{ вытекает } x_1 \underset{R}{\sim} x_3 \\
\textit{симметричность}: &\quad \forall\, x_1, x_2 \in X \; x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1 .
\end{aligned}$$

Среди бинарных отношений (0-13) – (0-16) первое и последнее являются эквивалентностями, а (0-14) и (0-15) не являются (они не симметричны).

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $x_1 \sim x_2$, означающее, что x_1 и x_2 лежат в одном и том же подмножестве этого разбиения, очевидно, является эквивалентностью.

Наоборот, пусть на множестве X задано отношение эквивалентности R. Рассмотрим для каждого $x \in X$ подмножество в X, состоящее из всех элементов, эквивалентных x. Оно называется *классом эквивалентности* элемента x и обозначается

$$[x]_R = \{z \in X \mid x \underset{R}{\sim} z\} = \{z \in X \mid z \underset{R}{\sim} x\}$$

(второе равенство выполняется благодаря симметричности отношения R). Любые два класса $[x]_R$ и $[y]_R$ либо вообще не пересекаются, либо полностью совпадают. В самом деле, если существует элемент z, эквивалентный и x и y, то в силу симметричности и транзитивности отношения $\underset{R}{\sim}$ элементы x и y будут эквивалентны между собой, а значит, любой элемент, эквивалентный x, будет эквивалентен также и y, и наоборот. Таким образом, множество X распадается в дизъюнктное объединение различных классов эквивалентности.

Множество классов эквивалентности по отношению $R \subset X \times X$ обозначается X/R и называется *фактором* множества X по эквивалентности R. Сюрьекия

$$f : X \twoheadrightarrow X/R, \quad x \mapsto [x]_R, \tag{0-17}$$

сопоставляющая каждому элементу $x \in X$ его класс эквивалентности $[x]_R \in X/R$, называется *отображением факторизации*. Слои этого отображения суть классы эквивалентных элементов. Наоборот, любое сюрьективное отображение $f : X \twoheadrightarrow Y$ является отображением факторизации по отношению эквивалентности $x_1 \sim x_2$, означающему, что $f(x_1) = f(x_2)$.

Пример 0.4 (классы вычетов)

Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (0-16) обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и опускать индекс n, когда понятно чему он равен. Класс эквивалентности

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z - x) \mathrel{\vdots} n\} \tag{0-18}$$

называется *классом вычетов по модулю* n. Отображение факторизации

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)\,, \quad z \mapsto [z]_n$$

называется *приведением по модулю* n. Множество $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n\,,\ [1]_n\,,\ \dots\,,\ [n-1]_n\,.$$

При желании их можно воспринимать как остатки от деления на n, но в практических вычислениях удобнее работать с ними именно как с *подмножествами* в $\mathbb{Z}$, поскольку возможность по-разному записывать один и тот же класс часто упрощает вычисления. Например, остаток от деления 12^{100} на 13 можно искать как

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}\,. \tag{0-19}$$

Упражнение 0.10. Докажите правомочность этого вычисления: проверьте, что классы вычетов $[x+y]_n$ и $[xy]_n$ не зависят от выбора чисел $x \in [x]_n$ и $y \in [y]_n$, т. е. правила

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{0-20}$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \tag{0-21}$$

корректно определяют на множестве $\mathbb{Z}/(n)$ операции сложения и умножения[1].

0.4.1. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap_\nu R_\nu \subset X \times X$ также является отношением эквивалентности. В самом деле, если каждое из множеств $R_\nu \subset X \times X$ содержит диагональ

$$\Delta = \{(x,x) \mid x \in X\} \subset X \times X\,,$$

переходит в себя при симметрии $(x,y) \leftrightarrows (y,x)$ и вместе с каждой парой точек вида (x,y), (y,z) содержит также и точку (x,z), то этими свойствами обладает и пересечение $\bigcap_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества $R \subset X \times X$ существует *наименьшее по включению* отношение эквивалентности $\overline{R}$, содержащее R, а именно, пересечение всех содержащих R отношений эквивалентности. Отношение $\overline{R}$ называется эквивалентностью, *порождённой* отношением R.

Упражнение 0.11. Проверьте, что $(x,y) \in \overline{R}$ если и только если в X существует такая конечная последовательность точек $x = z_0,\ z_1,\ z_2,\ \dots\ ,\ z_n = y$, что $(x_{i-1}, x_i) \in R$ или $(x_i, x_{i-1}) \in R$ при каждом $i = 1, 2, \dots, n$.

К сожалению, по данному подмножеству $R \subset X \times X$ не всегда легко судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу может быть не просто.

[1] Именно такое умножение $[12]^{100} = \underbrace{[12] \cdot [12] \cdot\ \cdots\ \cdot [12]}_{100} = \left[12^{100}\right]$ было использовано в (0-19).

Пример 0.5 (дроби)
Множество рациональных чисел $\mathbb{Q}$ обычно определяют как множество дробей a/b с $a, b \in \mathbb{Z}$ и $b \neq 0$. При этом под *дробью* понимается класс эквивалентности упорядоченных пар (a, b), где $a \in \mathbb{Z}$, $b \in \mathbb{Z} \smallsetminus 0$, по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \quad \text{с произвольными } c \in \mathbb{Z} \smallsetminus \{0\}\,. \tag{0-22}$$

Отношения (0-22) выражают собою равенства дробей $a/b = (ac)/(bc)$, но сами по себе не образуют эквивалентности. Например, при $a_1 b_2 = a_2 b_1$ в двухшаговой цепочке отождествлений $(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$ самый левый и самый правый элементы могут не отождествляться напрямую по правилу (0-22), как, например, $3/6$ и $5/10$. Поэтому эквивалентность, порождённая отождествлениями (0-22), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{0-23}$$

Оказывается, что к этим отношениям больше уже ничего добавлять не надо.

Упражнение 0.12. Проверьте, что набор отношений (0-23) рефлексивен, симметричен и транзитивен.

Тем самым, он является минимальным отношением эквивалентности, содержащим все отождествления (0-22). Отметим, что если в отношениях (0-22) разрешить нулевые c, то все пары (a, b) окажутся эквивалентны паре $(0, 0)$.

0.5. Композиции отображений. Отображение $X \to Z$, получающееся в результате последовательного выполнения двух отображений $f : X \to Y$ и $g : Y \to Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf. Таким образом, композиция gf определена если и только если образ f содержится в множестве, на котором определено отображение g, и $gf : X \to Z\,,\ x \mapsto g(f(x))$.

Хотя композицию и принято записывать точно так же, как умножение чисел, единственным общим свойством этих операций является их *ассоциативность* или *сочетательный закон*: композиция трёх последовательных отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T\,,$$

как и произведение трёх чисел, не зависит от того, в каком порядке перемножаются последовательные пары элементов, т. е. $(hg)f = h(gf)$, если хотя бы одна из двух частей этого равенства определена. Действительно, в этом случае вторая часть тоже определена, и обе части действуют на каждую точку $x \in X$ по правилу $x \mapsto h(g(f(x)))$.

В остальном алгебраические свойства композиции весьма далеки от привычных свойств умножения чисел. Если композиция fg определена, то противоположная композиция gf часто бывает не определена. Даже если $f, g : X \to X$ являются эндоморфизмами одного и того же множества X, так что обе композиции fg и gf определены, равенство $fg = gf$ может не выполняться.

Упражнение 0.13. Рассмотрим на плоскости пару различных прямых ℓ_1, ℓ_2, пересекающихся в точке O, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. При каком условии на прямые выполняется равенство $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Общие множители тоже бывает нельзя сокращать, т. е. ни равенство $fg = fh$, ни равенство $gf = hf$, вообще говоря, не влекут равенства $g = h$.

Пример 0.6 (эндоморфизмы двухэлементного множества)
Двухэлементное множество $X = \{1, 2\}$ имеет ровно четыре эндоморфизма. Если кодировать отображение $f : X \to X$ двубуквенным словом $(f(1), f(2))$, как в прим. 0.1 на стр. 4, то эти четыре эндоморфизма запишутся словами $(1, 1)$, $(1, 2) = \mathrm{Id}_X$, $(2, 1)$ и $(2, 2)$. Все композиции между ними определены, и таблица композиций gf имеет вид:

$$\begin{array}{c|cccc} g\diagdown f & (1,1) & (1,2) & (2,1) & (2,2) \\ \hline (1,1) & (1,1) & (1,1) & (1,1) & (1,1) \\ (1,2) & (1,1) & (1,2) & (2,1) & (2,2) \\ (2,1) & (2,2) & (2,1) & (1,2) & (1,1) \\ (2,2) & (2,2) & (2,2) & (2,2) & (2,2) \end{array} \tag{0-24}$$

Обратите внимание на то, что $(2, 2)\circ(1, 1) \neq (1, 1)\circ(2, 2)$ и что $(1, 1)\circ(1, 2) = (1, 1)\circ(2, 1)$, хотя $(1, 2) \neq (2, 1)$, и $(1, 1) \circ (2, 2) = (2, 1) \circ (2, 2)$, хотя $(1, 1) \neq (2, 1)$.

Лемма 0.1 (левые обратные отображения)
Если $X \neq \varnothing$, то следующие условия на отображение $f : X \to Y$ эквивалентны:

1) f инъективно

2) существует такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$

3) для любых отображений $g_1, g_2 : Z \to X$ из равенства $fg_1 = fg_2$ вытекает равенство $g_1 = g_2$.

Доказательство. Импликация (1) ⇒ (2): для точек $y = f(x) \in \operatorname{im} f$ положим $g(y) = x$, а в точках $y \notin \operatorname{im} f$ зададим g как угодно[1]. Импликация (2) ⇒ (3): если $fg_1 = fg_2$, то умножая обе части слева на любое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, получаем $g_1 = g_2$. Импликация (3) ⇒ (1) доказывается от противного. Пусть $x_1 \neq x_2$, но $f(x_1) = f(x_2)$. Положим $g_1 = \mathrm{Id}_X$, и пусть $g_2 : X \xrightarrow{\sim} X$ переставляет между собою точки x_1, x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$. □

Определение 0.2
Отображение $f : X \to Y$, удовлетворяющее лем. 0.1, называется *обратимым слева*, и любое отображение $g : Y \to X$, такое что $gf = \mathrm{Id}_X$, называется *левым обратным* к f.

Упражнение 0.14. В условиях лем. 0.1 убедитесь, что вложение f тогда и только тогда имеет несколько различных левых обратных, когда оно не сюрьективно.

[1] Например, отобразим их все в одну и ту же произвольно выбранную точку $x \in X$.

0.5.1. Правое обратное отображение и аксиома выбора. Желание гармонии требует «правой» версии лем. 0.1: хочется, чтобы следующие свойства отображения $f: X \to Y$ тоже были эквивалентны:

1) f сюрьективно
2) существует такое отображение $g: Y \to X$, что $fg = \mathrm{Id}_Y$
3) для любых отображений $g_1, g_2 : Y \to Z$ из равенства $g_1 f = g_2 f$ вытекает равенство $g_1 = g_2$.

Отображение f, удовлетворяющее свойству (2), называются *обратимым справа*, и всякое такое отображение $g: Y \to X$, что $fg = \mathrm{Id}_Y$, называется *правым обратным* к f или *сечением* эпиморфизма f. Второе название связано с тем, что отображение g, удовлетворяющее свойству (2), переводит каждую точку $y \in Y$ в точку $g(y) \in f^{-1}(y)$, лежащую в слое отображения f над точкой y. В строгой теории множеств, углубления в которую мы пытаемся избежать, импликация (1) ⇒ (2) постулируется в качестве одной из аксиом. Эта аксиома называется *аксиомой выбора* и утверждает, что в каждом слое любого сюрьективного отображения можно выбрать по элементу[1].

Итак, импликация (1) ⇒ (2) является частью строго определения понятия «множество». Доказательство импликации (2) ⇒ (3) полностью симметрично доказательству аналогичной импликации из лем. 0.1: применяя отображения, стоящие в обеих частях равенства $g_1 f = g_2 f$, вслед за таким отображением $g: Y \to X$, что $fg = \mathrm{Id}_Y$, получаем равенство $g_1 = g_2$. Импликация (3) ⇒ (1), как и в лем. 0.1, доказывается от противного: если $y \notin \operatorname{im} f$, то свойство (3) не выполняется для отображения $g_1 = \mathrm{Id}_Y$ и любого отображения $g_2 : Y \to Y$, переводящего точку y в какую-нибудь точку из $\operatorname{im} f$ и оставляющего на месте все остальные точки. Таким образом, перечисленные выше свойства (1) – (3) действительно эквивалентны друг другу.

0.5.2. Обратимые отображения. Если отображение $g: X \xrightarrow{\sim} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки. В этом случае правило $y \mapsto g^{-1}(y)$ определяет отображение $g^{-1}: Y \to X$, которое является одновременно и левым, и правым обратным к g в смысле опр. 0.2 и n° 0.5.1, т. е.

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X \tag{0-25}$$

Отображение g^{-1} называется *обратным* к биективному отображению g.

Предложение 0.4
Следующие условия на отображение $g: X \to Y$ эквивалентны друг другу:

1) g взаимно однозначно
2) существует такое отображение $g': Y \to X$, что[2] $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

[1] Иными словами, если имеется множество попарно непересекающихся множеств, то в каждом из них можно выбрать по элементу.
[2] Т. е. g' *двусторонне* обратно к g.

3) g обладает левым и правым обратными отображениями[1].

При выполнении этих условий все левые и правые обратные к g отображения равны друг другу и отображению g^{-1}, описанному перед формулировкой предложения.

Доказательство. Импликация (1) ⇒ (2) уже была установлена. Очевидно, что (2) ⇒ (3). Докажем, что (3) ⇒ (2). Если у отображения $g : X \to Y$ есть левое обратное $f : Y \to X$ и правое обратное $h : Y \to X$, то $f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h$ и условие (2) выполнено для $g' = f = h$. Остаётся показать, что (2) ⇒ (1), и $g' = g^{-1}$. Так как $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, поскольку для всех $x \in g^{-1}(y)$ выполнено равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$, прообраз $f^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, и $g' = g^{-1}$. □

0.6. Группы преобразований. Непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$. Если группа преобразований G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G. Если подмножество $H \subset G$ тоже является группой, то H называются *подгруппой* группы G.

Пример 0.7 (группы перестановок)
Множество $\mathrm{Aut}(X)$ всех взаимно однозначных отображений $X \to X$ является группой. Эта группа называется *симметрической группой* или *группой перестановок* множества X. Все прочие группы преобразований множества X являются подгруппами этой группы. Группа перестановок n-элементного множества $\{1, 2, \dots, n\}$ обозначается S_n и называется n-той *симметрической группой*. Согласно предл. 0.2 на стр. 6 порядок $|S_n| = n!$. Перестановки

$$\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$$

принято записывать строчками $\sigma = (\sigma_1, \dots, \sigma_n)$ их значений $\sigma_i \overset{\text{def}}{=} \sigma(i)$, как в прим. 0.1 на стр. 4. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ представляют собою отображения

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & & 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \text{и} & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 & & 2 & 3 & 4 & 1 \end{array}$$

а их композиции записываются как $\sigma\tau = (4, 2, 1, 3)$ и $\tau\sigma = (4, 1, 3, 2)$.

[1]Обратите внимание, что совпадения левого обратного отображения с правым обратным отображением не требуется.

Упражнение 0.15. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (0-24) на стр. 13.

Пример 0.8 (абелевы группы)
Группа G, в которой любые два элемента $f, g \in G$ перестановочны, т. е. удовлетворяют соотношению $fg = gf$, называется *коммутативной* или *абелевой*. Примерами абелевых групп являются группы параллельных переносов плоскости или пространства, а также группа SO_2 поворотов плоскости вокруг фиксированной точки. Для каждого натурального $n \geqslant 2$ повороты на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка n*.

0.7. Частично упорядоченные множества. Бинарное отношение[1] $x \leqslant y$ на множестве Z называется *частичным порядком*, если оно рефлексивно и транзитивно[2], но в отличие от эквивалентности не симметрично, а *кососимметрично*, т. е. из $x \leqslant y$ и $y \leqslant x$ вытекает равенство $x = y$. Если на множестве задан частичный порядок, мы пишем $x < y$, если $x \leqslant y$ и $x \neq y$. Частичный порядок на множестве Z называется *тотальным* (а также *линейным* или просто *порядком*), если любые два элемента сравнимы, т. е. для всех $x, y \in Z$ выполняется одно из трёх альтернативных условий: или $x < y$, или $x = y$, или $y < x$. Например, обычное неравенство между числами является линейным порядком на множестве натуральных чисел $\mathbb{N}$, тогда как отношение делимости $n \mid m$, означающее, что n делит m, задаёт на $\mathbb{N}$ частичный порядок, который не является линейным. Другим важным примером частичного, но не линейного порядка является отношение включения $X \subseteq Y$ на множестве $\mathcal{S}(M)$ всех подмножеств заданного множества M.

Упражнение 0.16 (предпорядок). *Предпорядком* на множестве Z называется любое рефлексивное транзитивное бинарное отношение $x \precsim y$. Убедитесь, что для каждого предпорядка бинарное отношение $x \sim y$, означающее, что одновременно $x \precsim y$ и $y \precsim x$, является отношением эквивалентности и что на факторе $Z/\!\sim$ бинарное отношение $[x] \leqslant [y]$, означающее, что $x \precsim y$, корректно определено[3] и является частичным порядком. Продумайте, как всё это работает для отношения делимости $n \mid m$ на множестве целых чисел $\mathbb{Z}$.

Множество P с зафиксированным на нём частичным порядком называется *частично упорядоченным множеством*, сокращённо — чумом. Если порядок на P тотальный, мы будем говорить, что чум P *линейно упорядочен*. Всякое подмножество X чума P также является чумом по отношению к частичному порядку, имеющемуся на P. Если этот индуцированный с P порядок на X оказывается линейным, подмножество $X \subset P$ называют *цепью* в чуме P. Элементы x, y чума P называются *сравнимыми*, если $x \leqslant y$ или $y \leqslant x$. Если же ни одно из этих условий не выполняется, то x и y называются *несравнимыми*. Несравнимые элементы автоматически различны. Частичный порядок линеен тогда и только тогда, когда любые два элемента сравнимы.

Отображение $f : M \to N$ между чумами M, N называется *сохраняющим порядок*[4]

[1] См. n° 0.4 на стр. 9.
[2] Так же, как и отношение эквивалентности, ср. с опр. 0.1 на стр. 10.
[3] Т. е. выполнение или невыполнение условия $x \precsim y$ не зависит от выбора представителей x и y в классах $[x]$ и $[y]$.
[4] А также *неубывающим* или *нестрого возрастающим*.

или *морфизмом* чумов, если для всех $x, y \in M$ соотношение $x \leqslant y$ влечёт соотношение $f(x) \leqslant f(y)$. Два чума M, N называются *изоморфными*, если имеется сохраняющая порядок биекция $M \xrightarrow{\sim} N$. В таком случае мы пишем $M \simeq N$. Отображение f называется *строго возрастающим*, если для всех $x, y \in M$ соотношение $x < y$ влечёт соотношение $f(x) < f(y)$. Всякое сохраняющее порядок вложение является строго возрастающим. Обратное справедливо для возрастающих отображений из линейного упорядоченного множества, однако неверно в общем случае.

Элемент y чума P называется *верхней гранью* подмножества $X \subset P$, если $x \leqslant y$ для всех $x \in X$. Если при этом $y \notin X$, то верхняя грань y называется *внешней*. В таком случае для всех $x \in X$ выполнено строгое неравенство $x < y$.

Элемент $m^* \in X$ называется *максимальным* в подмножестве $X \subset P$, если неравенство $m^* \leqslant x$ для $x \in X$ выполняется только при $x = m^*$. Заметьте, что максимальный элемент не обязан быть сравним со всеми элементами $x \in X$ и, тем самым, может не являться верхней гранью для X. Частично упорядоченное множество может иметь несколько различных максимальных элементов или не иметь их вовсе, как, например, чум $\mathbb{N}$ отношению к делимости или к обычному неравенству между числами. Линейно упорядоченный чум имеет не более одного максимального элемента, и если такой элемент существует, то он является верхней гранью.

Симметричным образом, элемент $m_* \in X$ называется *минимальным*, если неравенство $m_* \leqslant x$ выполняется только для $x = m_*$. Аналогично определяются и нижние грани, и всё сказанное выше о максимальных элементах и верхних гранях в равной степени относится и к минимальным элементам и нижним граням.

0.8. Вполне упорядоченные множества. Линейно упорядоченное множество W называется *вполне упорядоченным*, если каждое непустое подмножество $S \subset W$ содержит такой элемент $s_* \in S$, что $s_* \leqslant s$ для всех $s \in S$. Этот элемент автоматически единствен и называется *начальным элементом* подмножества S. Например, множество натуральных чисел $\mathbb{N}$ со стандартным отношением неравенства между числами вполне упорядочено, как и любое дизъюнктное объединение вида $\mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \ldots$, в котором все элементы каждой копии множества $\mathbb{N}$ полагаются строго большими всех элементов всех предыдущих копий. Пустое множество тоже вполне упорядочено. Напротив, множество $\mathbb{Q}$ со стандартным отношением неравенства между числами не является вполне упорядоченным.

Вполне упорядоченные множества замечательны тем, что их элементы можно рекурсивно перебрать точно так же, как и элементы множества $\mathbb{N}$. А именно, пусть некоторое утверждение $\Phi(w)$ зависит от элемента w вполне упорядоченного множества W. Если $\Phi(w)$ истинно для начального элемента w_* множества W, и для каждого $w \in W$ истинность утверждения $\Phi(x)$ при всех $x < w$ влечёт за собою истинность утверждения $\Phi(w)$, то $\Phi(w)$ истинно для всех $w \in W$.

Упражнение 0.17. Убедитесь в этом.

Такой способ доказательства утверждения $\Phi(w)$ для всех $w \in W$ называется *трансфинитной индукцией*. Используемые для индуктивного перехода подмножества, состоящие из всех элементов, предшествующих данному элементу w, называются *начальны-*

ми интервалами частично упорядоченного множества W и обозначаются

$$[w) \overset{\text{def}}{=} \{x \in W \mid x < w\}.$$

Элемент $w \in W$ называется *точной верхней гранью* начального интервала $[w) \subset W$ и однозначно восстанавливается по интервалу $[w)$ как начальный элемент множества $W \smallsetminus [w)$. Отметим, что начальный элемент $w_* \in W$ является точной верхней гранью пустого начального интервала $[w_*) = \varnothing$.

Упражнение 0.18. Покажите, что собственное подмножество $I \subsetneq W$ тогда и только тогда является начальным интервалом вполне упорядоченного множества W, когда $[x) \subset I$ для каждого $x \in I$, и в этом случае точная верхняя грань интервала I однозначно восстанавливается по I как начальный элемент дополнения $W \smallsetminus I$.

Между вполне упорядоченными множествами имеется отношение порядка $U \leqslant W$, означающее, что U изоморфно с сохранением порядка некоторому начальному интервалу $[w) \subset W$. Если при этом U и W не изоморфны, мы пишем $U < W$. Хорошим упражнением на трансфинитную индукцию является

Упражнение 0.19. Убедитесь, что для любой пары вполне упорядоченных множеств U, W выполнено ровно одно из соотношений: или $U < W$, или $U \simeq W$, или $W < U$.

Классы изоморфных вполне упорядоченных множеств называют *ординалами*. Множество $\mathbb{N}$ со стандартным порядком можно воспринимать как множество всех конечных ординалов. Все остальные ординалы, включая $\mathbb{N}$, называются *трансфинитными*.

0.9. Лемма Цорна. Рассмотрим произвольное частично упорядоченное множество P и обозначим через $\mathcal{W}(P)$ множество всех подмножеств $W \subset P$, которые вполне упорядочены имеющимся на P отношением $x \leqslant y$. Множество $\mathcal{W}(P)$ непусто и содержит пустое подмножество $\varnothing \subset P$, а также все конечные цепи[1] $C \subset P$ и, в частности, все элементы множества P.

Лемма 0.2
Не существует такого отображения $\varrho : \mathcal{W}(P) \to P$, что $\varrho(W) > w$ для всех $W \in \mathcal{W}(P)$ и $w \in W$.

Доказательство. Пусть такое отображение ϱ существует. Назовём вполне упорядоченное подмножество $W \subset P$ рекурсивным, если $\varrho([w)) = w$ для всех $w \in W$. Например, подмножество

$$\Big\{\varrho(\varnothing),\ \varrho\big(\{\varrho(\varnothing)\}\big),\ \varrho\Big(\big\{\varrho(\varnothing),\ \varrho(\{\varrho(\varnothing)\})\big\}\Big)\Big\}$$

рекурсивно и может неограниченно расширяться вправо. Любые два различных рекурсивных вполне упорядоченных подмножества с общим начальным элементом таковы, что одно из них является начальным интервалом другого.

Упражнение 0.20. Докажите это.

Обозначим через $U \subset P$ объединение всех рекурсивных вполне упорядоченных подмножеств в P с начальным элементом $\varrho(\varnothing)$.

[1] Т. е. конечные линейно упорядоченные подмножества.

Упражнение 0.21. Убедитесь, что подмножество $U \subset P$ вполне упорядочено и рекурсивно.

Поскольку элемент $\varrho(U)$ строго больше всех элементов из U, он не лежит в U. С другой стороны, множество $W = U \cup \{\varrho(U)\}$ вполне упорядочено, рекурсивно, и его начальным элементом является $\varrho(\varnothing)$. Следовательно, $W \subset U$, откуда $\varrho(U) \in U$. Противоречие. □

Предложение 0.5
Если каждое вполне упорядоченное подмножество чума P имеет верхнюю грань[1], то в P есть максимальный элемент[2] (возможно не единственный).

Доказательство. Если максимального элемента нет, то для любого $p \in P$ имеется такой элемент $p' \in P$, что $p < p'$. Тогда для каждого вполне упорядоченного подмножества $W \subset P$ найдётся такой элемент $w^* \in P$, что $w < w^*$ для всех $w \in W$. Сопоставляя каждому $W \in \mathcal{W}$ один[3] из таких элементов w^*, мы получаем отображение $\varrho : \mathcal{W} \to P$, которого не может быть по лем. 0.2. □

Определение 0.3 (полные чумы)
Частично упорядоченное множество называется *полным*, если каждая его цепь имеет верхнюю грань.

Следствие 0.1 (лемма Цорна)
В каждом полном чуме есть максимальный элемент (возможно не единственный). □

Упражнение 0.22 (лемма Бурбаки – Витта о неподвижной точке). Пусть отображение из полного чума в себя $f : P \to P$ таково, что $f(x) \geqslant x$ для всех $x \in P$. Покажите, что существует такое $p \in P$, что $f(p) = p$.

Упражнение 0.23 (теорема Цермелло). Докажите, что каждое множество можно вполне упорядочить.

Упражнение 0.24 (теорема Хаусдорфа о максимальной цепи). Докажите, что в любом чуме каждая цепь содержится в некоторой максимальной по включению цепи.

[1] Т. е. для любого вполне упорядоченного $W \subset P$ найдётся такой $p \in P$, что $w \leqslant p$ для всех $w \in W$.

[2] Т. е. такой $p^* \in P$, что неравенство $p^* \leqslant x$ выполняется в P только для $x = p^*$, см. последние два абзаца перед n° 0.8 на стр. 17.

[3] Для этого придётся воспользоваться аксиомой выбора из n° 0.5.1 на стр. 14.

§1. Поля, коммутативные кольца и абелевы группы

1.1. 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 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 элементов 0 и 1, таких 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, а операции сложения и умножения — как операции сложения и умножения классов вычетов, определённые формулами (0-20) – (0-21) 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: $0+1=1+0=1$, 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 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

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

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 $\mathbb{R}$ ни 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. 20 за исключением свойства (1-8) существования мультипликативно обратных элементов.

Если, кроме существования обратных, из списка аксиом поля исключаются требование наличия единицы (1-7) 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] См. прим. 0.5 на стр. 12.

[3] См. n° 0.4.1 на стр. 11.

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

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*.

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.

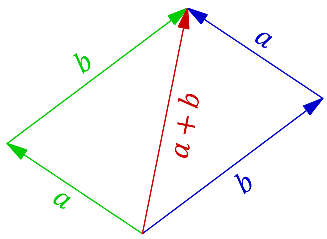


Рис. 1⋄1. Правило параллелограмма.

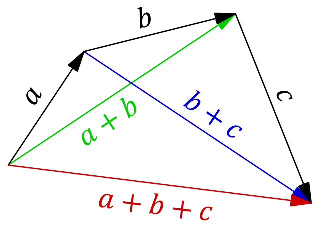


Рис. 1⋄2. Правило четырёхугольника.

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. 20 утверждают, то множество $\mathbb{F}^{\times} \stackrel{\text{def}}{=} \mathbb{F} \smallsetminus 0$ 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 $\mathbb{F}^{\times}$ 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 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 1.1. Аксиома нетривиальности (1-10) 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.

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

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

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 (1-12) имеется операция *деления* на любые ненулевые элементы

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

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

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

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 $\text{нод}(a, b)$.

Упражнение 1.4. Обобщите проделанные только что рассуждения: 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 также, что уравнение $n = a_1x_1 + \dots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ если и только если $d|n$.

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. Если $m = ka = \ell b$, то $kd\alpha = \ell d\beta$, и $k\alpha = \ell\beta$. Поскольку $\text{нод}(\alpha, \beta) = 1$, существуют такие $x, y \in \mathbb{Z}$, что $\alpha x + \beta y = 1$. Умножая обе части последнего равенства на ℓ, мы заключаем, что $\ell = \ell\alpha x + \ell\beta y = \ell\alpha x + k\alpha y$ делится на α, а значит $m = \ell b$ делится на $c = \alpha b$, 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]:

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

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

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

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

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

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

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

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

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

$$\begin{pmatrix} m & p & q \\ n & r & s \end{pmatrix}$$

кроме, может быть, итоговой (полученной перестановкой строк и/или сменой знака в одной из строк) выполняются равенства $m = pa + qb$, $n = ra + sb$ и $ps - qr = 1$.

Из упражнения вытекает, что в возникающей в конце вычисления таблице вида

$$\begin{pmatrix} d' & x & y \\ 0 & k & \ell \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & k & \ell \\ d' & x & y \end{pmatrix}$$

(где $d' \in \mathbb{Z}$ может отличаться от итогового $d \in \mathbb{N}$ лишь знаком) имеют место равенства

$$d' = ax + by\,, \quad ka = -\ell b\,, \quad \ell x - ky = 1\,.$$

Из первого вытекает, 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

$$a = \ell ax - kay = \ell ax + \ell by = \ell d' \quad \text{и} \quad b = \ell bx - kby = -kax - kby = -kd'$$

оба делятся на d', откуда $d = |d'| =$ нод(a, b), как и утверждалось.

Замечание 1.2. С вычислительной точки зрения отыскание нод(a, b) при помощи алгоритма 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 их нод по алгоритму Евклида – Гаусса занимает 6 строк:

$$\begin{aligned}
&\begin{pmatrix} 10\,203 & 1 & 0 \\ 4\,687 & 0 & 1 \end{pmatrix} && (1) \mapsto (1) - 2 \cdot (2) \\
&\begin{pmatrix} 829 & 1 & -2 \\ 4\,687 & 0 & 1 \end{pmatrix} && (2) \mapsto (2) - 6 \cdot (1) \\
&\begin{pmatrix} 829 & 1 & -2 \\ -287 & -6 & 13 \end{pmatrix} && (1) \mapsto (1) + 3 \cdot (2) \\
&\begin{pmatrix} -32 & -17 & 37 \\ -287 & -6 & 13 \end{pmatrix} && (2) \mapsto (2) - 9 \cdot (1) \\
&\begin{pmatrix} -32 & -17 & 37 \\ 1 & 147 & -320 \end{pmatrix} && (1) \mapsto (1) + 32 \cdot (2) \\
&\begin{pmatrix} 0 & 4\,687 & 10\,203 \\ 1 & 147 & -320 \end{pmatrix}\,,
\end{aligned} \tag{1-18}$$

откуда нод$(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687$, 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 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 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 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 1.8. Пользуясь лем. 1.3, 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 1.3. (нод в произвольном кольце) В произвольном коммутативном кольце K принято называть *наибольшим общим делителем* элементов $a, b \in K$ любой элемент $d \in K$, 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 $d = ax + by$.

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

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:

$$[a] + [b] \stackrel{\text{def}}{=} [a+b]\,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\,. \tag{1-19}$$

Согласно упр. 0.10 на стр. 11, эти операции определены корректно[3]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (1-19) 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 $\text{нод}(m, n) = 1$ 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. (1-18) на стр. 25 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 $\mathbb{Z}/(n)^{\times}$. Порядок этой группы равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается через $\varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}/(n)^{\times}\right|$ и называется *функцией Эйлера* числа $n \in \mathbb{Z}$.

---

[1] См. прим. 0.4 на стр. 10.

[2] См. n° 0.4 на стр. 9.

[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. 24.

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

$$a: \mathbb{Z}/(n)^{\times} \xrightarrow{\sim} \mathbb{Z}/(n)^{\times}, \quad [x] \mapsto [ax], \tag{1-20}$$

обратной к которой является умножение на вычет $[a]^{-1}$. Последовательно применяя отображение (1-20) к произвольному элементу $[z] \in \mathbb{Z}/(n)^{\times}$, получаем цепочку его образов

$$[z] \xrightarrow{a} [az] \xrightarrow{a} [a^2z] \xrightarrow{a} [a^3z] \xrightarrow{a} \dots, \tag{1-21}$$

которые начнут повторяться, ибо множество вычетов конечно. В силу биективности отображения (1-20), самым первым повторно встретившимся элементом цепочки (1-21) станет её начальный элемент $[z]$, т. е. цепочка (1-21) является циклом. В силу всё той же биективности отображения (1-20) два таких цикла, проходящие через классы $[x]$ и $[y]$, либо не пересекаются, либо полностью совпадают. Если циклы не пересекаются, то отображения умножения на классы $[x]^{-1}[y]$ и $[y]^{-1}[x]$ задают взаимно обратные биекции между ними. Мы заключаем, что множество $\mathbb{Z}/(n)^{\times}$ распадается в объединение непересекающихся циклов (1-21) *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*.

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 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

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ раз}} = 0. \tag{1-22}$$

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

$$(a+b)^p = a^p + b^p. \tag{1-23}$$

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 $(1 + \dots + 1) \cdot a^k b^{p-k}$. Стоящая в скобках сумма $\binom{p}{k}$ единиц поля $\mathbb{F}_p$ 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.

[1] См. n° 0.5.2 на стр. 14.

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 (1-23), 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 1.9. Выведите малую теорему Ферма из теоремы Эйлера[1].

Упражнение 1.10. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod p$ для простого $p \nmid m$.

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

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)\,. \tag{1-24}$$

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

Упражнение 1.11. 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 $0 = \varphi(0)$. 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 $\varphi : A \to B$ 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

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

Предложение 1.1
Каждый непустой слой[3] гомоморфизма абелевых групп $\varphi : A \to B$ 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 $\ker\varphi = 0$.

[1] См. прим. 1.6 на стр. 27.
[2] См. n° 0.5 на стр. 12.
[3] Ср. с n° 0.3 на стр. 5.

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 $\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$, 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 $\psi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^{\frac{p-1}{2}}$. По малой теореме Ферма[1] все $(p-1)/2$ ненулевых квадратов лежат в его ядре. Поэтому $|\operatorname{im} \psi| \leqslant 2$.

Упражнение 1.12. 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 1.13. 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: $\varphi_1 + \varphi_2 : a \mapsto \varphi_1(a) + \varphi_2(a)$. Нулевым элементом группы $\operatorname{Hom}(A, B)$ является *нулевой гомоморфизм*, отображающий все элементы группы A в нулевой элемент группы B.

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

$$\begin{gathered} f(a_1 + a_2) = f(a_1) + f(a_2) \\ f(a_1 a_2) = f(a_1) f(a_2) \,. \end{gathered} \tag{1-25}$$

Поскольку гомоморфизм колец $\varphi : A \to B$ 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 $\varphi : A \to B$ 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 $\varphi : A \to B$ является подкольцом в B, но он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$.

Упражнение 1.14. Убедитесь, что отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[0] \mapsto [0]$, $[1] \mapsto [3]$, является гомоморфизмом колец.

[1] См. сл. 1.1 на стр. 29.

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 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 $\forall\, a \in A\;\; \varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$. □

1.5.4. 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, $\varphi(1) = 1$ 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 $\varkappa : \mathbb{Z} \to K$, заданный правилом

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

Его 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

$$\varkappa_p : \mathbb{Z}/(p) \to K\,, \quad a \pmod p \mapsto \varkappa(a)\,. \tag{1-27}$$

По предл. 1.3 гомоморфизм (1-27) 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 $\operatorname{char} K$.

[1] Напомню, что *целостным* называется кольцо с единицей без ненулевых делителей нуля, см. n° 1.4.1 на стр. 27.

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 (1-26). 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 1.15. 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 1.16 (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

$$F_p : \mathbb{F} \to \mathbb{F}, \quad x \mapsto x^p, \tag{1-28}$$

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. 1.7 и лем. 1.4 на стр. 28). Гомоморфизм (1-28) 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. 1.1 на стр. 29.

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

$$\prod_\nu A_\nu = A_1 \times \ldots \times A_\nu \overset{\text{def}}{=} \{(a_1, \dots, a_m) \mid a_\nu \in A_\nu \ \forall\, \nu\} \tag{1-29}$$

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

$$(a_1, \dots, a_m) + (b_1, \dots, b_m) \overset{\text{def}}{=} (a_1 + b_1, \dots, a_m + b_m). \tag{1-30}$$

Упражнение 1.17. 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 (1-29) называется *прямым произведением* абелевых групп A_i. Если все группы A_i конечны, прямое произведение (1-29) 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:

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

Упражнение 1.18. 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 $(1, \dots , 1)$.

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, в произведении $\mathbb{F}_p\times\mathbb{F}_q$ конечных полей $\mathbb{F}_p$ и $\mathbb{F}_q$, состоящих из p и q элементов, есть $(p-1)(q-1)$ обратимых пар (a, b), составляющих мультипликативную группу $\mathbb{F}_p^\times\times\mathbb{F}_q^\times$, и $p+q-1$ делитель нуля вида $(a, 0)$ и $(0, b)$.

В общем случае элемент $a = (a_1, \dots , a_m) \in K_1 \times \ldots \times K_m$ 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:

$$\left(\prod K_\nu\right)^\times = \prod K_\nu^\times \tag{1-31}$$

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 $z \pmod{n_i}$:

$$\begin{gathered} \varphi : \mathbb{Z}/(n) \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m) \\ [z]_n \mapsto \left([z]_{n_1}, \dots , [z]_{n_m}\right), \end{gathered} \tag{1-32}$$

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:

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

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. 26, 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 (1-32) 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

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

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 $z + 15\,n = 816\,641$.

[1] По всё той же лем. 1.3 на стр. 26.

[2] См. n° 1.2.2 на стр. 24.

Ответы и указания к некоторым упражнениям

Упр. 0.1. Ответ: 2^n.

Упр. 0.2. Ответ на второй вопрос — нет. Пусть $X = \{1, 2\}$, $Y = \{2\}$. Все их парные пересечения и объединения суть $X \cap Y = Y \cap Y = Y \cup Y = Y$ и $X \cup Y = X \cup X = X \cap X = X$, и любая формула, составленная из $X, Y, \cap, \cup$, даст на выходе или $X = \{1, 2\}$, или $Y = \{2\}$, тогда как $X \smallsetminus Y = \{1\}$.

Упр. 0.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. 0.5. Если X конечно, то инъективное или сюрьективное отображение $X \to X$ автоматически биективно. Если X бесконечно, то в X есть подмножество, изоморфное $\mathbb{N}$. Инъекция $\mathbb{N} \hookrightarrow \mathbb{N}$, $n \mapsto (n+1)$, и сюрьекция $\mathbb{N} \twoheadrightarrow \mathbb{N}$, $n \mapsto \max(1, (n-1))$, обе не биективны и продолжаются до точно таких же отображений $X \to X$ тождественным действием на $X \smallsetminus \mathbb{N}$.

Упр. 0.6. Ответ: нет. Воспользуйтесь «диагональным трюком» Кантора: пусть все биекции $\mathbb{N} \to \mathbb{N}$ занумерованы натуральными числами; глядя на этот список, постройте биекцию, которая при каждом $k = 1, 2, 3, \dots$ отображает некоторое число $n_k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 0.7. Обозначим через $\sigma : X \xrightarrow{\sim} X$ биекцию, переставляющую между собою точки x и x' и тождественно действующую на остальные точки. Искомое отображение переводит биекцию $f : X \xrightarrow{\sim} X$ в композицию $\sigma \circ f : z \mapsto \sigma\big(f(z)\big)$.

Упр. 0.8. Ответ: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(k_1, \dots, k_m)$ с суммой $\sum k_i = n$. Такой набор можно закодировать словом, составленным из $(m-1)$ букв 0 и n букв 1: сначала пишем k_1 единиц, потом нуль, потом k_2 единиц, потом нуль, и т. д. (слово кончится k_m единицами, стоящими следом за последним, $(m-1)$-м нулём) .

Упр. 0.9. Ответ: $\binom{n+k}{k}$. Каждая такая диаграмма представляет собою ломаную, ведущую из левого нижнего угла прямоугольника в правый верхний. В такой ломаной ровно n горизонтальных звеньев и ровно k вертикальных.

Упр. 0.10. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \ell \in \mathbb{Z}$. Тогда $x' + y' = x + y + n(k + \ell)$ и $x'y' = xy + n(\ell x + ky + k\ell n)$ сравнимы по модулю n с $x + y$ и xy соответственно, т. е. $[x' + y']_n = [x + y]_n$ и $[x'y']_n = [xy]_n$.

Упр. 0.11. Положим $x \sim y$, если существует конечная последовательность точек

$$x = z_0,\ z_1,\ z_2,\ \dots,\ z_n = y$$

как в условии задачи. Проверьте, что это отношение эквивалентности и что оно содержится в любой эквивалентности $S \subset X \times X$, содержащей R.

Упр. 0.12. Рефлексивность и симметричность очевидны. Транзитивность: если $(p, q) \sim (r, s)$ и $(r, s) \sim (u, w)$, т. е. $ps - rq = 0 = us - rw$, то $psw - rqw = 0 = usq - rwq$, откуда $s(pw - uq) = 0$, и $pw = uq$, т. е. $(p, q) \sim (u, w)$.

Упр. 0.13. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi/2$, то отражение относительно ℓ_1, за которым следует отражение относительно ℓ_2, это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно пересекающихся прямых коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. 0.15. Таблица композиций gf в симметрической группе S_3:

$g \diagdown f$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,2,3)$	$(3,1,2)$	$(2,3,1)$	$(2,1,3)$	$(3,2,1)$
$(3,2,1)$	$(3,2,1)$	$(2,3,1)$	$(1,2,3)$	$(3,1,2)$	$(1,3,2)$	$(2,1,3)$
$(2,1,3)$	$(2,1,3)$	$(3,1,2)$	$(2,3,1)$	$(1,2,3)$	$(3,2,1)$	$(1,3,2)$
$(2,3,1)$	$(2,3,1)$	$(3,2,1)$	$(2,1,3)$	$(1,3,2)$	$(3,1,2)$	$(1,2,3)$
$(3,1,2)$	$(3,1,2)$	$(2,1,3)$	$(1,3,2)$	$(3,2,1)$	$(1,2,3)$	$(2,3,1)$

Упр. 0.16. Отношение $n \mid m$ на множестве $\mathbb{Z}$ не кососимметрично: $n \mid m$ и $m \mid n$ если и только если $|m| = |n| \neq 0$. Фактор множества $\mathbb{Z}$ по этому отношению эквивалентности можно отождествить с множеством $\mathbb{Z}_{\geqslant 0}$ неотрицательных целых чисел, на котором отношение $n \mid m$ является частичным порядком (обратите внимание, что нуль является нижней гранью этого множества, т. е. делит все элементы.)

Упр. 0.17. Пусть множество $S \subset W$ состоит из всех таких элементов $z \in W$, что утверждение $\Phi(z)$ ложно. Если $S \neq \varnothing$, то в нём есть начальный элемент $s_* \in S$. Поскольку утверждение $\Phi(w)$ истинно для всех $w < s_*$, утверждение $\Psi(s_*)$ тоже истинно, т. е. $s_* \notin S$. Противоречие.

Упр. 0.18. Обозначим через x_I начальный элемент дополнения $W \smallsetminus I$. Начальный интервал $[x_I) \subset W$ является объединением начальных интервалов $[y) \subset W$ по всем $y < x$. Так как I содержит все интервалы $[y)$ с $y < x_I$, мы заключаем, что $I \supseteq [x_I)$, откуда $I = [x_I)$.

Упр. 0.19. Пусть соотношение $U \geqslant W$ не выполняется. Покажем, что любой начальный отрезок $[u) \subset U$ изоморфен некоторому начальному отрезку $[w) \subset W$, где $w = w(u)$ однозначно восстанавливается по u. Это верно для пустого начального отрезка $\varnothing = [u_*]$, где $u_* \in U$ — минимальный элемент. Пусть это верно для всех начальных отрезков $[y) \subset U$ с $y < u$. Тогда $[y) = \bigcup_{y<u}[y)$ изоморфен объединению вложенных отрезков $\bigcup_{y<u}[w(y)) \subset W$. Если это объединение исчерпывает всё множество W, то $W \simeq [y)$, т. е. $W \leqslant U$ вопреки предположению. Положим $w(u) \in W$ равным минимальному элементу, не содержащемуся в $\bigcup_{y<u}[w(y))$. Проверьте, что $\bigcup_{y<u}[w(y)) = [w(u))$ и что отображение $u \mapsto w(u)$ устанавливает изоморфизм множества U либо со всем множеством W, либо с некоторым его начальным отрезком.

Упр. 0.20. Рассмотрим подмножество $Z \subseteq W_1$, состоящее из всех таких $z \in W_1$, что начальный интервал $[z)_1$ в множестве W_1 является одновременно начальным интервалом $[z)_2$ множества W_2. Множество Z не пусто, поскольку содержит общий начальный элемент множеств W_1 и W_2. Если $Z \subsetneq W_1$ и $Z \subsetneq W_2$, то по упр. 0.18 на стр. 18 подмножество Z является начальным интервалом как в W_1, так и в W_2, что невозможно, поскольку точные верхние границы этих интервалов в W_1 и W_2, с одной стороны, не лежат в Z и, стало быть, различны, а с другой стороны в силу рекурсивности множеств W_1 и W_2 обе они равны $\varrho(Z)$, то есть совпадают. Тем самым, $Z = W_1$ или $Z = W_2$. По упр. 0.18 в первом случае W_1 является начальным интервалом в W_2, а во втором — W_2 является начальным интервалом в W_1.

Упр. 0.21. Каждое подмножество $S \subset U$ имеет непустое пересечение с каким-нибудь рекурсивным вполне упорядоченным подмножеством $W \subset P$ с начальным элементом $\varrho(\varnothing)$. По упр. 0.20 подмножество W является начальным интервалом всех содержащих W рекурсивных вполне упорядоченных подмножеств с начальным элементом $\varrho(\varnothing)$. Поэтому начальный элемент пересечения $S \cap W$ не зависит от выбора W с $W \cap S \neq \varnothing$ и является начальным элементом подмножества S.

Каждый начальный интервал $[u) \subset U$ является начальным интервалом любого содержащего u множества W из цепи. В силу рекурсивности W элемент $\varrho[u) = u$.

Упр. 0.22. Пользуясь аксиомой выбора, зафиксируем для каждого $W \in \mathcal{W}(P)$ какую-нибудь верхнюю грань $b(W) \in P$. Если $f(x) > x$ для всех $x \in P$, то отображение $\beta : \mathcal{W}(P) \to P, W \mapsto f(b(W))$ противоречит лем. 0.2 на стр. 18.

Упр. 0.23. Обозначим через $\mathcal{S}(X)$ множество всех непустых подмножеств данного множества X, включая само X. При помощи аксиомы выбора постройте такое отображение $\mu : \mathcal{S}(X) \to X$, что $\mu(Z) \in Z$ для всех $Z \in \mathcal{S}(X)$. Обозначим через $\mathcal{W}(X)$ множество всех $W \in \mathcal{S}(X)$, которые можно вполне упорядочить так, что $\mu(X \smallsetminus [w)) = w$ для всех $w \in W$. Вдохновляясь лем. 0.2 на стр. 18 покажите, что $\mathcal{W}(X) \neq \varnothing$, и убедитесь, что $X \in \mathcal{W}(X)$.

Упр. 0.24. Убедитесь, что множество всех цепей, содержащих данную цепь, является полным чумом относительно отношения включения, и примените лемму Цорна.

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 $\begin{pmatrix} m & p & q \\ n & r & s \end{pmatrix}$ удовлетворяют равенствам $m = pa + qb$, $n = ra + sb$ и $ps - qr = 1$. Прибавляя к 1-й строке 2-ю, умноженную на k, получаем таблицу $\begin{pmatrix} m' & p' & q' \\ n & r & s \end{pmatrix}$, в которой $m' = m + nk$, $p' = p + kr$, $q' = q + ks$. Тогда

$$\begin{aligned} m' &= pa + qb + k(ra + sb) = p'a + q'b \\ p's - q'r &= ps - qr + krs - ksr = 1 \,. \end{aligned}$$

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. 26. 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. 1.10. 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. (1-23) на стр. 28, получаем

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

Упр. 1.12. 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. 1.13. По малой теореме Ферма[1] каждый элемент $x \in \operatorname{im}\psi$ удовлетворяет уравнению $x^2 = 1$.

Упр. 1.15. Ненулевой гомоморфизм полей инъективен, переводит единицу в единицу и перестановочен со сложением, вычитанием, умножением и делением[2]. 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. 1.16. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

[1] См. сл. 1.1 на стр. 29.

[2] См. n° 1.5.4 на стр. 31.