А. Л. Городенцев*

А Л Г Е Б Р А

1-й курс

Факультет математики НИУ ВШЭ
2025/26 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 из них знакомы читателю из школы или вводных летних занятий «Матфак — предисловие», 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, 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 непустого множества 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 по определению являются 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

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

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 $\operatorname{Hom}(X, Y)$.

Отображение $f : X \to Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\operatorname{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюръективные 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 такой $x \in X$, 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 сюръекции и все биекции.

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

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 $\operatorname{Aut}(X)$. 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 $\operatorname{Aut}(\mathbb{N})$?

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

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

$$w(f) \stackrel{\text{def}}{=} \big(f(1), f(2), \ldots, f(n)\big) \tag{0-1}$$

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

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

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.

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

Доказательство. Пусть X состоит из n элементов, а Y — из m, как в прим. 0.1 выше. Нас интересует количество всех n-буквенных слов, которые можно написать при помощи алфавита из m букв. Обозначим его через $W_m(n)$ и выпишем все эти слова на m страницах, поместив на i-ю страницу все слова, начинающиеся на i-ю букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Поэтому $W_m(n) = m \cdot W_m(n-1) = m^2 \cdot W(n-2) = \ldots = m^{n-1} \cdot W_m(1) = m^n$. □

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

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

Доказательство. Пусть $X = \{x_1, \ldots, x_n\}$. Биекции $X \xrightarrow{\sim} X$ записываются n-буквенными словами в n-буквеном алфавите $x_1, \ldots, x_n$, содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n

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

страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. Тогда на каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \\ = \ldots = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot V(1) = n!$. □

Замечание 0.2. Число $n! = n \cdot (n-1) \cdot \ldots \cdot 1$ называется *n-факториал*. Так как множество $\mathrm{Aut}(\varnothing)$ состоит из одного элемента $\mathrm{Id}_\varnothing$, мы полагаем $0! \stackrel{\text{def}}{=} 1$.

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

$$X = \bigsqcup\nolimits_{y \in \mathrm{im}(f)} f^{-1}(y)\,. \tag{0-3}$$

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.

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

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1 + \ldots + k_m = n \\ \forall i\ 0 \leqslant k_i \leqslant n}} \binom{n}{k_1 \ldots k_m} \cdot a_1^{k_1} \ldots a_m^{k_m}\,, \tag{0-5}$$

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

$$(a_1 + \ldots + a_m)(a_1 + \ldots + a_m) \ldots (a_1 + \ldots + a_m)$$

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 $a_1^{k_1} a_2^{k_2} \ldots a_m^{k_m}$, 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 $n = k_1 + \ldots + k_m$ попарно разных букв:

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

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 $k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!$ 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)

$$\binom{n}{k_1 \ldots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!}. \tag{0-6}$$

Тем самым, разложение (0-5) имеет вид

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1+\ldots+k_m=n \\ \forall i\ 0 \leqslant k_i \leqslant n}} \frac{n! \cdot a_1^{k_1} \ldots a_m^{k_m}}{k_1! \cdot \ldots \cdot k_m!}. \tag{0-7}$$

Упражнение 0.7. Сколько всего слагаемых в правой части формулы (0-7) ?

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

$$(a + b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}. \tag{0-8}$$

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

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

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

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

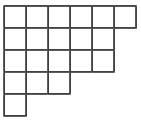
$$X = X_1 \sqcup X_2 \sqcup \ \ldots\ \sqcup X_k \tag{0-9}$$

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

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

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

которая называется *формой* разбиения (0-9). Форму разбиения удобно изображать *диаграммой Юнга* — картинкой вида

 , (0-10)

составленной из выровненных по левому краю горизонтальных клетчатых полосок, занумерованных сверху вниз, так что в i-й 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 (0-10) отвечает разбиению формы $\lambda = (6, 5, 5, 3, 1)$, имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 0.8. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток с левым верхним углом в левом верхнем углу диаграммы (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.

Объединяя элементы, стоящие в i-й 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 (0-9) заданной формы λ можно получить таким образом, возникает сюръективное 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 $\prod \lambda_i! = \prod_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod_{i=1}^{n} (i!)^{m_i} m_i!$ 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

$$\frac{n!}{\prod_{i=1}^{n} m_i! \cdot (i!)^{m_i}}. \tag{0-11}$$

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

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

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{0-12}$$

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

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

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \pmod{n} \tag{0-15}$$

(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:

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

Среди бинарных отношений (0-12) – (0-15) первое и последнее являются эквивалентностями, а (0-13) и (0-14) 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. Сюрьекция

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]_R\,, \tag{0-16}$$

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 (0-15) 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

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z - x) \vdots n\} \tag{0-17}$$

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

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

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

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}\,. \tag{0-18}$$

Упражнение 0.9. 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

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{0-19}$$

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

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

[1] Именно такое умножение $[12]^{100} = \underbrace{[12]\cdot[12]\cdot\ldots\cdot[12]}_{100} = \left[12^{100}\right]$ было использовано в (0-18).

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 0.10. 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 $(z_{i-1}, z_i) \in R$ или $(z_i, z_{i-1}) \in R$ 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.

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

$$(a, b) \sim (ac, bc) \quad \text{с произвольными } c \in \mathbb{Z} \smallsetminus \{0\}\,. \tag{0-21}$$

Отношения (0-21) 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 (0-21), как, например, $3/6$ и $5/10$. Поэтому эквивалентность, порождённая отождествлениями (0-21), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{0-22}$$

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

Упражнение 0.11. Проверьте, что набор отношений (0-22) рефлексивен, симметричен и транзитивен.

Тем самым, он является минимальным отношением эквивалентности, содержащим все отождествления (0-21). Отметим, что если в отношениях (0-21) 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 0.12. 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. 5, 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:

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

(0-23)

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 всякое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, называется *левым обратным* к f или *ретракцией* Y на $f(X)$.

Упражнение 0.13. В условиях лем. 0.1 убедитесь, что вложение f тогда и только тогда имеет несколько различных левых обратных, когда оно не сюръективно.

0.5.1. Правое обратное отображение и аксиома выбора. Стремление к гармонии вызывает желание иметь «правую» версию лем. 0.1 — хочется, чтобы следующие три свойства отображения $f : X \to Y$ тоже были эквивалентны:

1) f сюръективно

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), называется *обратимым справа*, а 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 сюръективного отображения можно выбрать по элементу[2].

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

[2] Иными словами, если имеется множество попарно непересекающихся множеств, то в каждом из них можно выбрать по элементу.

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) доказывается, как в лем. 0.1, от противного: при $y \notin \operatorname{im} f$ свойство (3) не выполняется для $g_1 = \mathrm{Id}_Y$ 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, если включить аксиому выбора в список свойств, определяющих множества.

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.

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X \tag{0-24}$$

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[1] $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

3) g обладает левым и правым обратными отображениями[2].

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 $g' = g^{-1}$. □

[1] Т. е. g' *двусторонне* обратно к g.

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

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-й *симметрической группой*. Согласно предл. 0.2 на стр. 5 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 $\sigma_i \stackrel{\text{def}}{=} \sigma(i)$, как в прим. 0.1 на стр. 5. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ представляют собою отображения

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

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

Упражнение 0.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (0-23) на стр. 12.

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

[1] См. n° 0.4 на стр. 9.
[2] Ср. с опр. 0.1 на стр. 9.

$x < y$, когда $x \leqslant y$ и $x \neq y$. Частичный порядок на множестве Z называется *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 0.15 (предпорядок). *Предпорядком* на множестве Z называется любое рефлексивное транзитивное бинарное отношение $x \prec y$. Убедитесь, что для каждого предпорядка бинарное отношение $x \sim y$, означающее, что одновременно $x \prec y$ и $y \prec x$, является отношением эквивалентности, и на факторе $Z/\sim$ корректно определено[1] бинарное отношение $[x] \leqslant [y]$, означающее, что $x \prec y$, которое 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 линейный, чум P называется *линейно упорядоченным*. Всякое подмножество X любого 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*[2] или *морфизмом* чумов, если $f(x) \leqslant f(y)$ для всех $x \leqslant y$. 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 $f(x) < f(y)$ для всех $x < y$. 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 для $x \in X$ неравенство $m^* \leqslant x$ 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 $\mathbb{N}$ по отношению к делимости или к обычному неравенству между числами. Линей-

[1] Т. е. выполнение или невыполнение условия $x \lesssim y$ не зависит от выбора представителей x и y в классах $[x]$ и $[y]$.

[2] А также *неубывающим* или *нестрого возрастающим*.

но 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* в X, если для $x \in X$ неравенство $m_* \geqslant x$ выполняется только при $x = m_*$. 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 также, 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 0.16. 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 *начальными интервалами* частично упорядоченного множества W и обозначаются

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

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 0.17. 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 можно биективно и с сохранением порядка отобразить на W или на какой-нибудь начальный интервал $[w) \subset W$. Если при этом U и W не изоморфны, мы пишем $U < W$. Хорошим упражнением на трансфинитную индукцию является

Упражнение 0.18. 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] $C \subset P$, 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

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

рекурсивно и его можно расширять дальше вправо, пока P не исчерпается, что противоречит наложенному на ϱ условию. Уточним сказанное. Если два рекурсивных вполне упорядоченных подмножества имеют общий начальный элемент, то либо они совпадают, либо одно из них является начальным интервалом другого.

Упражнение 0.19. Докажите это.

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

Упражнение 0.20. 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[2], то в P есть максимальный элемент[3] (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[4] из таких элементов w^*, мы получаем отображение $\varrho : \mathcal{W} \to P$,

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

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

[3] 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.

[4] Для этого придётся воспользоваться аксиомой выбора из n° 0.5.1 на стр. 13.

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 0.21 (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 0.22 (теорема Цермелло). Докажите, что каждое множество можно вполне упорядочить.

Упражнение 0.23 (теорема Хаусдорфа о максимальной цепи). Докажите, что в любом чуме каждая цепь содержится в некоторой максимальной по включению цепи.

§1. Поля, коммутативные кольца и абелевы группы

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

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

свойства сложения

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

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

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

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

свойства умножения

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

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

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

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

свойства, связывающие сложение с умножением

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

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

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

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

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, т. е. «чётное» $=0$ и «нечётное» $=1$, со сложением и умножением, заданными формулами (0-19) – (0-20) на стр. 10. С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как «ложь» $=0$ и «истина» $=1$, сложение — как логическое «исключающее или»[1], а умножение — как логическое «и»[2]. При такой интерпретации алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

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

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

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

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

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

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

Сложение и умножение дробей определяется формулами

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

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

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

1.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти операции обладают всеми свойствами из опр. 1.1 на стр. 20 за исключением свойства (1-8) существования мультипликативно обратных элементов и условия $0 \neq 1$. Если, кроме этих двух аксиом из списка аксиом поля исключается требование наличия единицы (1-7), то множество K с двумя операциями, удовлетворяющими оставшимся аксиомам, называется просто *коммутативным кольцом*. Примерами отличных от полей колец с единицами являются кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные целые числа, многочлены с чётными целыми коэффициентами, многочлены без свободного члена с коэффициентами в любом коммутативном кольце и т. п.

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

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

[2] См. прим. 0.5 на стр. 11.

[3] См. n° 0.4.1 на стр. 11.

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

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

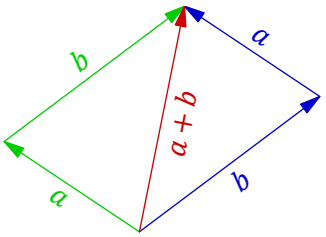


Рис. 1⋄1. Правило параллелограмма.

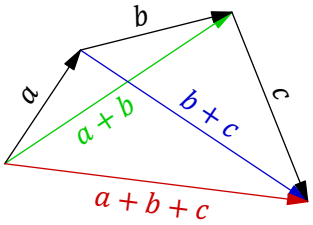


Рис. 1⋄2. Правило четырёхугольника.

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

Пример 1.5 (мультипликативная группа поля)
Четыре аксиомы умножения из опр. 1.1 на стр. 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 для любого элемента a выполняется равенство $0 \cdot a = 0$, а в любом коммутативном кольце с единицей — равенство $(-1) \cdot a = -a$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Упражнение 1.7. Объясните почему.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Согласно упр. 0.9 на стр. 10, эти операции определены корректно[3]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (1-20) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы выполнены.

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

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

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

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

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[1] См. n° 0.5.2 на стр. 14.

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

[1] См. прим. 1.6 на стр. 28.
[2] См. n° 0.5 на стр. 12.

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

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

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

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

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

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

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

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

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

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

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

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

[1] Ср. с n° 0.3 на стр. 6.
[2] См. сл. 1.1 на стр. 29.

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

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

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

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

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

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

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

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

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[1] См. сл. 1.1 на стр. 29.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Аналогично проверяется, что φ перестановочно с умножением, т. е. является гомоморфизмом колец. Если $[z]_n \in \ker\varphi$, то z делится на каждое n_i, а значит, по лем. 1.3 на стр. 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 (1-33) биективно. Этот факт известен как *китайская теорема об остатках*.

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

Пример 1.11

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

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

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

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

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

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

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

[2] См. п° 1.2.2 на стр. 24.

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

§2. Многочлены и расширения полей

Всюду в этом параграфе мы обозначаем через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

2.1. Ряды и многочлены. Бесконечное выражение вида

$$f(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \dots \text{, где } a_i \in K, \tag{2-1}$$

называется *формальным степенным рядом* от x с коэффициентами в кольце K. Ряды

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \dots \end{aligned} \tag{2-2}$$

равны, если $a_i = b_i$ для всех i. Сложение и умножение рядов (2-2) осуществляется по стандартным правилам раскрытия скобок и приведения подобных слагаемых: коэффициенты s_m и p_m рядов $s(x) = f(x) + g(x) = s_0 + s_1 x + s_2 x^2 + \dots$ и $p(x) = f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \dots$ суть[1]

$$\begin{aligned} s_m &= a_m + b_m \\ p_m &= \sum_{\alpha+\beta=m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \dots + a_{m-1} b_1 + a_m b_0 \end{aligned} \tag{2-3}$$

Упражнение 2.1. Убедитесь, что эти две операции удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной x с коэффициентами в кольце K обозначается через $K[\![x]\!]$. Начальный коэффициент a_0 ряда (2-1) называется *свободным членом* этого ряда. Самый левый ненулевой коэффициент в (2-1) называется *младшим* коэффициентом ряда f, а его номер — *порядком* ряда f и обозначается $\operatorname{ord} f$. Если в кольце K нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца тоже является целостным и $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.

Кольцо $K[\![x_1, \dots, x_n]\!]$ формальных степенных рядов от n переменных определяется по индукции: $K[\![x_1, \dots, x_n]\!] \stackrel{\text{def}}{=} K[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$ представляет собою множество формальных сумм вида $F(x) = \sum_{\nu_1, \dots, \nu_n \in \mathbb{Z}_{\geqslant 0}} a_{\nu_1 \dots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$.

2.1.1. Алгебраические операции над рядами. Назовём *n-арной алгебраической операцией* в $K[\![x]\!]$ правило, сопоставляющее n рядам $f_1, \dots, f_n$ новый ряд f так, что каждый коэффициент ряда f вычисляется по коэффициентам рядов $f_1, \dots, f_n$ при помощи конечного числа[2] операций в K. Например, сложение и умножение рядов — это бинарные алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[3].

[1] Говоря формально, операции, о которых тут идёт речь, являются операциями над *последовательностями* (a_ν) и (b_ν) элементов кольца K. Буква x служит лишь для облегчения их восприятия.

[2] Которое может зависеть от номера коэффициента.

[3] Очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда. Однако при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений.

Пример 2.1 (замена переменной)
Подстановка в ряд (2-1) вместо x любого ряда $g(x) = b_1x + b_2x^2 + \dots$ с нулевым свободным членом является бинарной алгебраической операцией, дающей на выходе ряд

$$f(g(x)) = a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 + \dots = \\ = a_0 + (a_1b_1)\cdot x + (a_1b_2 + a_2b_1^2)\cdot x^2 + (a_1b_3 + 2\,a_2b_1b_2 + a_3b_1^3)\cdot x^3 + \dots\,,$$

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых в f.

Пример 2.2 (обращение)
Покажем, что ряд $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[\![x]\!]$ обратим в $K[\![x]\!]$ если и только если его свободный член a_0 обратим в K, и в этом случае обращение $f \mapsto f^{-1}$ является унарной алгебраической операцией над обратимым рядом f. Пусть

$$(a_0 + a_1x + a_2x^2 + \dots)\cdot(b_0 + b_1x + b_2x^2 + \dots) = 1\,.$$

Приравнивая коэффициенты при одинаковых степенях x в левой и правой части, получаем бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1\\ a_0b_1 + a_1b_0 &= 0\\ a_0b_2 + a_1b_1 + a_2b_0 &= 0\\ \dots\dots\dots\dots\dots\dots\dots\dots \end{aligned} \tag{2-4}$$

на коэффициенты b_i. Разрешимость первого уравнения равносильна обратимости a_0, и в этом случае $b_0 = a_0^{-1}$ и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$ при всех $k \geqslant 1$.

Упражнение 2.2. Вычислите в $\mathbb{Q}[\![x]\!]$ а) $(1-x)^{-1}$ б) $(1-x^2)^{-1}$ в) $(1-x)^{-2}$.

2.1.2. Многочлены. Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от $x_1, \dots, x_n$ с коэффициентами в K образуют в кольце степенных рядов подкольцо, которое обозначается $K[x_1, \dots, x_n] \subset K[\![x_1, \dots, x_n]\!]$. Многочлен от одной переменной x представляет собою формальное выражение вида $f(x) = a_0 + a_1x + \dots + a_nx^n$. Самый правый ненулевой коэффициент в нём называется *старшим*, а его номер — *степенью* многочлена f и обозначается $\deg f$. Многочлены со старшим коэффициентом 1 называются *приведёнными*, а многочлены степени нуль — *константами*.

Так как старший коэффициент произведения равен произведению старших коэффициентов сомножителей, для многочленов f_1, f_2 с коэффициентами в целостном[1] кольце K выполняется равенство $\deg(f_1f_2) = \deg(f_1) + \deg(f_2)$. В частности, кольцо $K[x]$ тоже целостное, и обратимыми элементами в нём являются только обратимые константы.

Упражнение 2.3. Покажите, что $y^n - x^n$ делится в $\mathbb{Z}[x, y]$ на $y - x$ и найдите частное.

2.1.3. Дифференциальное исчисление. Заменим в $f(x) = a_0 + a_1x + a_2x^2 + \dots$ переменную x на $x + t$, где t — ещё одна переменная. Получим ряд

$$f(x + t) = a_0 + a_1(x + t) + a_2(x + t)^2 + \dots \in K[\![x, t]\!]\,.$$

[1] Т. е. с единицей и без делителей нуля.

Раскроем в нём все скобки, затем сгруппируем слагаемые по степеням переменной t и обозначим через $f_m(x) \in K[\![x]\!]$ ряд, возникающий как коэффициент при t^m:

$$f(x+t) = f_0(x) + f_1(x)\cdot t + f_2(x)\cdot t^2 + f_3(x)\cdot t^3 + \ldots = \sum_{m\geqslant 0} f_m(x)\cdot t^m\,. \tag{2-5}$$

Упражнение 2.4. Убедитесь, что $f_0(x) = f(x)$ совпадает с исходным рядом f.

Ряд $f_1(x)$ называется *производной* от исходного ряда f и обозначается f' или $\frac{d}{dx}f$. Он однозначно определяется равенством

$$f(x+t) = f(x) + f'(x)\cdot t + (\text{члены, делящиеся на } t^2)$$

и может быть вычислен при помощи упр. 2.3 как результат подстановки $t = 0$ в ряд

$$\frac{f(x+t)-f(x)}{t} = \sum_{k\geqslant 1} a_k \frac{(x+t)^k - x^k}{t} = \sum_{k\geqslant 1} a_k\big((x+t)^{k-1} + (x+t)^{k-2}x + \ldots + x^{k-1}\big)\,,$$

что даёт

$$f'(x) = \sum_{k\geqslant 1} k\,a_k x^{k-1} = a_1 + 2a_2 x + 3a_3 x^2 + \ldots\,. \tag{2-6}$$

Пример 2.3 (ряды с нулевой производной)
Из формулы (2-6) вытекает, что производная от константы равна нулю. Если[1] $\operatorname{char} K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = a_0$. Но если $\operatorname{char} K = p > 0$, то производная от каждого монома вида x^{kp} занулится, поскольку коэффициент m при x^{m-1} в формуле (2-6) представляет собою сумму m единиц кольца K. Мы заключаем, над целостным кольцом K характеристики $p > 0$ равенство $f'(x) = 0$ означает, что $f(x) = g(x^p)$ для некоторого $g \in K[\![x]\!]$.

Упражнение 2.5. Покажите, что при простом $p \in \mathbb{N}$ для любого ряда $g \in \mathbb{F}_p[\![x]\!]$ выполняется равенство $g(x^p) = g(x)^p$.

Предложение 2.1 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[\![x]\!]$ справедливы равенства

$$(\alpha f)' = \alpha\cdot f'\,,\quad (f+g)' = f'+g'\,,\quad (fg)' = f'\cdot g + f\cdot g'\,. \tag{2-7}$$

Кроме того, если ряд g не имеет свободного члена, то

$$\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)\,, \tag{2-8}$$

а если ряд f обратим, то

$$\frac{d}{dx}f^{-1} = -f'/f^2\,. \tag{2-9}$$

Доказательство. Первые два равенства в (2-7) вытекают прямо из формулы (2-6). Для доказательства третьего перемножим ряды

$$f(x+t) = f(x) + t\cdot f'(x) + (\text{члены, делящиеся на } t^2)$$
$$g(x+t) = g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\,.$$

[1] См. n° 1.5.5 на стр. 31.

С точностью до членов, делящихся на t^2, получим

$$f(x+t)g(x+t) = f(x)g(x) + t\cdot(f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } t^2)\,,$$

откуда $(fg)' = f'\cdot g + f\cdot g'$. Формула (2-8) доказывается похожим образом: подставляя в $f(x)$ вместо x ряд $g(x+t)$, получаем $f\big(g(x+t)\big) = f\big(g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\big)$. Полагая $\tau(x,t) \stackrel{\text{def}}{=} g(x+t) - g(x) = t\cdot g'(x) + (\text{члены, делящиеся на } t^2)$ и переписывая правую часть предыдущего ряда как

$$\begin{aligned} f\big(g(x+t)\big) = f\big(g(x) + \tau(x,t)\big) = \\ = f(g(x)) + \tau(x,t)\cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x,t)^2) = \\ = f(g(x)) + t\cdot g'(x)\cdot f'(g(x)) + (\text{члены, делящиеся на } t^2)\,, \end{aligned}$$

заключаем, что $\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)$. Для доказательства формулы (2-9) достаточно продифференцировать обе части равенства $f\cdot f^{-1} = 1$. □

Упражнение 2.6. Покажите, что при $\operatorname{char}\Bbbk = 0$ в разложении (2-5) каждый ряд $f_m(x)$ равен $\frac{1}{m!}\big(\frac{d}{dx}\big)^m f(x)$, где $\big(\frac{d}{dx}\big)^m$ означает m-кратное применение операции $\frac{d}{dx}$.

2.2. Делимость в кольце многочленов. Школьный алгоритм «деления уголком» работает для многочленов с коэффициентами в произвольном коммутативном кольце с единицей при условии, что многочлен-делитель имеет обратимый старший коэффициент.

Предложение 2.2 (деление с остатком)
Пусть K — произвольное коммутативное кольцо с единицей, и старший коэффициент многочлена $u\in K[x]$ обратим. Тогда для любого $f\in K[x]$ существуют такие $q, r\in K[x]$, что $f = uq + r$ и $\deg(r) < \deg(u)$ или $r = 0$. Если кольцо K целостное, то q и r однозначно определяются этими свойствами по f и u.

Доказательство. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$ и $u = b_k x^k + \ldots + b_1 x + b_0$, где b_k обратим. Если $n < k$, можно взять $q = 0$ и $r = f$. Если $k = 0$, т. е. $u = b_0$, можно взять $r = 0$, $q = b_0^{-1} f$. Пусть $n \geqslant k > 0$ и предложение справедливо для всех многочленов f с $\deg f < n$. Тогда многочлен $f - a_n b_k^{-1} x^{n-k} u$ имеет степень, строго меньшую чем n, и по индукции представляется в виде $qu + r$, где $\deg r < \deg u$ или $r = 0$. Тем самым, $f = (q + a_n b_k^{-1} x^{n-k})\cdot u + r$, как и утверждалось. Если кольцо K целостное и $p, s\in K[x]$ таковы, что $\deg(s) < \deg(u)$ и $up + s = f = uq + r$, то $u(q-p) = r - s$. При $p - q \neq 0$ степень левой части не менее $\deg u$, что строго больше степени правой. Поэтому, $p - q = 0$, откуда и $r - s = 0$. □

Определение 2.1
Многочлены q и r, удовлетворяющие условиям предл. 2.2 называются *неполным частным* и *остатком* от деления f на u в $K[x]$.

Следствие 2.1
Для любых многочленов f, g с коэффициентами в любом поле $\Bbbk$ существует единственная такая пара многочленов $q, r\in\Bbbk[x]$, что $f = g\cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$. □

Пример 2.4 (вычисление значения многочлена в точке)
Остаток от деления многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0$ на линейный двучлен $x - \alpha$ имеет степень нуль и равен значению $f(\alpha)$ многочлена f при $x = \alpha$, в чём легко убедиться, подставляя

$x = \alpha$ в равенство $f(x) = (x-\alpha)\cdot q(x) + r$. При «делении уголком» значение $f(\alpha)$ вычисляется в виде

$$f(\alpha) = \alpha\Big(\dots\alpha\big(\alpha(\alpha a_n + a_{n-1}) + a_{n-2}\big) + \dots\Big) + a_0\,,$$

что гораздо эффективнее «лобовой подстановки» значения $x = \alpha$ в $a_n x^n + \dots + a_1 x + a_0$.

Предложение 2.3
Над произвольным полем $\Bbbk$ для любого набора многочленов $f_1, \dots, f_n \in \Bbbk[x]$ существует единственный приведённый многочлен $d \in \Bbbk[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i. Он представляется в виде

$$d = f_1 h_1 + \dots + f_n h_n\,, \quad \text{где} \quad h_i \in \Bbbk[x]\,. \tag{2-10}$$

Произвольный многочлен $g \in \Bbbk[x]$ представим в виде (2-10) если и только если $d \mid g$.

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены. Существование доказывается тем же рассуждением, что и в n° 1.4.2 на стр. 27. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (2-10), через $(f_1, \dots, f_n) \stackrel{\text{def}}{=} \big\{ f_1 h_1 + \dots + f_n h_n \,\big|\, h_i \in \Bbbk[x] \big\}$. Это подкольцо в $\Bbbk[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg с любым $h \in \Bbbk[x]$. Кроме того, $(f_1, \dots, f_n)$ содержит каждый из многочленов f_i, и все многочлены из $(f_1, \dots, f_n)$ делятся на любой общий делитель всех многочленов f_i. Возьмём в качестве d приведённый многочлен наименьшей степени в $(f_1, \dots, f_n)$. Для любого $g \in (f_1, \dots, f_n)$ остаток $r = g - qd$ от деления g на d лежит в $(f_1, \dots, f_n)$, и так как неравенство $\deg r < \deg d$ невозможно, мы заключаем, что $r = 0$, т. е. все $g \in (f_1, \dots, f_n)$ делятся на d. □

Определение 2.2
Многочлен d из предл. 2.3 называется *наибольшим общим делителем*[1] многочленов f_i и обозначается $\text{нод}(f_1, \dots, f_n)$.

2.2.1. Взаимная простота. Из предл. 2.3 вытекает, что для любого поля $\Bbbk$ взаимная простота[2] многочленов $f_1, \dots, f_m \in \Bbbk[x]$, т. е. наличие таких $h_1, \dots, h_m \in \Bbbk[x]$, что $h_1 f_1 + \dots + h_n f_n = 1$, равносильна отсутствию у многочленов $f_1, \dots, f_n$ общих делителей положительной степени — точно также, как это происходит в кольце целых чисел $\mathbb{Z}$.

Определение 2.3
Необратимый многочлен $f \in K[x]$ с коэффициентами в целостном[3] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 2.7. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 1.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: каждый многочлен f положительной степени является произведением конечного числа неприводимых многочленов, причём в любых двух таких представлениях $p_1 \dots p_k = f = q_1 \dots q_m$ одинаковое количество множителей $k = m$, и их можно перенумеровать так, чтобы $p_i = \lambda_i q_i$ при всех i для некоторых ненулевых констант $\lambda_i \in \Bbbk$.

[1] Ср. с зам. 1.3. на стр. 26.
[2] См. опр. 1.2 на стр. 26.
[3] Т. е. с единицей и без делителей нуля.

2.2.2. Алгоритм Евклида – Гаусса из n° 1.2.2 также применим к многочленам с коэффициентами из любого поля $\Bbbk$. Покажем, как он работает, вычислив нод(f, g) для

$$f = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \text{ и } g = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4\,.$$

Как и в n° 1.2.2 на стр. 24, составляем таблицу

$$\begin{pmatrix} f & 1 & 0 \\ g & 0 & 1 \end{pmatrix} = \begin{pmatrix} x^7 + 3x^6 + 4x^5 + x^4 + 3x^3 + 5x^2 + 3x + 4 & 1 & 0 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}.$$

и преобразуем её строки, умножая какую-нибудь из них на ненулевую константу и прибавляя к результату другую строку, умноженную на подходящий многочлен, так, чтобы степень одного из многочленов в левом столбце строго уменьшалась, пока один из них не обнулится:

$$\begin{aligned}
(1) \mapsto (1) - x^2\,(2): &\quad \begin{pmatrix} -2x^6 - 7x^5 - 11x^4 - 4x^3 + x^2 + 3x + 4 & 1 & -x^2 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(1) \mapsto (1) + 2x\,(2): &\quad \begin{pmatrix} 3x^5 + 11x^4 + 20x^3 + 15x^2 + 11x + 4 & 1 & -x^2 + 2x \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(1) \mapsto (1) - 3\,(2): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(2) \mapsto 4\,(2) + x\,(1): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ 7x^4 + 23x^3 + 38x^2 + 20x + 16 & x & -x^3 + 2x^2 - 3x + 4 \end{pmatrix} \\
(2) \mapsto 4\,(2) + 7\,(1): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(1) \mapsto (1) + 4x\,(2): &\quad \begin{pmatrix} 7x^3 + 19x^2 + 22x - 8 & 16x^2 + 28x + 1 & -16x^4 + 4x^3 + 7x^2 - 18x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(1) \mapsto (1) - 7\,(2): &\quad \begin{pmatrix} -16x^2 - 48x - 64 & 16x^2 - 48 & -16x^4 + 32x^3 - 32x + 32 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(2) \mapsto (2) + x\,(1)/16: &\quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 2x^2 + 6x + 8 & x^3 + x + 7 & -x^5 + 2x^4 - 4x^3 - x^2 + 4x - 5 \end{pmatrix} \\
(2) \mapsto (2) - 2\,(1): &\quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 0 & x^3 + 2x^2 + x + 1 & -x^5 - x^2 - 1 \end{pmatrix}
\end{aligned}$$

Полученный результат означает, что нод$(f, g) = x^2 + 3x + 4 = -(x^2 - 3) \cdot f + (x^4 - 2x^3 + 2x - 2) \cdot g$, а нок$(f, g) = (x^3 + 2x^2 + x + 1) \cdot f = (x^5 + x^2 + 1) \cdot g$.

Упражнение 2.8. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$$

выполняются равенства $p = rf + sg$, $q = uf + wg$, а многочлен $rw - us$ является ненулевой константой, и выведите из них, что в итоговой таблице вида

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & m_1 & m_2 \\ d' & h_1 & h_2 \end{pmatrix}$$

многочлен $d' = fh_1 + gh_2$ делит f и g, а многочлен $c' = fm_1 = -gm_2$ делит любое общее кратное f и g.

2.3. Корни многочленов. Число $\alpha \in K$ называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в прим. 2.4 на стр. 39, это равносильно тому, что $f(x)$ делится в $K[x]$ на $x - \alpha$.

Упражнение 2.9. Пусть $\Bbbk$ — поле. Проверьте, что многочлен степени 2 или 3 неприводим в $\Bbbk[x]$ если и только если у него нет корней в поле $\Bbbk$.

Предложение 2.4
Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \dots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, $\deg(f) \geqslant s$ или $f = 0$.

Доказательство. Так как в K нет делителей нуля и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в равенство $f(x) = (x - \alpha_1) \cdot q(x)$ значения $x = \alpha_2, \dots, \alpha_s$, убеждаемся, что они являются корнями многочлена $q(x)$, и применяем индукцию. □

Следствие 2.2
Пусть кольцо K целостное, и $f, g \in K[x]$ имеют степени, не превосходящие n. Если $f(\alpha_i) = g(\alpha_i)$ для более, чем n попарно разных $\alpha_i \in K$, то $f = g$ в $K[x]$.

Доказательство. Так как $\deg(f - g) \leqslant n$, и у $f - g$ больше n корней, $f - g = 0$. □

Пример 2.5 (интерполяционный многочлен Лагранжа)
Пусть $\Bbbk$ — поле. По сл. 2.2 для любых наборов из $n + 1$ различных чисел $a_0, a_1, \dots, a_n \in \Bbbk$ и произвольных значений $b_0, b_1, \dots, b_n \in \Bbbk$ имеется не более одного многочлена $f \in \Bbbk[x]$ степени $\leqslant n$ со значениями $f(a_i) = b_i$ при всех i. Единственный такой многочлен всегда существует и называется *интерполяционным многочленом Лагранжа*. Чтобы выписать его явно заметим, что произведение $\prod_{\nu \neq i} (x - a_\nu)$ зануляется во всех точках a_ν кроме i-той, где его значение отлично от нуля. Деля на него, получаем многочлен $f_i(x) = \prod_{\nu \neq i} (x - a_\nu) / \prod_{\nu \neq i} (a_i - a_\nu)$ со значениями $f_i(a_\nu) = 0$ при $\nu \neq i$ и $f_i(a_i) = 1$. Искомый многочлен Лагранжа имеет вид

$$\sum_{i=0}^{n} b_i f_i(x) = \sum_{i=0}^{n} b_i \prod_{\nu \neq i} \frac{x - a_\nu}{a_i - a_\nu}\,.$$

2.3.1. Присоединение корней. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу[1] $\mathbb{Z}/(n)$. А именно, обозначим через $(f) = \{fh \mid h \in \Bbbk[x]\}$ подкольцо в $\Bbbk[x]$, состоящее из всех многочленов, делящихся на f. Сдвиги этого подкольца на всевозможные элементы $g \in \Bbbk[x]$ обозначаются

$$[g]_f = g + (f) = \{g + fh \mid h \in \Bbbk[x]\}$$

и называются *классами вычетов* по модулю f. Два таких класса $[g_1]_f$ и $[g_2]_f$ либо не пересекаются, либо совпадают, причём последнее означает, что $g_1 - g_2 \in (f)$.

Упражнение 2.10. Убедитесь, что отношение $g_1 \equiv g_2 \pmod f$, означающее, что $g_1 - g_2 \in (f)$, является эквивалентностью[2].

Множество классов вычетов обозначается через $\Bbbk[x]/(f)$. Сложение и умножение в нём задаётся формулами $[g]_f + [h]_f \stackrel{\text{def}}{=} [g + h]_f$, $[g]_f \cdot [h]_f \stackrel{\text{def}}{=} [gh]_f$.

[1] См. n° 1.4 на стр. 27.
[2] См. опр. 0.1 на стр. 9.

Упражнение 2.11. Проверьте корректность[1] этого определения и выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулём кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей — класс $[1]_f = 1 + (f)$. Так как константы не делятся на многочлены положительной степени, классы всех констант $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$ гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому классы чисел $c \in \Bbbk$ обычно записываются как c, а не $[c]_f$.

Упражнение 2.12. Покажите, что для любого $\alpha \in \Bbbk$ кольцо $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Каждый многочлен $g \in \Bbbk[x]$ однозначно представляется в виде $g = fh + r$, где $\deg r < \deg f$. Поэтому в каждом классе $[g]_f$ есть ровно один многочлен $r \in [g]_f$ с $\deg(r) < \deg(f)$. Таким образом, каждый элемент кольца $\Bbbk[x]/(f)$ однозначно записывается в виде

$$[a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}\,,\ \text{где } \vartheta = [x]_f \text{ и } a_i \in \Bbbk\,.$$

Класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, ибо

$$f(\vartheta) = f\left([x]_f\right) = [f(x)]_f = [0]_f\,.$$

В таких обозначениях сложение и умножение вычетов представляет собою формальное сложение и умножение записей $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$ по стандартным правилам раскрытия скобок и приведения подобных слагаемых с учётом соотношения $f(\vartheta) = 0$. По этой причине кольцо $\Bbbk[x]/(f)$ часто обозначают через $\Bbbk[\vartheta]$, где $f(\vartheta) = 0$, и называют *расширением* поля $\Bbbk$ путём *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$.

Например, кольцо $\mathbb{Q}[x]/(x^2-2)$ можно воспринимать как множество формальных записей вида $a + b\sqrt{2}$, где $\sqrt{2} \stackrel{\text{def}}{=} [x]$. Сложение и умножение таких записей происходит по стандартным правилам раскрытия скобок с учётом того, что $\sqrt{2}\cdot\sqrt{2} = 2$:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (cb + ad)\sqrt{2}\,.$$

Упражнение 2.13. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$.

Предложение 2.5
Пусть $\Bbbk$ — произвольное поле и $f \in \Bbbk[x]$. Кольцо $\Bbbk[x]/(f)$ является полем если и только если f неприводим в $\Bbbk[x]$.

Доказательство. Если $f = gh$, где степени f и g строго меньше $\deg f$, ненулевые классы $[g], [h]$ являются делителями нуля в кольце $\Bbbk[x]/(f)$, что невозможно в поле. Если f неприводим, то $\text{нод}(f, g) = 1$ для любого $g \notin (f)$, и значит, $fh + gq = 1$ для некоторых $h, q \in \Bbbk[x]$, откуда $[q]\cdot[g] = [1]$, т. е. класс $[g]$ обратим в $\Bbbk[x]/(f)$. □

Упражнение 2.14. Найдите $(1+\vartheta)^{-1}$ в поле $\mathbb{Q}[\vartheta]$, где $\vartheta^2 + \vartheta + 1 = 0$.

[1] Т. е. независимость классов $[g+h]_f$ и $[gh]_f$ от выбора представителей $g \in [g]_f$ и $h \in [h]_f$.

Теорема 2.1
Для любого поля $\Bbbk$ и произвольного $f \in \Bbbk[x]$ существует такое поле $\mathbb{F} \supset \Bbbk$, что в кольце $\mathbb{F}[x]$ многочлен f разлагается в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\Bbbk$ и каждого многочлена степени $< n$ из $\Bbbk[x]$ искомое поле имеется[1]. Рассмотрим многочлен f степени n. Если он приводим, т. е. $f = gh$ и $\deg g, \deg h < n$, то по индуктивному предположению существует поле $\mathbb{L} \supset \Bbbk$ над которым g полностью разлагается на линейные множители, а также поле $\mathbb{F} \supset \mathbb{L}$ над которым полностью разлагается h, а с ним и f. Если f неприводим, рассмотрим поле $\mathbb{L} = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ в качестве классов констант, и многочлен f делится в $\mathbb{L}[x]$ на $(x - \vartheta)$, где $\vartheta = [x]_f \in \mathbb{L}$. Частное от этого деления имеет степень $n-1$ и по индукции раскладывается на линейные множители над некоторым полем $\mathbb{F} \supset \mathbb{L}$. Тем самым и f полностью раскладывается над $\mathbb{F}$. □

Теорема 2.2 (китайская теорема об остатках)
Пусть многочлен $f = f_1 \dots f_m \in \Bbbk[x]$ является произведением m попарно взаимно простых многочленов $f_i \in \Bbbk[x]$. Тогда отображение

$$\varphi : \frac{\Bbbk[x]}{(f)} \to \frac{\Bbbk[x]}{(f_1)} \times \dots \times \frac{\Bbbk[x]}{(f_m)}, \quad [g]_f \mapsto ([g]_{f_1}, \dots, [g]_{f_m}), \tag{2-11}$$

корректно определено и является изоморфизмом колец.

Доказательство. Проверка того, что отображение (2-11) корректно определено[2], является гомоморфизмом колец и имеет нулевое ядро, дословно та же, что в n° 1.7 на стр. 34, и мы оставляем её читателям. Докажем, что гомоморфизм (2-11) сюръективен. Для каждого i обозначим через $F_i = f/f_i$ произведение всех многочленов f_ν кроме i-го. Так как f_i взаимно прост с каждым f_ν при $\nu \neq i$, многочлены F_i и f_i взаимно просты по лем. 1.3 на стр. 26. Поэтому существует такой многочлен $h_i \in \Bbbk[x]$, что $[1]_{f_i} = [F_i]_{f_i}[h_i]_{f_i} = [F_i h_i]_{f_i}$ в $\Bbbk[x]/(f_i)$. Мы заключаем, что класс многочлена $F_i h_i$ нулевой во всех кольцах $\Bbbk[x]/(f_\nu)$ с $\nu \neq i$ и равен единице в $\Bbbk[x]/(f_i)$. Поэтому для любого набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f_i)$ многочлен $g = \sum_i r_i F_i h_i$ таков, что $[g]_{f_i} = [r_i]_{f_i}$ сразу для всех i. □

2.3.2. Общие корни нескольких многочленов $f_1, \dots, f_m \in \Bbbk[x]$ с коэффициентами в поле $\Bbbk$ искать обычно проще, чем корни каждого из многочленов f_i в отдельности, так как общие корни являются корнями многочлена нод$(f_1, \dots, f_m)$, который находится при помощи алгоритма Евклида и как правило имеет меньшую степень, чем любой из f_i. Отметим, что при нод$(f_1, \dots, f_m) = 1$ многочлены f_i не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$, поскольку существуют такие $h_i \in \Bbbk[x]$, что $f_1 h_1 + \dots + f_m h_m = 1$.

2.3.3. Кратные корни. Пусть $\Bbbk$ — произвольное поле. Число $\alpha \in \Bbbk$ называется m-кратным корнем многочлена $f \in \Bbbk[x]$, если $f(x) = (x-\alpha)^m \cdot g(x)$ и $g(\alpha) \neq 0$. Корни кратности $m = 1$ называются *простыми*, а более высоких кратностей — *кратными*.

Предложение 2.6
Число α является кратным корнем многочлена f если и только если $f(\alpha) = f'(\alpha) = 0$.

[1] Заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \Bbbk$.
[2] Т. е. $\varphi([g]_f) = \varphi([h]_f)$ при $[g]_f = [h]_f$.

Доказательство. Если корень α кратный, то $f(x) = (x-\alpha)^2 g(x)$. Дифференцируя, получаем

$$f'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big)\,,$$

откуда $f'(\alpha) = 0$. Если корень α не кратный, то $f(x) = (x-\alpha)g(x)$, где $g(\alpha) \neq 0$. Подставляя $x = \alpha$ в $f'(x) = (x-\alpha)g'(x) + g(x)$, получаем $f'(\alpha) = g(\alpha) \neq 0$. □

Предложение 2.7
Если $\operatorname{char}\Bbbk = 0$, то $\alpha \in \Bbbk$ является m-кратным корнем многочлена $f \in \Bbbk[x]$ если и только если

$$f(\alpha) = \frac{d}{dx}f(\alpha) = \ldots = \frac{d^{m-1}}{dx^{m-1}}f(\alpha) = 0 \quad \text{и} \quad \frac{d^m}{dx^m}f(\alpha) \neq 0\,.$$

Доказательство. Если $f(x) = (x-\alpha)^m g(x)$, то $f'(x) = (x-\alpha)^{m-1}\big(mg(x) + (x-\alpha)g'(x)\big)$. При $g(\alpha) \neq 0$ второй множитель в последнем равенстве ненулевой при $x = \alpha$. Поэтому α является m-кратным корнем f если и только если α является $(m-1)$-кратным корнем f'. □

2.3.4. Сепарабельность. Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если он взаимно прост со своей производной. Это равносильно отсутствию у f кратных корней в любом кольце $K \supset \Bbbk$. В самом деле, если $\deg \operatorname{нод}(f, f') \geqslant 1$ или $f' = 0$, то по теор. 2.1 $\operatorname{нод}(f, f')$ или, соответственно, сам f имеет корень в некотором поле $\mathbb{F} \supset \Bbbk$, и по предл. 2.6 этот корень кратный для f. Наоборот, если $\operatorname{нод}(f, f') = 1$, то $pf + qf' = 1$ для подходящих $p, q \in \Bbbk[x]$, и поэтому f и f' не могут одновременно обратиться в нуль ни в каком расширении $K \supset \Bbbk$.

Пример 2.6 (сепарабельность и несепарабельность неприводимых многочленов)
Если многочлен $f \in \Bbbk[x]$ неприводим, то он взаимно прост со всеми ненулевыми многочленами меньшей степени. Поэтому $\operatorname{нод}(f, f') = 1$, если $f' \neq 0$ в $\Bbbk[x]$. Поскольку над полем характеристики нуль каждый многочлен положительной степени имеет ненулевую производную, все неприводимые многочлены над таким полем сепарабельны. Если $\operatorname{char}\Bbbk = p > 0$, то $f' = 0$ если и только если[1] $f(x) = g(x^p)$ для некоторого $g(x) = b_m x^m + \ldots + b_1 x + b_0 \in \Bbbk[x]$. Так как в характеристике p возведение в p-тую степень является гомоморфизмом колец[2] и тождественно действует на простом поле $\mathbb{F}_p$, для любого многочлена g с коэффициентами в простом конечном поле $\Bbbk = \mathbb{F}_p$ выполняются равенства

$$g(x^p) = b_m x^{pm} + \ldots + b_1 x^p + b_0 = b_m^p x^{pm} + \ldots + b_1^p x^p + b_0^p = \\ = (b_m x^m + \ldots + b_1 x + b_0)^p = g^p(x)\,.$$

Поэтому в $\mathbb{F}_p[x]$ каждый многочлен с нулевой производной является чистой p-той степенью и тем самым приводим. Мы заключаем, что в $\mathbb{F}_p[x]$ все неприводимые многочлены тоже сепарабельны.

Упражнение 2.15*. Покажите, что неприводимый многочлен над любым конечным полем сепарабелен.

Неприводимый многочлен над бесконечным полем положительной характеристики не обязательно сепарабелен. Например, можно показать, что над полем $\Bbbk = \mathbb{F}_p(t)$ рациональных функций от одной переменной t с коэффициентами в поле $\mathbb{F}_p$ многочлен $f(x) = x^p - t$ неприводим, но поскольку $f' = 0$, многочлен f не сепарабелен.

[1] См. прим. 2.3 на стр. 38.
[2] См. прим. 1.7 на стр. 28.

2.4. Поле комплексных чисел $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2+1)$ получается из поля $\mathbb{R}$ присоединением корня неприводимого над $\mathbb{R}$ многочлена $t^2+1=0$ и состоит из элементов $x+iy$, где $x, y \in \mathbb{R}$, а $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2=-1$. Обратным к ненулевому числу $x+yi$ является число

$$\frac{1}{x+yi} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}\cdot i\,.$$

Комплексное число $z = x+yi$ удобно изображать на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат (x,y) *радиус вектором* z, ведущим из начала координат в точку $z=(x,y)$, как на рис. 2⋄1. Координаты (x,y) называются *действительной* и *мнимой* частями числа $z \in \mathbb{C}$ и обозначаются через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$, а длина $|z| \stackrel{\text{def}}{=} \sqrt{x^2+y^2}$ называется *модулем* или *абсолютной величиной* комплексного числа z. Множество всех таких $\vartheta \in \mathbb{R}$, что поворот плоскости вокруг нуля на угол ϑ совмещает направление координатной оси x с направлением вектора z, называется *аргументом* числа z и обозначается $\mathrm{Arg}(z) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где $\alpha \in \mathbb{R}$ — ориентированная длина какой-нибудь дуги единичной окружности, ведущей из точки $(1,0)$ в точку[1] $z/|z|$. Таким образом, каждое комплексное число имеет вид $z = |z|\cdot(\cos\alpha + i\cdot\sin\alpha)$, где $\alpha \in \mathrm{Arg}(z)$, и $\mathrm{Re}(z) = |z|\cdot\cos\alpha$, а $\mathrm{Im}(z) = |z|\cdot\sin\alpha$.

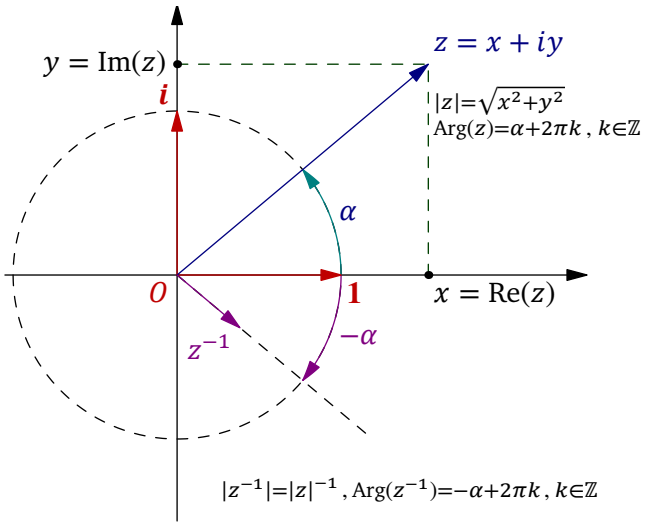


Рис. 2⋄1. Числа $z = |z|\cdot(\cos\alpha + i\sin\alpha)$ и $z^{-1} = |z|^{-1}(\cos\alpha - i\sin\alpha)$.

На множестве векторов в $\mathbb{R}^2$ имеется своя внутренняя операция сложения векторов, относительно которой радиус векторы точек $z \in \mathbb{R}^2$ образуют абелеву группу. Зададим на множестве векторов в $\mathbb{R}^2$ операцию умножения требованием, чтобы длины перемножаемых векторов перемножались, а аргументы — складывались, т. е.

$$\begin{gathered} |z_1 z_2| = |z_1|\cdot|z_2| \\ \mathrm{Arg}(z_1 z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2) \stackrel{\text{def}}{=} \{\vartheta_1+\vartheta_2 \mid \vartheta_1 \in \mathrm{Arg}(z_1),\ \vartheta_2 \in \mathrm{Arg}(z_2)\}\,. \end{gathered} \tag{2-12}$$

Упражнение 2.16. Проверьте корректность нижней формулы, т. е. убедитесь, что любые два числа в правом множестве отличаются на целое кратное 2π.

[1] Любые две таких дуги отличаются друг от друга на целое число оборотов, а «ориентированность» означает, что длину дуги следует брать со знаком «+», если движение вдоль неё происходит против часовой стрелки, и со знаком «−» если по часовой стрелке.

Лемма 2.1
Множество радиус векторов точек z евклидовой координатной плоскости $\mathbb{R}^2$ с описанными выше сложением и умножением является полем. Отображение $\mathbb{C} \to \mathbb{R}^2$, сопоставляющее комплексному числу $x + iy \in \mathbb{C}$ точку $z = (x, y) \in \mathbb{R}^2$, является изоморфизмом полей.

Доказательство. Радиус векторы точек плоскости образуют абелеву группу по сложению. Очевидно также, что ненулевые векторы образуют абелеву группу относительно операции умножения, задаваемой формулами (2-12). Единицей этой группы служит единичный направляющий вектор оси x, а обратный к ненулевому z вектор z^{-1} имеет $|z^{-1}| = 1/|z|$ и $\operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z)$ (см. рис. 2⋄1). Для проверки дистрибутивности заметим, что для любого $a \in \mathbb{R}^2$ отображение

$$a : \mathbb{R}^2 \to \mathbb{R}^2, \quad z \mapsto az,$$

состоящее в умножении всех векторов на a по формулам (2-12), представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b + c) = ab + ac$ утверждает, что поворотная гомотетия перестановочна со сложением векторов[2]. Но это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы. Таким образом, радиус векторы точек евклидовой координатной плоскости $\mathbb{R}^2$ образуют поле. Векторы, параллельные горизонтальной координатной оси, составляют в нём подполе, изоморфное полю $\mathbb{R}$. Если обозначить через i единичный направляющий вектор вертикальной координатной оси, то радиус вектор каждой точки $z = (x, y) \in \mathbb{R}^2$ однозначно запишется в виде $z = x + iy$, где числа $x, y \in \mathbb{R}$ понимаются как векторы, параллельные горизонтальной координатной оси, а сложение и умножение происходят по правилам поля $\mathbb{R}^2$. При этом $i^2 = -1$ и для любых векторов $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ выполняются равенства $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ и

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1),$$

которыми описывается сложение и умножение вычетов $[x + yt]$ в поле $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$. □

2.4.1. Комплексное сопряжение. Числа $z = x + iy$ и $\overline{z} \stackrel{\text{def}}{=} x - iy$ называются *комплексно сопряжёнными*. В терминах комплексного сопряжения обратное к ненулевому $z \in \mathbb{C}$ число можно записать как $z^{-1} = \overline{z}/|z|^2$. На геометрическом языке комплексное сопряжение $z \mapsto \overline{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси x. С алгебраической точки зрения сопряжение является инволютивным[3] автоморфизмом поля $\mathbb{C}$, т. е. $\overline{\overline{z}} = z$ для всех $z \in \mathbb{C}$, и $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$ для всех $z_1, z_2 \in \mathbb{C}$.

2.4.2. Тригонометрия. Почти вся школьная тригонометрия представляет собою трудно для восприятия закодированную запись заурядных алгебраических вычислений с комплексными числами, лежащими на единичной окружности.

Пример 2.7 (формулы сложения аргументов)
Произведение $z_1 z_2$ чисел $z_1 = \cos\varphi_1 + i\sin\varphi_1$ и $z_2 = \cos\varphi_2 + i\sin\varphi_2$ согласно лем. 2.1 равно $\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)$, а лобовое перемножение этих чисел путём раскрытия скобок

[1] *Поворотной гомотетией* относительно точки 0 на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки 0 и растяжения в ϱ раз относительно 0. Так такие растяжения и повороты коммутируют друг с другом, неважно в каком порядке выполняется эта композиция.

[2] Т. е. является гомоморфизмом аддитивных групп.

[3] Эндоморфизм $\iota : X \to X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \mathrm{Id}_X$. По предл. 0.4 на стр. 14 всякая инволюция автоматически биективна.

даёт $z_1z_2 = (\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)$, откуда $\cos(\varphi_1+\varphi_2) = \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2$ и $\sin(\varphi_1+\varphi_2) = \cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2$. Таким образом мы *доказали* тригонометрические формулы сложения аргументов.

Пример 2.8 (тригонометрические функции кратных углов)
По лем. 2.1 число $z = \cos\varphi + i\sin\varphi \in \mathbb{C}$ имеет $z^n = \cos(n\varphi) + i\sin(n\varphi)$. Раскрывая скобки в биноме $(\cos\varphi + i\sin\varphi)^n$ по форм. (0-8) на стр. 7, получаем равенство

$$\begin{aligned}\cos(n\varphi) + i\sin(n\varphi) &= (\cos\varphi + i\sin\varphi)^n = \\ &= \cos^n\varphi + i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi - i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \ldots = \\ &= \left(\binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots\right) + \\ &\quad + i\cdot\left(\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\right)\end{aligned}$$

заключающее в себе сразу все мыслимые формулы для кратных углов:

$$\cos(n\varphi) = \binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots$$
$$\sin(n\varphi) = \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots$$

Например, $\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\cdot\sin^2\varphi = 4\cos^3\varphi - 3\cos^2\varphi$.

Упражнение 2.17. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

2.4.3. Корни из единицы и круговые многочлены. Решим в поле $\mathbb{C}$ уравнение $z^n = 1$. Сравнивая модули левой и правой части, заключаем, что $|z| = 1$. Сравнивая аргументы, получаем $n\operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$. С точностью до прибавления целых кратных 2π существует ровно n различных вещественных чисел, попадающих при умножении на n в множество $\{2\pi k \mid k \in \mathbb{Z}\}$. Это все геометрически различные углы $2\pi k/n$ с $0 \leqslant k \leqslant n-1$. Мы заключаем, что уравнение $z^n = 1$ имеет ровно n корней

$$\zeta_k = \cos(2\pi k/n) + i\sin(2\pi k/n), \quad \text{где} \quad k = 0, 1, \ldots, (n-1), \tag{2-13}$$

расположенных в вершинах правильного n-угольника, вписанного в единичную окружность так, что его вершина ζ_0 находится в точке 1, см. рис. 2⋄2 и рис. 2⋄3.

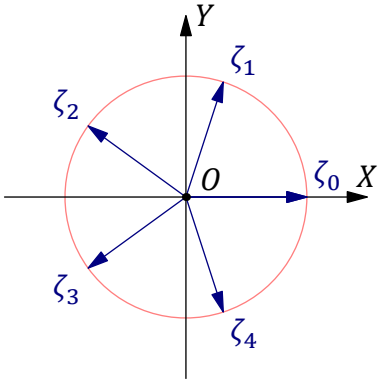


Рис. 2⋄2. Группа $\boldsymbol{\mu}_5$.

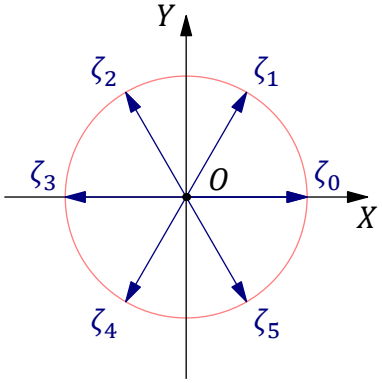


Рис. 2⋄3. Группа $\boldsymbol{\mu}_6$.

Корни (2-13) образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-й степени из единицы*. Корень $\zeta \in \boldsymbol{\mu}_n$ называются *первообразным корнем* степени n из единицы, если все остальные элементы группы $\boldsymbol{\mu}_n$ представляются в виде ζ^k с $k \in \mathbb{N}$. Например, первообразным является корень $\zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$, имеющий наименьший положительный аргумент. Но бывают и другие: на рис. 2⋄2 все четыре отличных от 1 элемента группы $\boldsymbol{\mu}_5$ являются первообразными корнями, тогда как в группе $\boldsymbol{\mu}_6$ на рис. 2⋄3 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1} = \zeta_1^5$. Множество всех первообразных корней обозначается через $R_n \subset \boldsymbol{\mu}_n$.

Упражнение 2.18. Покажите, что $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n) \in R_n$ если и только если $\text{нод}(k, n) = 1$.

Приведённый многочлен $\Phi_n(z) = \prod_{\zeta \in R_n}(z - \zeta)$, корнями которого являются все первообразные корни n-й степени из единицы и только они, называется n-тым *круговым* или *циклотомическим* многочленом. Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z-\zeta_1)(z-\zeta_2)(z-\zeta_3)(z-\zeta_4) = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z-\zeta_1)(z-\zeta_4) = z^2 - z + 1\,.$$

Упражнение 2.19*. Попытайтесь доказать, что при всех $n \in \mathbb{N}$ многочлен Φ_n имеет целые коэффициенты и неприводим[1] в $\mathbb{Q}[x]$.

Пример 2.9 (уравнение $z^n = a$)
Число $z = |z| \cdot (\cos\varphi + i\sin\varphi) \in \mathbb{C}$ является корнем уравнения $z^n = a$ если и только если $|z|^n = |a|$ и $n\varphi \in \operatorname{Arg}(a)$. При $a \neq 0$ имеется ровно n таких чисел. Они выражаются через $r = |a|$ и $\alpha \in \operatorname{Arg} a$ по формуле

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\alpha + 2\pi k}{n} + i\,\sin\frac{\alpha + 2\pi k}{n}\right), \quad 0 \leqslant k \leqslant n-1\,,$$

и располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ с центром в нуле так, что радиус вектор одной из его вершин образует с осью x угол α/n.

2.5. Конечные поля можно строить присоединяя к $\mathbb{F}_p = \mathbb{Z}/(p)$ корень какого-нибудь неприводимого многочлена $f \in \mathbb{F}_p[x]$. Если $\deg f = n$, то получающееся таким образом поле вычетов $\mathbb{F}_p[x]/(f)$ состоит из p^n элементов вида $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$, где $a_i \in \mathbb{F}_p$ и $f(\vartheta) = 0$.

Пример 2.10 (поле $\mathbb{F}_9$)
Многочлен $x^2 + 1 \in \mathbb{F}_3[x]$ неприводим, так как не имеет корней в $\mathbb{F}_3$. Присоединяя к $\mathbb{F}_3$ его корень, получаем поле $\mathbb{F}_9 \stackrel{\text{def}}{=} \mathbb{F}_3[x]/(x^2+1)$, состоящее из девяти элементов вида $a + bi$, где $a, b \in \mathbb{F}_3 = \{-1, 0, 1\}$ и $i^2 = -1$. Расширение $\mathbb{F}_3 \subset \mathbb{F}_9$ похоже на расширение $\mathbb{R} \subset \mathbb{C}$. Аналогом комплексного сопряжения в поле $\mathbb{F}_9$ является гомоморфизм Фробениуса[2] $F_3 : \mathbb{F}_9 \to \mathbb{F}_9, z \mapsto z^3$, тождественно действующий на простом подполе $\mathbb{F}_3 \subset \mathbb{F}_9$ и переводящий i в $-i$.

Упражнение 2.20. Составьте для поля $\mathbb{F}_9$ таблицы умножения и обратных элементов, перечислите в $\mathbb{F}_9$ все квадраты и кубы и убедитесь, что мультипликативная группа $\mathbb{F}_9^\times$ изоморфна $\boldsymbol{\mu}_8$.

[1] Т. е. не являются произведениями многочленов строго меньшей степени.
[2] См. прим. 1.10 на стр. 32.

Пример 2.11 (поле $\mathbb{F}_4$)
Многочлен $x^2+x+1 \in \mathbb{F}_2[x]$ неприводим, так как не имеет корней в $\mathbb{F}_2$. Присоединяя к $\mathbb{F}_2$ его корень, получаем поле $\mathbb{F}_4 \stackrel{\text{def}}{=} \mathbb{F}_2[x]/(x^2+x+1)$, состоящее из 0, 1, $\omega = [x]$ и $1+\omega = \omega^2 = \omega^{-1}$, причём[1] $\omega^2+\omega+1 = 0$. Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ тоже похоже на $\mathbb{R} \subset \mathbb{C}$, если понимать второе расширение как результат присоединения к $\mathbb{R}$ первообразного комплексного кубического корня ω из единицы, который также удовлетворяет уравнению $\omega^2+\omega+1=0$. В поле $\mathbb{F}_4$ аналогом комплексного сопряжения $\mathbb{C} \to \mathbb{C}$, переводящего $\omega \in \mathbb{C}$ в $\overline{\omega} = \omega^2$, также является гомоморфизм Фробениуса[2] $F_2 : \mathbb{F}_4 \to \mathbb{F}_4$, $z \mapsto z^2$, который тождественно действует на простом подполе $\mathbb{F}_2 \subset \mathbb{F}_4$ и переводит корни многочлена x^2+x+1 друг в друга.

Упражнение 2.21. Убедитесь, что мультипликативная группа $\mathbb{F}_4^\times$ изоморфна $\boldsymbol{\mu}_3$.

Теорема 2.3
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ существует конечное поле $\mathbb{F}_q$ из $q = p^n$ элементов.

Доказательство. Рассмотрим в $\mathbb{F}_p[x]$ многочлен $f(x) = x^q - x$. По теор. 2.1 существует такое поле $\mathbb{F} \supset \mathbb{F}_p$, что f полностью раскладывается в $\mathbb{F}[x]$ в произведение q линейных множителей. Так как $f'(x) = -1$, многочлен f сепарабелен[3], и все эти множители различны. Таким образом, в поле $\mathbb{F}$ имеется ровно q таких чисел α, что $\alpha^q = \alpha$. Обозначим множество этих чисел через $\mathbb{F}_q$ и покажем, что $\mathbb{F}_q \subset \mathbb{F}$ является подполем. Очевидно, что $0, 1 \in \mathbb{F}$ лежат в $\mathbb{F}_q$. Если $\alpha \in \mathbb{F}_q$, то $\alpha^{-1} \in \mathbb{F}_q$, так как $\bigl(\alpha^{-1}\bigr)^q = \bigl(\alpha^q\bigr)^{-1} = \alpha^{-1}$, и $-\alpha \in \mathbb{F}_q$, так как $(-\alpha)^q = -\alpha^q = -\alpha$ при $p \neq 2$, а в характеристике два $-\alpha = \alpha$. Если $\alpha, \beta \in \mathbb{F}_q$, то $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, т. е. $\alpha\beta \in \mathbb{F}_q$. Поскольку $\operatorname{char}\mathbb{F} = p$, в поле $\mathbb{F}$ выполняется равенство[4] $(\alpha+\beta)^p = \alpha^p+\beta^p$. Применяя его n раз, заключаем, что $(\alpha+\beta)^q = (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$ для всех $\alpha, \beta \in \mathbb{F}_q$, откуда $\alpha+\beta \in \mathbb{F}_q$. □

Упражнение 2.22. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

2.5.1. Конечные мультипликативные подгруппы поля. Рассмотрим абелеву группу A, операцию в которой будем записывать мультипликативно. Если группа A конечна, то среди степеней любого элемента $b \in A$ встречаются одинаковые, скажем $b^n = b^k$ с $n > k$. Умножая обе части этого равенства на b^{-k}, заключаем, что $b^{n-k} = 1$. Таким образом, для каждого $b \in A$ существует такое $m \in \mathbb{N}$, что $b^m = 1$. Наименьшее из этих m называется *порядком* элемента b и обозначается $\operatorname{ord} b$. Если $\operatorname{ord} b = n$, то элементы $b^0 = 1$, $b^1 = b$, b^2, …, b^{n-1} попарно различны, и каждая целая степень b^k совпадает с одним из них: если $k = nq + r$, где r — остаток от деления k на n, то $b^k = (b^n)^q b^r = b^r$. В частности, $b^m = 0$ если и только если $m \vdots \operatorname{ord} b$.

Упражнение 2.23. Покажите, что порядок любого элемента из конечной абелевой группы A делит $|A|$.

Группа A называется *циклической*, если она исчерпывается целыми степенями какого-нибудь элемента $a \in A$, т. е. $A = \{a^n \mid n \in \mathbb{Z}\}$. Для конечной группы A это равносильно равенству $\operatorname{ord} a = |A|$. Каждый обладающий этим свойством элемент $a \in A$ называется *образующей* циклической группы A. Например, группа $\boldsymbol{\mu}_n \subset \mathbb{C}$ комплексных корней n-й степени из единицы[5] циклическая, и её образующими являются первообразные корни.

[1] Отметим, что $-1 = 1$ в $\mathbb{F}_2$, что позволяет обходиться без минусов.
[2] См. прим. 1.10 на стр. 32.
[3] См. n° 2.3.4 на стр. 45.
[4] См. прим. 1.10 на стр. 32.
[5] См. n° 2.4.3 на стр. 48.

Предложение 2.8
Если порядки элементов мультипликативной абелевой группы A ограничены сверху, то максимальный из них делится на порядок любого элемента $a \in A$.

Доказательство. Достаточно для любых двух элементов $a_1, a_2 \in A$, имеющих порядки m_1, m_2, построить элемент $b \in A$, порядок которого равен нок(m_1, m_2). Если нод$(m_1, m_2) = 1$, положим $b = a_1 a_2$. Тогда $b^{m_1 m_2} = a_1^{m_1 m_2} a_2^{m_2 m_1} = 1$. Если $b^k = 1$, то $a_1^k = a_2^{-k}$, откуда $1 = a_1^{km_1} = a_2^{-km_1}$, и значит, $km_1 \vdots m_2$. Так как m_1 и m_2 взаимно просты, $k \vdots m_2$. Меня ролями a_1 и a_2, заключаем, что $k \vdots m_1$, а значит, $k \vdots m_1 m_2$. Тем самым, $\operatorname{ord}(b) = m_1 m_2 = \text{нок}(m_1, m_2)$.

Пусть нод$(m_1, m_2) \neq 1$. Для каждого простого $p \in \mathbb{N}$ обозначим через $\nu_i(p)$ показатель, с которым p входит в разложение числа m_i на простые множители[1]. Тогда

$$\text{нок}(m_1, m_2) = \prod\nolimits_p p^{\max(\nu_1(p), \nu_2(p))}.$$

Положим $\ell_1 = \prod p^{\nu_1(p)}$ по всем простым $p \in \mathbb{N}$ с $\nu_1(p) > \nu_2(p)$, и $\ell_2 = \text{нок}(m_1, m_2)/\ell_1$. Тогда нод$(\ell_1, \ell_2) = 1$ и $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ для некоторых $k_1, k_2 \in \mathbb{N}$. Элементы $b_1 = a_1^{k_1}$, $b_2 = a_2^{k_2}$ имеют взаимно простые порядки ℓ_1, ℓ_2, и по уже доказанному их произведение $b = b_1 b_2$ имеет порядок $\ell_1 \ell_2 = \text{нок}(m_1, m_2)$. □

Следствие 2.3
Любая конечная подгруппа A в мультипликативной группе $\Bbbk^\times$ произвольного поля $\Bbbk$ является циклической.

Доказательство. Обозначим через m максимальный из порядков элементов группы A. Согласно предл. 2.8, все элементы группы A являются корнями многочлена $x^m - 1 = 0$. Поэтому их не более m и все они исчерпываются степенями имеющегося в A элемента m-того порядка. □

Теорема 2.4
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 2.3 на стр. 50.

Доказательство. Пусть поле $\mathbb{F}$ имеет характеристику p и состоит из q элементов. По сл. 2.3 мультипликативная группа $\mathbb{F}^\times$ является циклической. Обозначим её образующую через $\zeta \in \mathbb{F}^\times$. Тогда $\mathbb{F} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$ и $\zeta^{q-1} = 1$. Чтобы доказать теорему, построим ещё одно поле из q элементов, изоморфное как полю $\mathbb{F}$, так и подходящему полю из теор. 2.3. Для этого обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен минимальной степени с корнем ζ.

Упражнение 2.24. Убедитесь, что такой многочлен g существует, неприводим в $\mathbb{F}_p[x]$ и делит все многочлены $f \in \mathbb{F}_p[x]$ с корнем ζ.

Из упражнения вытекает, что кольцо $\mathbb{F}_p[x]/(g)$ является полем, а правило $[h]_g \mapsto h(\zeta)$ корректно задаёт ненулевой гомоморфизм колец $\mathbb{F}_p[x]/(g) \to \mathbb{F}$. Он инъективен по предл. 1.3 на стр. 31 и сюръективен, так как все ζ^m содержатся в его образе. Тем самым, $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$. В частности, поле $\mathbb{F}$ состоит из $q = p^n$ элементов $a_{n-1}\zeta^{n-1} + \dots + a_1\zeta + a_0$, где $a_i \in \mathbb{F}_p$, $n = \deg g$.

Так как ζ является корнем многочлена $f(x) = x^q - x$, из упр. 2.24 вытекает, что $f = gu$ для некоторого $u \in \mathbb{F}_p[x]$. Подставляя в это равенство q элементов поля $\mathbb{F}_q$, построенного в теор. 2.3 и состоящего в точности из q корней многочлена f, мы заключаем, что хотя бы один

[1] См. упр. 1.8 на стр. 26.

из них — назовём его $\xi \in \mathbb{F}_q$ — является корнем многочлена g. Правило $[h]_g \mapsto h(\xi)$ корректно задаёт вложение полей $\mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

Следствие 2.4 (из доказательства теор. 2.4)
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ в $\mathbb{F}_p[x]$ имеется неприводимый многочлен степени n. □

Следствие 2.5
Каждое конечное поле $\mathbb{F}$ состоит из p^n элементов, где простое $p = \operatorname{char}\mathbb{F}$, и для каждого $n \in \mathbb{N}$ и простого p имеется единственное с точностью до изоморфизма поле из p^n элементов. □

§3. Дроби и ряды

В этом параграфе мы продолжаем обозначать через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

3.1. Кольца частных. Способ изготовления поля $\mathbb{Q}$ из кольца $\mathbb{Z}$ как множества дробей с целым числителем и ненулевым целым знаменателем[1] применим в любом коммутативном кольце K с единицей. Подмножество $S \subset K$ называется *мультипликативным*, если $1 \in S$ и $st \in S$ для всех $s, t \in S$. Например, множество всех целых неотрицательных степеней q^k любого элемента $q \in K$ мультипликативно[2]. Множество $K^\circ \subset K$, состоящее из всех не делящих нуль ненулевых элементов, тоже мультипликативно. В частности, множество всех ненулевых элементов любого целостного кольца мультипликативно. Каждое мультипликативное подмножество $S \subset K$ задаёт на множестве упорядоченных пар $K \times S$ отношение эквивалентности $\sim_S$, порождённое[3] отождествлениями $(a, s) \sim_S (at, st)$ для всех $t \in S$. Класс эквивалентности пары (a, s) по модулю этого отношения называется *дробью* со знаменателем в S и обозначается a/s. Множество всех таких дробей обозначается KS^{-1} или $K[S^{-1}]$ и называется *кольцом частных* или *локализацией* кольца K со знаменателями в S.

Пример 3.1
Пусть $K = \mathbb{Z}/(6)$ и $S = \{[1], [2], [-2]\}$. Каждая дробь в KS^{-1} имеет представление со знаменателем $[1]$: $[a]/[\pm 2] = [a][\mp 2]/[\pm 2][\mp 2] = [\mp a][2]/[1][2] = [\mp a]/[1]$. В частности, $[0]/[\pm 2] = [0]/[1]$. Далее, $[\pm 2]/[1] = [\pm 2][2]/[1][2] = [\mp 1][2]/[1][2] = [\mp 1]/[1]$. Наконец, $[3]/[1] = [3][2]/[1][2] = = [0]/[2] = [0]/[1]$. Тем самым, KS^{-1} исчерпывается дробями $[0]/[1]$, $[1]/[1]$ и $[-1]/[1]$.

Упражнение 3.1. Убедитесь, что эти три дроби различны.

Обратите внимание, что

$$\frac{[2]}{[1]} = \frac{[-1]}{[1]}\text{, но } [2]\cdot[1] \neq [-1]\cdot[1]\text{, и } \quad \frac{[3]}{[1]} = \frac{[0]}{[1]}\text{, но } [3]\cdot[1] \neq [0]\cdot[1]\,.$$

Лемма 3.1
$a/s = b/t$ в KS^{-1} если и только если $atu = bsu$ в K для некоторого $u \in S$.

Доказательство. Положим $(a, s) \approx (b, t)$, если $atu = bsu$ для некоторого $u \in S$. Двухшаговая цепочка отождествлений $(a, s) \sim_S (atu, stu) = (bsu, tsu) \sim_S (b, t)$ показывает, что отношение $\approx$ содержится в отношении $\sim_S$. Остаётся проверить, что отношение $\approx$ является отношением эквивалентности — тогда оно совпадёт с $\sim_S$ в силу минимальности последнего. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a, s) \approx (b, t)$ и $(b, t) \approx (c, r)$, т. е. существуют такие $u, w \in S$, что $atu = bsu$ и $brw = ctw$. Тогда

$$ar(tuw) = (atu)rw = (bsu)rw = (brw)su = (ctw)su = cs(tuw)\,,$$

т. е. $(a, s) \approx (c, r)$. □

[1] См. прим. 0.5 на стр. 11 и прим. 1.2 на стр. 21.
[2] Мы по определению полагаем $q^0 = 1$.
[3] Т. е. наименьшее по включению отношение эквивалентности $R \subset (K \times S) \times (K \times S)$, содержащее все пары вида $\big((a, s), (at, st)\big)$, где $t \in S$, см. n° 0.4.1 на стр. 11.

Лемма 3.2
Операции $\frac{a}{r} + \frac{b}{s} \stackrel{\text{def}}{=} \frac{as+br}{rs}$ и $\frac{a}{r} \cdot \frac{b}{s} \stackrel{\text{def}}{=} \frac{ab}{rs}$ корректно задают на KS^{-1} структуру коммутативного кольца с единицей $1/1$ и нулём $0/1$.

Доказательство. Так как каждое отождествление $\sim_S$ является цепочкой элементарных отождествлений $(a, r) \sim_S (au, ru)$, где $u \in S$, достаточно проверить, что результаты операций не меняются при замене $\frac{a}{r}$ на $\frac{au}{ru}$, а $\frac{b}{s}$ — на $\frac{bw}{sw}$, где $u, w \in S$, что очевидно:

$$\frac{au}{ru} + \frac{bw}{sw} = \frac{ausw + bwru}{rusw} = \frac{(as+br)\cdot wu}{rs\cdot wu} = \frac{as+br}{rs}$$
$$\frac{au}{ru} \cdot \frac{bw}{sw} = \frac{aubw}{rusw} = \frac{(ab)\cdot wu}{rs\cdot wu} = \frac{ab}{rs}.$$

Проверку выполнения в KS^{-1} всех аксиом коммутативного кольца с единицей мы оставляем читателю в качестве упражнения. □

Следствие 3.1
Кольцо KS^{-1} нулевое если и только если S содержит нуль.

Доказательство. Если $0 \in S$, то любая дробь $a/s = (a\cdot 0)/(s\cdot 0) = 0/0 = (0\cdot 0)/(1\cdot 0) = 0/1$ эквивалентна нулю. С другой стороны, $1/1 = 0/1$ только если существует такой $s \in S$, что $1\cdot 1\cdot s = 0\cdot 1\cdot s = 0$, откуда $s = 0 \in S$. □

Теорема 3.1
Отображение $\iota_S\colon K \to KS^{-1}$, переводящее $a \in K$ в дробь $a/1 \in KS^{-1}$, является гомоморфизмом колец с ядром $\ker \iota_S = \{a \in K \mid \exists\, s \in S\colon as = 0\}$. Образ $\iota_S(s)$ любого элемента $s \in S$ обратим в KS^{-1}. Для любого гомоморфизма $\varphi\colon K \to R$ в целостное кольцо R, переводящего каждый элемент из S в обратимый элемент из R, существует единственный такой гомоморфизм колец $\varphi_S\colon KS^{-1} \to R$, что $\varphi = \varphi_S \circ \iota_S$.

Доказательство. Очевидно, что ι_S является гомоморфизмом. Дробь $\iota_S(a) = a/1$ равна $0/1$ если и только если найдётся такой $s \in S$, что $a\cdot 1\cdot s = 0\cdot 1\cdot s = 0$. Обратным к $\iota_S(s) = s/1$ элементом является дробь $1/s$. Остаётся доказать последнее утверждение. Для продолжения гомоморфизма $\varphi\colon K \to R$ до гомоморфизма $\varphi_S\colon KS^{-1} \to R$ нет иного выбора как положить $\varphi_S(1/s) = 1/\varphi(s)$, так как в кольце R должны выполняться равенства $\varphi_S(1/s)\cdot\varphi_S(s) = \varphi_S\bigl(s\cdot(1/s)\bigr) = \varphi(1) = 1$. Следовательно, искомое продолжение обязано задаваться формулой $\varphi_S(a/s) \stackrel{\text{def}}{=} \varphi(a)/\varphi(s)$. Она корректна, поскольку при замене $\frac{a}{s}$ на $\frac{au}{su}$ с $u \in S$ имеем $\varphi_S\left(\frac{au}{su}\right) = \frac{\varphi(au)}{\varphi(su)} = \frac{\varphi(a)\varphi(u)}{\varphi(s)\varphi(u)} = \frac{\varphi(a)}{\varphi(s)}$. Бесхитростную проверку того, что построенное отображение φ_S перестановочно со сложением и умножением, мы оставляем читателю. □

Упражнение 3.2. Пусть $K = \mathbb{Z}/(30)$, а $S = \{[2^k]_{30} \mid k = 0, \dots, 4\}$. Покажите, что $KS^{-1} \simeq \mathbb{Z}/(15)$.

Пример 3.2 (поле частных целостного кольца)
Если кольцо K не имеет делителей нуля, его ненулевые элементы образуют мультипликативную систему. Кольцо частных со знаменателями в этой системе является полем. Оно называется *полем частных* целостного кольца K и обозначается Q_K. Равенство $a/b = c/d$ в Q_K равносильно равенству $ac = bd$ в K, а гомоморфизм $\iota\colon K \hookrightarrow Q_K$, $a \mapsto a/1$, инъективен, и любой гомоморфизм $\varphi\colon K \to R$ в целостное кольцо R, переводящий все ненулевые элементы из K в обратимые элементы кольца R, единственным способом продолжается до вложения поля частных $\widetilde{\varphi}\colon Q_K \hookrightarrow R$.

Пример 3.3 (поле $\mathbb{Q}$)
Полем частных целостного кольца $\mathbb{Z}$ является поле рациональных чисел $\mathbb{Q} = Q_{\mathbb{Z}}$, которое канонически вкладывается в любое поле характеристики нуль в качестве простого подполя[1].

Пример 3.4 (поле рядов Лорана)
Поле частных кольца формальных степенных рядов $\Bbbk[\![x]\!]$ с коэффициентами в произвольном поле $\Bbbk$ обозначается $\Bbbk(\!(x)\!) \stackrel{\text{def}}{=} Q_{\Bbbk[\![x]\!]}$. Так как любой ряд с ненулевым свободным членом обратим[2] в $\Bbbk[\![x]\!]$, каждая дробь $p(x)\,/\,q(x) \in \Bbbk(\!(x)\!)$ однозначно представляется в виде $x^m h(x)$, где $h \in \Bbbk[\![x]\!]$ имеет ненулевой свободный член, а показатель $m \in \mathbb{Z}$ равен разности показателей младших членов рядов p и q. Иначе говоря, поле $\Bbbk(\!(x)\!)$ состоит из формальных степенных рядов вида $f(x) = \sum_{k \geqslant m(f)} a_k x^k$, в которых допускается конечное число мономов отрицательной степени. Такие ряды называются *рядами Лорана*, а поле $\Bbbk(\!(x)\!)$ — *полем рядов Лорана*. Номер $m(f) \in \mathbb{Z}$ самого левого ненулевого коэффициента ряда Лорана f называется *порядком* ряда f.

3.2. Рациональные функции. Поле частных кольца $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от x. Его элементами являются дроби вида $p(x)/q(x)$ с $p, q \in \Bbbk[x]$.

Предложение 3.1
Если $g = g_1 \ldots g_m$, где $g_i \in \Bbbk[x]$ и $\text{нод}(g_i, g_j) = 1$ при $i \neq j$, то при любом $f \in \Bbbk[x]$ дробь $f\,/\,g$ единственным образом представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \cdots + \frac{f_m}{g_m}, \tag{3-1}$$

где $h \in \Bbbk[x]$ и $\deg f_i < \deg g_i$ при всех i.

Доказательство. Деля f на g с остатком[3], заключаем, что $f/g = h + r/g$, где h — неполное частное, а остаток r имеет степень $\deg r < \deg g$. Если $g = g_1 g_2$ и $\text{нод}(g_1, g_2) = 1$, то $[g_2]_{g_1}$ обратим в $\Bbbk[x]\,/\,(g_1)$. Представим $[r]_{g_1}\,/\,[g_2]_{g_1} = [f_1]_{g_1}$ многочленом f_1 степени $\deg f_1 < \deg g_1$. Тогда $r = f_1 \cdot g_2 + f_2 \cdot g_1$ для некоторого $f_2 \in \Bbbk[x]$. Сравнивая степени, заключаем, что $\deg f_2 < \deg g_2$. Таким образом, $r/g = f_1/g_1 + f_2/g_2$ и к каждой из этих дробей применимо то же рассуждение, если её знаменатель является произведением взаимно простых многочленов. Это доказывает существование разложения (3-1). Для доказательства его единственности, умножим обе части разложения (3-1) на g. Получим равенство вида $f = hg + f_1 G_1 + \ldots + f_m G_m$, где через $G_i = g/g_i$ обозначено произведение всех многочленов g_ν кроме i-го. Так как $\deg(f_1 G_1 + \ldots + f_m G_m) < \deg g$, многочлен h является неполным частным, а $r = f_1 G_1 + \ldots + f_m G_m$ — остатком от деления f на g. Каждый f_i является тем единственным многочленом степени $< \deg g_i$, класс которого в $\Bbbk[x]/(g_i)$ равен $[f]_{g_i}\,/\,[G_i]_{g_i}$. Таким образом, все ингредиенты формулы (3-1) однозначно определяются многочленами f и $g_1, \ldots, g_n$. □

Предложение 3.2
Любую дробь вида $f\,/\,g^m$, в которой $\deg f < \deg g^m = m \deg g$, можно единственным образом представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \cdots + \frac{f_m}{g^m}, \tag{3-2}$$

где $\deg f_i < \deg g$ при всех i.

[1] См. n° 1.5.6 на стр. 32.
[2] См. прим. 2.2 на стр. 37.
[3] См. n° 2.2 на стр. 39.

Доказательство. Представление (3-2) равносильно записи f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \ldots + f_{m-1} g + f_m\,, \tag{3-3}$$

аналогичном записи целого числа f в g-ичной позиционной системе исчисления: f_m является остатком от деления f на g, f_{m-1} — остатком от деления частного $(f - f_m)/g$ на g, f_{m-2} — остатком от деления частного $\left(\frac{f-f_m}{g} - f_{m-1}\right)/g$ на g и т. д. □

3.2.1. Разложение на простейшие дроби. Из предыдущих двух предложений вытекает, что каждая дробь $f/g \in \Bbbk(x)$ допускает *единственное* представление в виде суммы неполного частного от деления f на g и дробей вида p/q^m, где q пробегает неприводимые делители знаменателя g, показатель m меняется от 1 до кратности вхождения q в разложение g на неприводимые множители, и в каждой из таких дробей $\deg p < \deg q$. Такое представление называется *разложением f/g на простейшие дроби* и бывает полезно в практических вычислениях с рациональными функциями.

Пример 3.5
Вычислим 2022-ю производную, а также первообразную[1] от $1/(1+x^2)$. Разложим эту дробь в поле $\mathbb{C}(x)$ на простейшие:

$$\frac{1}{1+x^2} = \frac{\alpha}{1+ix} + \frac{\beta}{1-ix}\,, \quad \text{где} \quad \alpha,\, \beta \in \mathbb{C}\,.$$

Подставляя $x = \pm i$ в равенство $1 = \alpha(1-ix) + \beta(1+ix)$, находим $\alpha = \beta = 1/2$, т. е.

$$\frac{1}{1+x^2} = \frac{1}{2}\left(\frac{1}{1+ix} + \frac{1}{1-ix}\right).$$

Теперь дифференцируем каждое слагаемое:

$$\left(\frac{d}{dx}\right)^{2022} \frac{1}{1+x^2} = \frac{2022!}{2}\left(\frac{(-i)^{2022}}{(1+ix)^{2023}} + \frac{i^{2022}}{(1-ix)^{2023}}\right) =$$

$$= -2022! \cdot \frac{1}{2}\frac{(1-ix)^{2023} + (1+ix)^{2023}}{(1+x^2)^{2023}} = 2022! \cdot \sum_{\nu=0}^{1011} \binom{2023}{2\nu} \cdot \frac{(-1)^{\nu+1} x^{2\nu}}{(1+x^2)^{2023}}\,,$$

и интегрируем каждое слагаемое:

$$\int \frac{dx}{1+x^2} = \frac{1}{2}\int \frac{dx}{1+ix} + \frac{1}{2}\int \frac{dx}{1-ix} = \frac{\ln(1+ix) - \ln(1-ix)}{2i} = \frac{1}{2i}\ln\frac{1+ix}{1-ix} = \operatorname{arctg} x\,.$$

Подчеркнём, что все проделанные вычисления корректно определены в кольце $\mathbb{C}[\![x]\!]$, а все написанные равенства суть равенства между элементами этого кольца[2].

[1] Т. е. такой ряд f без свободного члена, что $f'(x) = 1/(1+x^2)$. Подробнее см. в n° 3.3 на стр. 59.

[2] В частности, последнее равенство вытекает из определения тангенса:

$$\operatorname{tg} t \stackrel{\text{def}}{=} \frac{\sin t}{\cos t} = \frac{1}{i}\cdot\frac{e^{it} - e^{-it}}{e^{it} + e^{-it}} = \frac{1}{i}\cdot\frac{e^{2it} - 1}{e^{2it} + 1} \in \mathbb{C}[\![t]\!]\,.$$

Полагая $\operatorname{tg} t = x$, получаем $e^{2it} = \frac{1+ix}{1-ix}$. Про экспоненту и логарифм мы ещё подробно поговорим в n° 3.3 на стр. 59 ниже.

3.2.2. Разложение рациональной функции в степенной ряд. По теор. 3.1 на стр. 54 существует единственное вложение $\Bbbk(x) \hookrightarrow \Bbbk((x))$, переводящее каждый многочлен в себя. Иначе говоря, каждую рациональную функцию можно разложить в ряд Лорана. Если основное поле $\Bbbk$ алгебраически замкнуто[1], такое разложение описывается довольно явными формулами. Пусть $\deg f < \deg g$ и знаменатель дроби f/g имеет вид:

$$g(x) = 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \prod (1 - \alpha_i x)^{m_i}, \tag{3-4}$$

где все числа $\alpha_i \in \Bbbk$ попарно различны.

Упражнение 3.3. Убедитесь, что числа α_i из разложения (3-4) суть корни многочлена

$$t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n = \prod (t - \alpha_i)^{m_i}.$$

По предл. 3.1 и предл. 3.2 функция f/g является суммой простейших дробей

$$\frac{\beta_{ij}}{(1 - \alpha_i x)^{k_{ij}}}, \tag{3-5}$$

где при каждом i показатели k_{ij} лежат в пределах $1 \leqslant k_{ij} \leqslant m_i$, а $\beta_{ij} \in \Bbbk$.

Если все кратности $m_i = 1$, то разложение на простейшие дроби имеет вид

$$\frac{f(x)}{(1 - \alpha_1 x) \ldots (1 - \alpha_n x)} = \frac{\beta_1}{1 - \alpha_1 x} + \ldots + \frac{\beta_n}{1 - \alpha_n x}.$$

Чтобы найти β_i, умножим обе части на общий знаменатель и подставим $x = \alpha_i^{-1}$. Получим

$$\beta_i = \frac{f\left(\alpha_i^{-1}\right)}{\prod_{v \neq i} \left(1 - (\alpha_v / \alpha_i)\right)} = \frac{\alpha_i^{n-1} f\left(\alpha_i^{-1}\right)}{\prod_{v \neq i} \left(\alpha_i - \alpha_v\right)}. \tag{3-6}$$

Мы заключаем, что когда все $m_i = 1$, дробь f/g является суммой $n = \deg g$ геометрических прогрессий:

$$\frac{f(x)}{g(x)} = \sum \left(\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \ldots + \beta_n \alpha_n^k\right) \cdot x^k, \tag{3-7}$$

где β_i находятся по формулам (3-6).

Простейшая дробь (3-5) с показателем $k_{ij} = m > 1$ раскладывается в ряд при помощи формулы Ньютона для бинома с отрицательным показателем

$$\frac{1}{(1 - x)^m} = \sum_{k \geqslant 0} \frac{(k + m - 1) \ldots (k + 2)(k + 1)}{(m - 1)!} \cdot x^k = \sum_{k \geqslant 0} \binom{k + m - 1}{m - 1} \cdot x^k, \tag{3-8}$$

которая получается $(m-1)$-кратным дифференцированием обеих частей разложения геометрической прогрессии $(1 - x)^{-1} = 1 + x + x^2 + x^3 + \ldots$.

Упражнение 3.4. Убедитесь, что $\left(\frac{d}{dx}\right)^n (1 - x)^{-1} = n! / (1 - x)^{n+1}$.

Таким образом, разложение простейшей дроби (3-5) имеет вид

$$\frac{\beta}{(1 - \alpha_i x)^m} = \beta \sum_{k \geqslant 0} \alpha_i^k \binom{k + m - 1}{m - 1} \cdot x^k. \tag{3-9}$$

[1] Т. е. каждый многочлен из $\Bbbk[x]$ полностью раскладывается в $\Bbbk[x]$ на линейные множители.

3.2.3. Решение линейных рекуррентных уравнений. Предыдущие вычисления можно использовать для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0\,, \tag{3-10}$$

где коэффициенты $a_1, \ldots, a_n \in \mathbb{C}$ — заданные числа. При $k \geqslant n$ уравнению (3-10) удовлетворяют коэффициенты z_k любого степенного ряда вида

$$z_0 + z_1 x + z_2 x^2 + \ldots = \frac{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}}{1 + a_1 x + a_2 x^2 + \ldots + a_n x^k}\,.$$

Если в числителе правой части подобрать коэффициенты $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ так, чтобы первые n коэффициентов $z_0, \ldots, z_{n-1}$ разложения полученной дроби в степенной ряд совпали с первыми n членами последовательности (3-10), то формулы (3-6) и (3-9) дадут явные выражения элементов последовательности z_k через k.

Пример 3.6 (числа Фибоначчи)
Найдём явное выражение через k для элементов последовательности z_k, в которой

$$z_0 = 0\,,\ z_1 = 1 \text{ и } z_k = z_{k-1} + z_{k-2} \text{ при } k \geqslant 2\,.$$

Рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ описывает коэффициенты ряда

$$x + z_2 x^2 + z_3 x^3 + \ldots = \frac{b_0 + b_1 x}{1 - x - x^2}\,,$$

у которого $z_0 = 0$ и $z_1 = 1$. Умножая обе части на знаменатель и сравнивая коэффициенты при x^0 и x^1, заключаем, что $b_0 = 0$, а $b_1 = 1$. Таким образом,

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+ x} + \frac{\beta_-}{1 - \alpha_- x}\,,$$

где $\alpha_\pm = (1 \pm \sqrt{5})/2$ суть корни многочлена $t^2 - t - 1$, а $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$ по формуле (3-6). Разложение $z(x)$ в ряд имеет вид

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \alpha_+ x} - \frac{1}{1 - \alpha_- x}\right) = \sum_{k \geqslant 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k\,,$$

т. е.

$$z_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k \sqrt{5}}\,.$$

Предложение 3.3
Если последовательность чисел $z_k \in \mathbb{C}$ удовлетворяет при $k \geqslant n$ рекуррентному уравнению

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0 \tag{3-11}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, то $z_k = \alpha_1^k \varphi_1(k) + \ldots + \alpha_r^k \varphi_r(k)$, где $\alpha_1, \ldots, \alpha_r$ — это все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \ldots + a_n\,, \tag{3-12}$$

а $\varphi_i(x) \in \mathbb{C}[x]$ и $\deg \varphi_i$ строго меньше кратности соответствующего корня α_i.

[1] Он называется *характеристическим многочленом* рекуррентного уравнения (3-10).

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[\![x]\!]$, коэффициенты которого решают уравнение (3-11), является суммой дробей вида $\beta(1-\alpha x)^{-m}$, где α пробегает различные корни многочлена (3-12), показатель m лежит в пределах от 1 до кратности соответствующего корня α, и для каждой пары α, m комплексное число $\beta = \beta(\alpha, m)$ однозначно вычисляется по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (3-9) коэффициент при x^k у разложения дроби $(1-\alpha x)^{-m}$ в степенной ряд имеет вид $\alpha^k \varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ является многочленом степени $m-1$ от k. □

3.3. Логарифм и экспонента. Всюду в этом разделе мы рассматриваем ряды с коэффициентами в поле $\Bbbk$ характеристики $\operatorname{char}\Bbbk = 0$. В этом случае для любого ряда $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Он называется *первообразной* или *интегралом* от f и обозначается

$$\int f(x)\,dx \stackrel{\text{def}}{=} a_0 x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \dots = \sum_{k\geqslant 1} \frac{a_{k-1}}{k}\,x^k\,. \tag{3-13}$$

Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\ln(1+x) \stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \dots\right)\,dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \dots = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k\,. \tag{3-14}$$

Единственный ряд со свободным членом 1, совпадающий со своей производной, называется *экспонентой* и обозначается

$$e^x \stackrel{\text{def}}{=} \sum_{k\geqslant 0} x^k/k! = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots\,. \tag{3-15}$$

3.3.1. Логарифмирование и экспоненцирование. Обозначим через $N = (x) \subset \Bbbk[\![x]\!]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U = 1+N \subset \Bbbk[\![x]\!]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом. Подстановка в аргумент логарифма вместо $1+x$ произвольного ряда $u(x) \in U$ означает подстановку в логарифмический ряд (3-14) вместо переменной x ряда $u(x) - 1$ без свободного члена и тем самым является алгебраической операцией[1]. Мы получаем отображение *логарифмирования*

$$\ln\colon U \to N\,, \quad u \mapsto \ln u\,. \tag{3-16}$$

Упражнение 3.5. Убедитесь, что $\frac{d}{dx}\ln u = u'/u$ и $\ln(1/u) = -\ln u$ для всех $u \in U$.

Подстановка в экспоненту (3-15) вместо x любого ряда $\tau(x) \in N$ даёт ряд $e^{\tau(x)}$ со свободным членом 1. Мы получаем *экспоненциальное отображение*

$$\exp\colon N \to U\,, \quad \tau \mapsto e^{\tau}\,. \tag{3-17}$$

Лемма 3.3
Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $u'/u = w'/w$ попарно эквивалентны друг другу.

[1] См. n° 2.1.1 на стр. 36.

Доказательство. Первое равенство влечёт за собой все остальные. Поскольку ряды с равными свободными членами совпадают если и только если совпадают их производные, первые два равенства и последние два равенства равносильны друг другу. Остаётся показать, что из последнего равенства следует первое. Но последнее равенство утверждает, что $u'/u - w'/w = (u'w - w'u)/uw = (w/u)\cdot(u/w)' = 0$ откуда $(u/w)' = 0$, т. е. $u/w = \mathrm{const} = 1$. □

Теорема 3.2
Экспоненциальное и логарифмическое отображения (3-17) и (3-16) являются взаимно обратными изоморфизмами абелевых групп, т. е. для любых рядов u, u_1, u_2 из U и τ, τ_1, τ_2 из N выполняются тождества $\ln e^{\tau} = \tau$, $e^{\ln u} = u$, $\ln(u_1u_2) = \ln(u_1) + \ln(u_2)$, $e^{\tau_1+\tau_2} = e^{\tau_1}e^{\tau_2}$.

Доказательство. Равенство $\ln e^{\tau} = \tau$ проверяется сравнением производных от обеих частей:

$$\left(\ln e^{\tau}\right)' = \frac{\left(e^{\tau}\right)'}{e^{\tau}} = \frac{e^{\tau}\tau'}{e^{\tau}} = \tau',$$

а равенство $e^{\ln u} = u$ — сравнением логарифмических производных:

$$\frac{\left(e^{\ln u}\right)'}{e^{\ln u}} = \frac{e^{\ln u}(\ln u)'}{e^{\ln u}} = \frac{u'}{u}.$$

Тем самым, экспоненцирование и логарифмирование являются взаимно обратными биекциями. Ряды $\ln(u_1u_2)$ и $\ln u_1 + \ln u_2$ совпадают, поскольку имеют нулевые свободные члены и равные производные:

$$\left(\ln(u_1u_2)\right)' = \frac{(u_1u_2)'}{u_1u_2} = \frac{u_1'u_2 + u_1u_2'}{u_1u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = \left(\ln u_1 + \ln u_2\right)'.$$

Поэтому логарифмирование — гомоморфизм, а значит, и обратное к нему экспоненцирование — тоже. □

Упражнение 3.6. Докажите в $\Bbbk[\![x,y]\!]$ равенство $e^{x+y} = e^x e^y$ непосредственным сравнением коэффициентов этих двух рядов.

3.3.2. Степенная функция и бином. Если $\mathrm{char}\,\Bbbk = 0$, то для любого $\alpha \in \Bbbk$ определён *биномиальный* ряд с показателем α:

$$(1+x)^{\alpha} \stackrel{\text{def}}{=} e^{\alpha\ln(1+x)}.$$

Подставляя вместо $1+x$ произвольные ряды $u \in U$, мы для любого числа $\alpha \in \Bbbk$ получаем алгебраическую операцию *возведения в α-тую степень* $U \to U$, $u \mapsto u^{\alpha}$, обладающую всеми интуитивно ожидаемыми от степенной функции свойствами. А именно, для любых рядов $u, v \in U$ и чисел $\alpha, \beta \in \Bbbk$ выполняются равенства

$$u^{\alpha}\cdot u^{\beta} = e^{\alpha\ln u}e^{\beta\ln u} = e^{\alpha\ln u+\beta\ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta}$$
$$\left(u^{\alpha}\right)^{\beta} = e^{\beta\ln(u^{\alpha})} = e^{\beta\ln\left(e^{\alpha\ln u}\right)} = e^{\alpha\beta\ln u} = u^{\alpha\beta}$$
$$(uv)^{\alpha} = e^{\alpha\ln(uv)} = e^{\alpha(\ln u+\ln v)} = e^{\alpha\ln u+\alpha\ln v} = e^{\alpha\ln u}\cdot e^{\alpha\ln v} = u^{\alpha}v^{\alpha}.$$

Например, для любого ряда u с единичным свободным членом ряд $u^{1/n}$ представляет собою $\sqrt[n]{u}$ в том смысле, что $\left(u^{1/n}\right)^n = u$. Чтобы явно найти коэффициенты a_i биномиального ряда

$$(1+x)^{\alpha} = a_0 + a_1x + a_2x^2 + \ldots$$

рассмотрим его логарифмическую производную

$$\frac{\bigl((1+x)^\alpha\bigr)'}{(1+x)^\alpha} = \frac{d}{dx}\ln(1+x)^\alpha = \alpha\frac{d}{dx}\ln(1+x) = \frac{\alpha}{1+x}\,.$$

Умножая левую и правую части на $(1+x)^{\alpha+1}$, получаем равенство

$$\bigl(a_1 + 2a_2x + 3a_3x^2 + \ldots\bigr)\cdot(1+x) = \alpha\cdot(1 + a_1x + a_2x^2 + a_3x^3 + \ldots)\,.$$

Сравнивая коэффициенты при x^{k-1} в правой и левой части, приходим к рекуррентному соотношению $ka_k + (k-1)a_{k-1} = \alpha a_{k-1}$, из которого

$$a_k = \frac{\alpha-(k-1)}{k}\cdot a_{k-1} = \frac{(\alpha-(k-1))(\alpha-(k-2))}{k(k-1)}\cdot a_{k-2} = \ldots$$
$$\ldots = \frac{(\alpha-(k-1))(\alpha-(k-2))\cdots(\alpha-1)\alpha}{k!}\,.$$

Стоящая в правой части дробь имеет в числителе и знаменателе по k множителей, представляющих собою последовательно уменьшающиеся на единицу числа: в знаменателе — от k до 1, в числителе — от α до $(\alpha-k+1)$. Эта дробь называется *биномиальным коэффициентом* и обозначается

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{3-18}$$

Таким образом, для любого $\alpha\in\Bbbk$ справедлива *формула Ньютона*

$$(1+x)^\alpha = \sum_{k\geqslant 0}\binom{\alpha}{k}x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3 + \ldots\,.$$

Пример 3.7 (бином с рациональным показателем)
Если $\alpha = n\in\mathbb{N}$, то при $k>n$ в числителе дроби (3-18) появится нулевой сомножитель. Поэтому разложение бинома в этом случае конечно и имеет вид

$$(1+x)^n = 1 + n\,x + \frac{n(n-1)}{2}\,x^2 + \ldots + x^n = \sum_{k=0}^{n}\binom{n}{k}\cdot x^k\,,$$

знакомый нам из форм. (0-8) на стр. 7. При $\alpha = -m$, где $m\in\mathbb{N}$, мы получаем разложение из форм. (3-8) на стр. 57

$$(1+x)^{-m} = 1 - m\,x + \frac{m(m+1)}{2}\,x^2 - \frac{m(m+1)(m+2)}{6}\,x^3 + \ldots = \sum_{k\geqslant 0}(-1)^k\binom{k+m-1}{k}\cdot x^k\,.$$

При $\alpha = 1/n$, где $n\in\mathbb{N}$, формула Ньютона разворачивает в степенной ряд радикал

$$\sqrt[n]{1+x} = 1 + \frac{1}{n}\,x + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)}{2}\,x^2 + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)\left(\frac{1}{n}-2\right)}{6}\,x^3 + \cdots =$$
$$= 1 + \frac{x}{n} - \frac{n-1}{2}\cdot\frac{x^2}{n^2} + \frac{(n-1)(2n-1)}{2\cdot 3}\cdot\frac{x^3}{n^3} - \frac{(n-1)(2n-1)(3n-1)}{2\cdot 3\cdot 4}\cdot\frac{x^4}{n^4} + \cdots$$

Например, при $n = 2$ и $k \geqslant 1$ в качестве коэффициента при x^k получается дробь

$$(-1)^{k-1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-3)}{2^k k!} = \frac{(-1)^{k-1}}{2k} \cdot \frac{1}{4^{k-1}} \cdot \binom{2k-2}{k-1},$$

т. е.

$$\sqrt{1+x} = 1 + \sum\nolimits_{k \geqslant 1} \frac{(-1)^{k-1}}{2k} \cdot \binom{2k-2}{k-1} \cdot \frac{x^k}{4^{k-1}}. \tag{3-19}$$

Пример 3.8 (числа Каталана)
Воспользуемся разложением (3-19) для получения явной формулы для *чисел Каталана*, часто возникающих в комбинаторных задачах. Вычислим произведение $n+1$ чисел

$$a_0 a_1 \ldots a_n, \tag{3-20}$$

делая за один шаг ровно одно из n умножений и заключая перемножаемые числа в скобки. В результате мы расставим n пар скобок в выражении (3-20). Количество различных расстановок скобок, возникающих таким образом, называется n-ым *числом Каталана* c_n. При $n = 1$ есть лишь одна расстановка скобок $(a_0 a_1)$, при $n = 2$ — две $(a_0(a_1 a_2))$ и $((a_0 a_1)a_2)$, при $n = 3$ — пять: $(a_0(a_1(a_2 a_3)))$, $(a_0((a_1 a_2)a_3))$, $((a_0 a_1)(a_2 a_3))$, $((a_0(a_1 a_2))a_3)$, $(((a_0 a_1)a_2)a_3)$. Множество всевозможных расстановок скобок в произведении (3-20) распадается в дизъюнктное объединение n подмножеств, в которых конфигурации наружных скобок имеют вид

$$(a_0(a_1 \ldots a_n)),\ ((a_0 a_1)(a_2 \ldots a_n)),\ \ldots,\ ((a_0 \ldots a_{n-2})(a_{n-1} a_n)),\ ((a_0 \ldots a_{n-1})a_n)$$

и которые состоят, соответственно, из c_{n-1}, $c_1 c_{n-2}$, $c_2 c_{n-3}$, …, $c_{n-2} c_1$, c_{n-1} элементов. Если дополнить последовательность чисел Каталана числом $c_0 \stackrel{\text{def}}{=} 1$, то получится соотношение

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \ldots + c_{n-2} c_1 + c_{n-1} c_0,$$

означающее, что *ряд Каталана* $c(x) \stackrel{\text{def}}{=} \sum_{k \geqslant 0} c_k x^k = 1 + c_1 x + c_2 x^2 + \ldots \in \mathbb{Z}[\![x]\!]$ удовлетворяет уравнению $c(x)^2 = (c(x) - 1)/x$, т. е. является лежащим в кольце $\mathbb{Z}[\![x]\!]$ корнем квадратного трёхчлена $xt^2 - t - 1 = 0$ от переменной t. В поле рядов Лорана $\mathbb{Q}(\!(x)\!) \supset \mathbb{Z}[\![x]\!]$ корни находятся по стандартной школьной формуле $t = (1 \pm \sqrt{1-4x})/2x$. Так как $1 + \sqrt{1-4x}$ не делится на $2x$ в $\mathbb{Z}[\![x]\!]$, корень $(1 + \sqrt{1-4x})/(2x) \notin \mathbb{Z}[\![x]\!]$. Тем самым, $c(x) = (1 - \sqrt{1-4x})/(2x)$, откуда по формуле (3-19)

$$c_k = \frac{1}{k+1} \binom{2k}{k}.$$

Отметим, что даже не сразу понятно, что это число — целое.

3.4. Действие $\mathbb{Q}[[d/dt]]$ на $\mathbb{Q}[t]$. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[\![x]\!]$ от переменной x и кольцо многочленов $\mathbb{Q}[t]$ от переменной t. Обозначим через

$$D = \frac{d}{dt} : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad g \mapsto g',$$

оператор дифференцирования. Оператор D можно подставить вместо переменной x в любой степенной ряд $\Phi(x) = \sum_{k \geqslant 0} \varphi_k x^k \in \mathbb{Q}[\![x]\!]$. Результатом такой подстановки, по определению, является линейное отображение

$$\Phi(D) : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad f \mapsto \sum_{k \geqslant 0} \varphi_k D^k f = \varphi_0 f + \varphi_1 f' + \varphi_2 f'' + \ldots. \tag{3-21}$$

Поскольку каждое дифференцирование уменьшает степень многочлена на единицу, все слагаемые в правой части (3-21) обратятся в нуль при $k > \deg f$. Таким образом, для каждого многочлена $f \in \mathbb{Q}[t]$, правая часть (3-21) является корректно определённым многочленом, каждый коэффициент которого вычисляется конечным числом действий с коэффициентами исходного многочлена f и первыми $\deg(f)$ коэффициентами ряда Φ. Линейность отображения (3-21) означает, что $\Phi(D)(\alpha f + \beta g) = \alpha\Phi(D)f + \beta\Phi(D)g$ для всех $\alpha, \beta \in \mathbb{Q}$ и $f, g \in \mathbb{Q}[t]$. Результатом подстановки оператора D в произведение рядов $\Phi(x)\Psi(x) \in \mathbb{Q}[\![x]\!]$ является *композиция* $\Phi(D) \circ \Psi(D) = \Psi(D) \circ \Phi(D)$ отображений $\Phi(D)$ и $\Psi(D)$.

Упражнение 3.7. Убедитесь в этом.

Таким образом, все отображения вида $\Phi(D)$ перестановочны друг с другом, и для биективности отображения $\Phi(D)$ необходимо и достаточно, чтобы степенной ряд $\Phi(x)$ был обратим[1] в кольце $\mathbb{Q}[\![x]\!]$. В силу линейности значение отображения $\Phi(D)$ на произвольном многочлене выражается через его значения $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ на базисных одночленах t^m:

$$\Phi(D)\left(a_0 + a_1 t + \ldots + a_n t^n\right) = a_0 + a_1\Phi_1(t) + \ldots + a_n\Phi_n(t)\,.$$

Многочлен $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ называется m-тым *многочленом Аппеля* ряда Φ. Его степень не превосходит m, а коэффициенты зависит лишь от первых $m+1$ коэффициентов ряда Φ.

Пример 3.9 (операторы сдвига)
Экспонента $e^D = 1 + D + D^2/2 + D^3/6 + \ldots$ имеет многочлены Аппеля

$$e^D t^m = \sum_{k\geqslant 0} \frac{1}{k!} D^k t^m = \sum_{k\geqslant 0} \frac{m(m-1)\ldots(m-k+1)}{k!}\, t^{m-k} = \sum_{k=0}^{m} \binom{m}{k} t^{m-k} = (t+1)^m\,.$$

Поэтому $e^D : f(t) \mapsto f(t+1)$ — это *оператор сдвига*. Так как ряды e^x и e^{-x} обратны друг другу в $\mathbb{Q}[\![x]\!]$, операторы e^D и e^{-D} тоже обратны друг другу, т. е. $e^{-D} : f(t) \mapsto f(t-1)$.

Упражнение 3.8. Убедитесь, что $e^{\alpha D} : f(t) \mapsto f(t+\alpha)$ при любом $\alpha \in \mathbb{Q}$.

Пример 3.10 (вычисление суммы степеней)
Для произвольно зафиксированного $m \in \mathbb{Z}_{\geqslant 0}$ рассмотрим сумму

$$S_m(n) \stackrel{\text{def}}{=} 0^m + 1^m + 2^m + 3^m + \ldots + n^m = \sum_{k=0}^{n} k^m \tag{3-22}$$

как функцию от n. При $m = 0, 1, 2, 3$ функции $S_m(n)$ достаточно известны:

$$\begin{aligned} S_0(n) &= 1 + \ldots + 1 = n \\ S_1(n) &= 1 + 2 + \ldots + n = n(n+1)/2 \\ S_2(n) &= 1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6 \\ S_3(n) &= 1^3 + 2^3 + \ldots + n^3 = n^2(n+1)^2/4 = S_1(n)^2\,. \end{aligned} \tag{3-23}$$

Чтобы получить для $S_m(t)$ явное выражение, применим к этой функции *разностный оператор*

$$\nabla : \varphi(t) \mapsto \varphi(t) - \varphi(t-1)\,.$$

[1] Т. е. имел ненулевой свободный член, см. прим. 2.2 на стр. 37.

Функция $\nabla S_m(t)$ принимает при всех $t \in \mathbb{Z}_{\geqslant 0}$ те же значения, что и многочлен t^m. Если существует такой многочлен $S_m(t) \in \mathbb{Q}[t]$, что $S_m(0) = 0$ и $\nabla S_m(t) = t^m$, то его значения в точках $t = 0,\ 1,\ 2,\ \ldots$ последовательно вычисляются, начиная с $S_m(0) = 0$, по формуле

$$S_m(n) = S_m(n-1) + \nabla S_m(n) = S_m(n-1) + n^m$$

и совпадают с суммами (3-22). Покажем, что уравнение $\nabla S_m(t) = t^m$ имеет в $\mathbb{Q}[t]$ единственное решение $S_m(t)$ с $S_m(0) = 0$. Согласно прим. 3.9 оператор $\nabla\colon\ \mathbb{Q}[t] \to \mathbb{Q}[t]$ имеет вид

$$\nabla = 1 - e^{-D} = \frac{1 - e^{-D}}{D} \circ D\,.$$

Ряд $(1 - e^{-x})/x$ имеет свободный член 1 и обратим в $\mathbb{Q}[\![x]\!]$. Обратный ему ряд

$$\mathrm{td}(x) \stackrel{\text{def}}{=} \frac{x}{1 - e^{-x}} \in \mathbb{Q}[\![x]\!]$$

называется *рядом Тодда*. Подставляя $x = D$ в равенство $\mathrm{td}(x) \cdot (1 - e^{-x}) = x$, получаем соотношение $\mathrm{td}(D) \circ \nabla = D$. Стало быть, $DS_m(t) = \mathrm{td}(D)\nabla S_m(t) = \mathrm{td}(D)t^m = \mathrm{td}_m(t)$ является многочленом Аппеля ряда Тодда, а искомый нами многочлен $S_m(t) = \int \mathrm{td}_m(t)\,dt$ получается из него интегрированием. Запишем ряд Тодда в «экспоненциальной форме»

$$\mathrm{td}(x) = \sum_{k \geqslant 0} \frac{a_k}{k!}\, x^k. \tag{3-24}$$

Тогда сумма m-тых степеней первых t натуральных чисел равна

$$S_m(t) = \int \Big(\sum_{k=0}^{m} \frac{a_k}{k!} D^k t^m \Big)\, dt = \int \Big(\sum_{k=0}^{m} \binom{m}{k} a_k t^{m-k} \Big)\, dt = \sum_{k=0}^{m} \binom{m}{k} \frac{a_k t^{m-k+1}}{m-k+1} =$$
$$= \frac{1}{m+1} \left(\binom{m+1}{1} a_m t + \binom{m+1}{2} a_{m-1} t^2 + \ldots + \binom{m+1}{m} a_1 t^m + \binom{m+1}{m+1} a_0 t^{m+1} \right).$$

Эту формулу часто символически пишут в виде

$$(m+1) \cdot S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}\,,$$

где стрелка у $a^{\downarrow}$ предписывает при раскрытии бинома $(a+t)^{m+1}$ заменять a^k на a_k. Коэффициенты a_k рекурсивно вычисляются из равенства $\mathrm{td}(x) \cdot (1 - e^{-x})/x = 1$, которое имеет вид

$$\left(1 + a_1 x + \frac{a_2}{2} x^2 + \frac{a_3}{6} x^2 + \frac{a_4}{24}\, x^4 + \ldots\right) \cdot \left(1 - \frac{1}{2}\, x + \frac{1}{6}\, x^2 - \frac{1}{24}\, x^3 + \frac{1}{120}\, x^4 - \ldots\right) = 1\,.$$

Упражнение 3.9. Найдите первую дюжину чисел a_k, проверьте формулы (3-23), дополните их явными формулами для $S_4(n)$ и $S_5(n)$ и вычислите[1] $S_{10}(1000)$.

[1] Яков Бернулли (1654–1705), пользуясь лишь пером и бумагой, сложил 10-е степени первой тысячи натуральных чисел примерно за 7 минут, о чём не без гордости написал в своём манускрипте «Ars Conjectandi», изданном в 1713 году уже после его кончины.

Замечание 3.1. (числа Бернулли) Название «ряд Тодда» вошло в обиход во второй половине XX века после работ Хирцебруха и Гротендика, где он использовался для формулировки и доказательства теоремы Римана – Роха. Во времена Бернулли и Эйлера предпочитали пользоваться рядом $\mathrm{td}(-x) = x/(e^x - 1)$, который отличается от $\mathrm{td}(x)$ ровно в одном члене, поскольку

$$\mathrm{td}(x) - \mathrm{td}(-x) = \frac{x}{1-e^{-x}} + \frac{x}{1-e^{x}} = x \cdot \frac{2 - e^x - e^{-x}}{(1-e^{-x})\cdot(1-e^x)} = x\,.$$

Тем самым, коэффициенты при x в $\mathrm{td}(x)$ и в $\mathrm{td}(-x)$ равны соответственно $1/2$ и $-1/2$, а все прочие коэффициенты при нечётных степенях x^{2k+1} с $k \geqslant 1$ в обоих рядах нулевые. Коэффициенты B_k в экспоненциальном представлении

$$\frac{x}{e^x - 1} = \sum_{k\geqslant 0} \frac{B_k}{k!}\, x^k$$

называются *числами Бернулли*. Таким образом, $B_k = a_k$ при $k \neq 1$ и обращаются в нуль при всех нечётных $k \geqslant 3$, а $B_1 = -a_1 = -1/2$. Со времён своего открытия числа Бернулли вызывают неослабевающий интерес. Им посвящена обширная литература[1] и специальный интернет-ресурс[2], на котором среди прочего есть программа для быстрого вычисления чисел B_k в виде несократимых рациональных дробей. Однако, не смотря на множество красивых теорем о числах Бернулли, про явную зависимость B_n от n известно немного, и любой содержательный новый взгляд в этом направлении был бы интересен.

Упражнение 3.10. Получите для чисел Бернулли рекурсивную формулу

$$(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} \cdot B_k\,.$$

[1] Начать знакомство с которой я советую с гл. 15 книги *К. Айрлэнд*, *М. Роузен*. «Классическое введение в современную теорию чисел» и § 8 гл. V книги *З. И. Боревич*, *И Р. Шафаревич*. «Теория чисел».

[2] http://www.bernoulli.org/

§4. Идеалы, факторкольца и разложение на множители

4.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 1.5.3 мы видели, что этим свойством обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Он обозначается

$$(a) = \{ka \mid k \in K\}, \tag{4-1}$$

и называется *главным* идеалом, порождённым a. Главные идеалы использовались нами при построении колец вычетов[1] $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)$, $m \mapsto [m]_n$, и $\Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f)$, $g \mapsto [g]_f$, переводящих целое число (соотв. многочлен) в класс его вычета. Среди главных идеалов имеются *тривиальный* идеал (0), состоящий только из нулевого элемента, и *несобственный* идеал (1), совпадающий со всем кольцом. Идеалы, отличные от всего кольца, называются *собственными*.

Упражнение 4.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей эквивалентны: а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 4.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных собственных идеалов.

Доказательство. Из упр. 4.1 вытекает, что в поле таких идеалов нет. Наоборот, если в кольце нет нетривиальных собственных идеалов, то главный идеал (b), состоящий из всех кратных произвольно взятого элемента $b \neq 0$, совпадает со всем кольцом. В частности, он содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент b обратим. □

4.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде $b_1a_1 + \ldots + b_ma_m$, где $a_1, \ldots, a_m$ — произвольные элементы множества M, а $b_1, \ldots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 4.2. Убедитесь, что $(M) \subset K$ является идеалом и совпадает с пересечением всех идеалов, содержащих множество M.

Любой идеал $I \subset K$ имеет вид (M) для подходящего множества образующих $M \subseteq I$: например, всегда можно положить $M = I$. Идеалы $I = (a_1, \ldots, a_k) = \{b_1a_1 + \ldots + b_ka_k \mid b_i \in K\}$, допускающие конечное множество образующих, называются *конечно порождёнными*. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 4.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов $a_1, \ldots, a_k \in M$, порождающий тот же идеал, что и M
2) любой идеал $I \subset K$ конечно порождён

[1] См. n° 1.4 на стр. 27 и n° 2.3.1 на стр. 42.

3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ в K стабилизируется в том смысле, что найдётся такое $n \in \mathbb{N}$, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

Доказательство. Ясно, что (1) влечёт (2). Чтобы получить (3) из (2), заметим, что объединение $I = \bigcup I_\nu$ всех идеалов цепочки тоже является идеалом. Согласно (2), идеал I порождён конечным набором элементов. Все они принадлежат некоторому идеалу I_n. Тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3), будем по индукции строить цепочку идеалов $I_n = (a_1, \ldots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \setminus I_{k-1}$ до тех пор, пока это возможно, т. е. пока $M \not\subset I_k$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий всё множество M, а значит, совпадающий с (M). □

Определение 4.1
Кольцо K, удовлетворяющее условиям лем. 4.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 4.1 (теорема Гильберта о базисе идеала)
Если кольцо K нётерово, то кольцо многочленов $K[x]$ также нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени не выше d из I, а через $L_\infty = \bigcup_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

Упражнение 4.3. Убедитесь, что все L_d (включая L_∞) являются идеалами в K.

Поскольку кольцо K нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, \ldots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$, старшие коэффициенты которых порождают идеал L_∞, равна D. Покажем, что идеал I порождается многочленами $f_i^{(\infty)}$ и $f_j^{(d)}$ с $d < D$.

Каждый многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, поскольку старший коэффициент многочлена g лежит в идеале L_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in K$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности $\delta_i = \deg g - \deg f_i^{(\infty)} \geqslant 0$, и можно образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{\delta_i}$, сравнимый с g по модулю I и имеющий $\deg h < \deg g$. Заменяем g на h и повторяем процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем строго уменьшать его степень, тем же способом сокращая старший член путём вычитания из h подходящих комбинаций многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 4.1
Если K нётерово, то кольцо многочленов $K[x_1, \ldots, x_n]$ также нётерово. □

Упражнение 4.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 4.2
Любая система полиномиальных уравнений с коэффициентами в нётеровом кольце эквивалентна некоторой конечной своей подсистеме.

Доказательство. Если кольцо K нётерово, то кольцо $K[x_1,\dots,x_n]$ тоже нётерово, и в любом множестве многочленов $M \subset K[x_1,\dots,x_n]$ можно указать такой конечный набор многочленов $f_1,\dots,f_m \in M$, что каждый многочлен $g \in M$ представляется в виде $g = h_1f_1 + \dots + h_mf_m$ для некоторых $h_i \in K[x_1,\dots,x_n]$. Поэтому любое уравнение вида $g(x_1,\dots,x_n) = 0$ с $g \in M$ является следствием m уравнений $f_1(x_1,\dots,x_n) = \dots = f_m(x_1,\dots,x_n) = 0$. □

4.1.2. Примеры ненётеровых колец. Кольцо многочленов от счётного множества переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементы которого суть конечные линейные комбинации с рациональными коэффициентами всевозможных мономов вида $x_{\nu_1}^{m_1}x_{\nu_2}^{m_2}\dots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 4.5. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \to \mathbb{R}$ всеми функциями, которые обращаются в нуле в нуль вместе со всеми своими производными.

Предостережение 4.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 4.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 4.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов из $\mathbb{C}[\![x]\!]$.

4.2. Фактор кольца. Пусть на коммутативном кольце K задано отношение эквивалентности, разбивающее K в дизъюнктное объединение классов эквивалентных элементов. Обозначим множество классов через X и рассмотрим сюръективное отображение факторизации

$$\pi\colon K \twoheadrightarrow X, \quad a \mapsto [a], \tag{4-2}$$

переводящее элемент $a \in K$ в его класс эквивалентности $[a] \subset K$, являющийся элементом множества X. Мы хотим задать на множестве X структуру коммутативного кольца, определив сложение и умножение теми же сами правилами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab], \tag{4-3}$$

которые мы использовали в кольцах вычетов. Если эти правила корректны, то аксиомы коммутативного кольца в X будут автоматически выполнены, как и для колец вычетов, поскольку формулы (4-3) сводят их проверку к проверке аксиом коммутативного кольца в K. В частности, нулевым элементом кольца X будет класс $[0]$. С другой стороны, если формулы (4-3) корректны, то они утверждают, что отображение (4-2) является гомоморфизмом колец. Но если это так, то согласно n° 1.5.3 на стр. 30 класс нуля $[0] = \ker\pi$, служащий ядром этого гомоморфизма, является идеалом в K, а класс $[a] \subset K$ произвольного элемента $a \in K$, служащий прообразом точки $[a] \in X$ при гомоморфизме (4-2), является аддитивным сдвигом ядра на элемент a:

$$[a] = \pi^{-1}(\pi(a)) = a + \ker\pi = a + [0] = \{a + b \mid b \in [0]\}.$$

Оказывается, что этих необходимых условий на классы также и достаточно для того, чтобы правила (4-3) были корректны, т. е. для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{4-4}$$

образует разбиение кольца K, и правила (4-3) корректно определяют на классах этого разбиения структуру коммутативного кольца с нулевым элементом $[0]_I = I$.

Упражнение 4.7. Убедитесь, что отношение сравнимости по модулю идеала $a_1 \equiv a_2 \pmod I$, означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, и проверьте, что формулы (4-3) корректны.

Определение 4.2
Классы эквивалентности (4-4) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (4-3) называется *факторкольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм $K \twoheadrightarrow K/I$, $a \mapsto [a]_I$, сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*.

Пример 4.1 (кольца вычетов)
Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть факторы кольца целых чисел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 4.2 (образ гомоморфизма)
Согласно n° 1.5.3, для любого гомоморфизма коммутативных колец $\varphi : A \to B$ имеется канонический изоморфизм колец $\overline{\varphi} : A/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$, $[a]_{\ker\varphi} \mapsto \varphi(a)$, переводящий каждый класс

$$[a]_{\ker\varphi} = a + \ker\varphi = \varphi^{-1}(\varphi(a))$$

в его образ $\varphi(a) = \varphi([a])$ при гомоморфизме φ.

Пример 4.3 (максимальные идеалы и гомоморфизмы вычисления)
Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если факторкольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что собственный[1] идеал $\mathfrak{m} \subset K$ максимален, если и только если он не содержится ни в каком строго большем собственном идеале, т. е. является максимальным элементом в чуме[2] собственных идеалов кольца K, частично упорядоченных по включению. В самом деле, обратимость всех ненулевых классов $[a]_{\mathfrak{m}}$ в факторкольце $K/\mathfrak{m}$ означает, что для любого $a \notin \mathfrak{m}$ найдутся такие $b \in K$, $m \in \mathfrak{m}$, что $ab + m = 1$ в K. Последнее равносильно тому, что идеал $(\mathfrak{m}, a) \supsetneq \mathfrak{m}$, порождённый $\mathfrak{m}$ и элементом $a \notin \mathfrak{m}$, содержит 1 и совпадает с K, т. е. что идеал $\mathfrak{m}$ не содержится ни в каком строго большем собственном идеале.

Из леммы Цорна[3] вытекает, что любой собственный идеал произвольного коммутативного кольца с единицей содержится в некотором максимальном идеале. В самом деле, множество всех собственных идеалов, содержащих произвольно заданный идеал $I \subset K$, тоже составляет чум по включению.

Упражнение 4.8. Убедитесь, что он полный, т. е. для любого линейно упорядоченного множества[4] M содержащих I собственных идеалов в K существует собственный идеал J^*, содержащий все идеалы из M.

[1] Т. е. отличный от всего кольца.
[2] См. n° 0.7 на стр. 15.
[3] См. сл. 0.1 на стр. 19.
[4] В данном случае это означает, что для любых $J_1, J_2 \in M$ выполняется включение $J_1 \subseteq J_2$ или включение $J_2 \subseteq J_1$.

По лемме Цорна существует такой собственный идеал $\mathfrak{m} \supset I$, который не содержится ни в каком большем собственном идеале, содержащем I. Такой идеал $\mathfrak{m}$ автоматически максимален по включению и в чуме всех собственных идеалов кольца K.

Максимальные идеалы возникают в кольцах функций как ядра *гомоморфизмов вычисления*. А именно, пусть X — произвольное множество, $p \in X$ — любая точка, $\Bbbk$ — любое поле, и K — какое-нибудь подкольцо в кольце всех функций $X \to \Bbbk$, содержащее тождественно единичную функцию 1 и вместе с каждой функцией $f \in K$ содержащее и все пропорциональные ей функции cf, $c \in \Bbbk$. Гомоморфизм вычисления $\mathrm{ev}_p : K \to \Bbbk$ переводит функцию $f \in K$ в её значение $f(p) \in \Bbbk$. Поскольку он сюръективен, его ядро $\ker \mathrm{ev}_p = \{f \in K \mid f(p) = 0\}$ является максимальным идеалом в K.

Упражнение 4.9. Убедитесь, что: а) каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$ б) в кольце непрерывных функций $[0,1] \to \mathbb{R}$ каждый максимальный идеал имеет вид $\ker \mathrm{ev}_p$ для некоторой точки $p \in [0,1]$. в) Укажите в кольце $\mathbb{R}[x]$ максимальный идеал, отличный от всех идеалов вида $\ker \mathrm{ev}_p$, где $p \in \mathbb{R}$.

Пример 4.4 (простые идеалы и гомоморфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*, если в факторкольце $K/\mathfrak{p}$ нет делителей нуля. Иначе говоря, идеал $\mathfrak{p} \subset K$ прост, если и только если из $ab \in \mathfrak{p}$ вытекает, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, главные идеалы $(p) \subset \mathbb{Z}$ и $(q) \subset \Bbbk[x]$, где $\Bbbk$ — поле, просты тогда и только тогда, когда число p просто, а многочлен q неприводим.

Упражнение 4.10. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x,y]$ прост, так как кольцо $\mathbb{Q}[x,y]/(x) \simeq \mathbb{Q}[y]$ целостное, но не максимален, поскольку строго содержится в идеале (x,y) многочленов без свободного члена[1]. Простые идеалы кольца K являются ядрами гомоморфизмов из кольца K во всевозможные поля. В самом деле, образ любого такого гомоморфизма, будучи подкольцом в поле, не имеет делителей нуля. Наоборот, факторкольцо $K/\mathfrak{p}$ по простому идеалу $\mathfrak{p} \subset K$ является подкольцом своего поля частных $Q_{K/\mathfrak{p}}$, и композиция факторизации и вложения $K \twoheadrightarrow K/\mathfrak{p} \hookrightarrow Q_{K/\mathfrak{p}}$ задаёт гомоморфизм из K в поле $Q_{K/\mathfrak{p}}$ с ядром $\mathfrak{p}$.

Упражнение 4.11. Убедитесь, что пересечение конечного множества идеалов содержится в простом идеале $\mathfrak{p}$ только если хотя бы один из пересекаемых идеалов содержится в $\mathfrak{p}$.

Пример 4.5 (конечно порождённые коммутативные алгебры)
Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида

$$A = K[x_1, \dots, x_n]/I\,,$$

где $I \subset K[x_1, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[2]. Классы $a_i = [x_i]_I$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями* между этими образующими. Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв $a_1, \dots, a_n$

[1] Т. е. в ядре гомоморфизма вычисления в нуле: $\mathrm{ev}_{(0,0)} : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{Q}$, $f(x,y) \mapsto f(0,0)$.

[2] Или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K.

при помощи операций сложения и умножения, производимых с учётом полиномиальных соотношений $f(a_1,\dots,a_n)=0$ для всех f из I. Из сл. 4.1 и идущего следом упр. 4.12:

Упражнение 4.12. Покажите, что факторкольцо нётерова кольца тоже нётерово.

мы получаем

Следствие 4.3
Всякая конечно порождённая коммутативная алгебра над нётеровым коммутативным кольцом нётерова, и все соотношения между её образующими являются следствиями конечного числа соотношений. □

4.3. Области главных идеалов. Целостное кольцо с единицей называется *областью главных идеалов*, если каждый его идеал является главным. Наблюдавшийся нами в §§ 1, 2 параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, объясняется тем, что оба кольца являются областями главных идеалов. Мы фактически установили это при построении наибольших общих делителей[1]. Ключевым элементом наших рассуждений было *деление с остатком*.

Пример 4.6 (евклидовы кольца)
Целостное кольцо K с единицей называется *евклидовым*, если на нём имеется *функция высоты*

$$\nu:\ K\to\mathbb{Z}_{\geqslant 0}=\mathbb{N}\cup\{0\},$$

с двумя свойствами: (1) $\nu(a)=0\iff a=0$; (2) для любых ненулевых $a,b\in K$ найдётся такое $q\in K$, что $\nu(a-bq)<\nu(b)$. Все такие q называются *неполными частными*, а соответствующие разности $r=a-bq$ — *остатками* от деления a на b относительно высоты ν. Подчеркнём, что никакой их единственности для заданных a,b не предполагается. В каждом ненулевом идеале I евклидова кольца K имеется ненулевой элемент $d\in I$ наименьшей в I высоты. Поскольку для любого $a\in I$ найдётся такое $q\in K$, что $\nu(a-dq)<\nu(d)$, и при этом $a-dq\in I$, мы заключаем, что $a-dq=0$ и, тем самым, $I=(d)$. Поэтому каждое евклидово кольцо K является областью главных идеалов.

Упражнение 4.13. Докажите евклидовость колец: а) $\mathbb{Z}$ с $\nu(z)=|z|$
б) $\Bbbk[x]$, где $\Bbbk$ — поле, с $\nu(f)=2^{\deg f}$ при $f\neq 0$ и $\nu(0)=0$
в) $\mathbb{Z}[i]\stackrel{\text{def}}{=}\{\,a+bi\in\mathbb{C}\mid a,b\in\mathbb{Z},\ i^2=-1\}$ с $\nu(z)=|z|^2$
г) $\mathbb{Z}[\omega]\stackrel{\text{def}}{=}\{a+b\omega\in\mathbb{C}\mid a,b\in\mathbb{Z},\ \omega^2+\omega+1=0\}$ с $\nu(z)=|z|^2$.

Функцию высоты $\nu:\ K\to\mathbb{Z}_{\geqslant 0}$ на любом евклидовом кольце K всегда можно выбрать так, чтобы для всех $a\in K$ и всех ненулевых $b\in K$ выполнялось дополнительное свойство $\nu(ab)\geqslant\nu(a)$. Для этого, задавшись какой-нибудь высотой ν', для всех $a\in K$ положим

$$\nu(a)=\min\nolimits_{x\in K\setminus 0}\nu'(ax).$$

Тогда по построению $\nu(ab)\geqslant\nu(a)$ для всех $a\in K$ и всех ненулевых $b\in K$. Очевидно, что $\nu(a)=0$, если и только если $a=0$. Убедимся, что ν обладает и вторым свойством евклидовой высоты. Пусть $\nu(b)=\nu'(bc)$ для ненулевого $c\in K$. Поскольку существует такое $q\in K$, что $\nu'(ac-bcq)<\nu'(bc)$, мы заключаем, что $\nu(a-bq)\leqslant\nu'\big((a-bq)c\big)<\nu'(bc)=\nu(b)$, как и требовалось. Высота ν со свойством $\nu(ab)\geqslant\nu(a)$ для всех ненулевых $b\in K$ называется *приведённой*.

Упражнение 4.14. Покажите, что в евклидовом кольце с приведённой высотой ν равенство $\nu(ab)=\nu(a)$ выполняется для ненулевых a,b, если и только если b обратим.

[1] См. n° 1.2.1 на стр. 23 и предл. 2.3 на стр. 40.

Существуют области главных идеалов, не являющиеся евклидовыми кольцами. Например, таковым является кольцо всех чисел вида $a + b\zeta \in \mathbb{C}$, где $a, b \in \mathbb{Z}$, а $\zeta = (1 + \sqrt{-19})/2$, однако содержательное обсуждение этого примера выходит за рамки понятий, которыми мы пока владеем. В прим. 4.7 на стр. 74 будет дана характеризация областей главных идеалов в терминах высот с немного более слабыми свойствами, чем у евклидовой высоты.

4.3.1. НОД и взаимная простота. В кольце главных идеалов K идеал

$$(a_1, \dots, a_n) = \{x_1a_1 + \dots + x_na_n \mid x_i \in K\},$$

порождённый любым набором элементов $a_1, \dots, a_n$, является главным и имеет вид (d) для некоторого $d \in K$. Таким образом, элемент d представляется в виде $d = a_1b_1 + \dots + a_nb_n$, где $b_i \in K$, делит все элементы a_i и делится на любой общий делитель элементов a_i, т. е. является *наибольшим общим делителем*[1] элементов $a_1, \dots, a_n$. Отметим, что наибольший общий делитель определён не однозначно, а с точностью до умножения на произвольный обратимый элемент из K.

Упражнение 4.15. Убедитесь, что в любом целостном коммутативном кольце K главные идеалы (a) и (b) совпадают, если и только если $a = sb$ для некоторого обратимого $s \in K$.

Поэтому всюду далее обозначение нод$(a_1, \dots, a_n)$ подразумевает целый класс элементов, получающихся друг из друга умножениями на обратимые константы, и все формулы, которые будут писаться, относятся к произвольно выбранному конкретному представителю этого класса[2]. В частности, равенство нод$(a_1, \dots, a_n) = 1$ означает, что у элементов a_i нет необратимых общих делителей. Так как в этом случае $1 = a_1b_1 + \dots + a_nb_n$ с $b_i \in K$, отсутствие необратимых общих делителей у элементов a_i в кольце главных идеалов равносильно их *взаимной простоте* в смысле опр. 1.2 на стр. 26.

Упражнение 4.16. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

4.4. Факториальность. Всюду в этом разделе мы по умолчанию обозначаем через K *целостное* кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b или, что то же самое, если $(a) = (b)$. Из упр. 4.15 выше вытекает, что a и b ассоциированы, если и только если они получаются друг из друга умножением на обратимый элемент кольца. Например, целые числа a и b ассоциированы в кольце $\mathbb{Z}$, если и только если $a = \pm b$, а многочлены $f(x)$ и $g(x)$ с коэффициентами из поля $\Bbbk$ ассоциированы в $\Bbbk[x]$, если и только если $f(x) = cg(x)$, где $c \in \Bbbk^*$ — ненулевая константа.

4.4.1. Неприводимые элементы. Ненулевой необратимый элемент q называется *неприводимым*, если из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, что главный идеал (q) собственный и не содержится строго ни в каком другом собственном главном идеале, т. е. максимален в частично упорядоченном отношением включения множестве собственных главных идеалов. Неприводимыми элементами в кольце $\mathbb{Z}$ являются простые числа, а в кольце $\Bbbk[x]$, где $\Bbbk$ — поле, — неприводимые многочлены.

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[3], либо ассоциированы, поскольку идеал $(p, q) = (d)$ для некоторого $d \in K$, и в виду максимальности (p) и (q) включения $(p) \subset (d)$ и $(q) \subset (d)$ влекут либо равенство $(d) = (K) = (1)$, либо равенство $(d) = (p) = (q)$. Обратите внимание, что в произвольном целостном кольце два

[1] См. зам. 1.3. на стр. 26.

[2] Что, конечно же, требует проверки корректности всех таких формул, которую мы, как правило, будем оставлять читателю в качестве упражнения.

[3] В смысле опр. 1.2 на стр. 26, т. е. существуют такие $x, y \in K$, что $px + qy = 1$.

неассоциированных неприводимых элемента могут и не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ неприводимые многочлены x и y не взаимно просты и не ассоциированы.

Предложение 4.2
В кольце главных идеалов K следующие свойства ненулевого элемента $p \in K$ эквивалентны:

1) идеал (p) максимален, т. е. факторкольцо $K/(p)$ является полем

2) идеал (p) прост, т. е. в факторкольце $K/(p)$ нет делителей нуля

3) p неприводим, т. е. из равенства $p = ab$ вытекает, что a или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна и имеет место в любом коммутативном кольце с единицей. Импликация (2) $\Rightarrow$ (3) имеет место в любом целостном кольце K. Действительно, из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и так как в $K/(p)$ нет делителей нуля, один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, откуда $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим.

Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Так как каждый собственный идеал в K главный, максимальность идеала (p) в чуме собственных главных идеалов означает его максимальность в чуме всех собственных идеалов. В прим. 4.3 на стр. 69 мы видели, что это равносильно тому, что $K/(p)$ поле. □

Предложение 4.3
Каждый ненулевой необратимый элемент целостного нётерова кольца является произведением конечного числа неприводимых.

Доказательство. Если элемент a неприводим, доказывать нечего. Пусть a приводим. Запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Эта процедура закончится, когда все сомножители станут неприводимы, что и требуется. Если же она никогда не закончится, мы сможем образовать бесконечную последовательность строго вложенных друг в друга главных идеалов $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$, что противоречит нётеровости. □

Определение 4.3
Целостное кольцо K называется *факториальным*, если каждый его необратимый ненулевой элемент является произведением конечного числа неприводимых, причём любые два таких разложения $p_1 \dots p_m = q_1 \dots q_k$ состоят из одинакового числа $k = m$ сомножителей, и после надлежащей их перенумерации можно указать такие обратимые $s_\nu \in K$, что $q_\nu = p_\nu s_\nu$ при всех ν.

4.4.2. Простые элементы. Ненулевой элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в факторкольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ произведение ab делится на p только если a или b делится на p. Каждый простой элемент p автоматически неприводим: если $p = xy$, то один из сомножителей, скажем x, делится на p, и тогда $p = pyz$, откуда $yz = 1$ и y обратим. Согласно предл. 4.2 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты. Однако в произвольном целостном кольце могут быть неприводимые непростые

элементы. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ таковым является число 2, так как в факторе $\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) = \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$ есть нильпотент — класс $[x+1] \in \mathbb{Z}[x]/(2, x^2+5)$. Среди прочего это означает, что квадрат $(1+\sqrt{5})^2 = 6+2\sqrt{5}$ делится в кольце $\mathbb{Z}[\sqrt{5}]$ на 2, хотя $1+\sqrt{5}$ не делится на 2, при том что 2 и $\sqrt{5}+1$ неприводимы и не ассоциированы друг с другом в кольце $\mathbb{Z}[\sqrt{5}]$.

Упражнение 4.17. Убедитесь в этом, и покажите, что $2 \cdot 2 = 4 = \big(\sqrt{5}+1\big) \cdot \big(\sqrt{5}-1\big)$ суть два *различных* разложения числа 4 на неприводимые множители в $\mathbb{Z}[\sqrt{5}]$.

Предложение 4.4
Целостное нётерово кольцо K факториально, если и только если все его неприводимые элементы просты.

Доказательство. Покажем сначала, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Тогда разложение ab на неприводимые множители содержит множитель, ассоциированный с q, и в силу своей единственности является произведением разложений a и b на неприводимые множители. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q. Наоборот, пусть все неприводимые элементы в K просты. Тогда по предл. 4.3 на стр. 73 каждый элемент кольца K является произведением конечного числа простых. Покажем, что в целостном кольце равенство $p_1 \dots p_k = q_1 \dots q_m$, в котором все сомножители просты, возможно только если $k = m$ и после надлежащей перенумерации каждый $p_i = s_i q_i$, где s_i обратим. Поскольку произведение $q_1 \dots q_m$ делится на p_1, один из его сомножителей делится на p_1. Будем считать, что это $q_1 = sp_1$. Так как q_1 неприводим, элемент s обратим. Пользуясь целостностью K, сокращаем обе части равенства $p_1 \dots p_k = q_1 \dots q_m$ на p_1 и получаем более короткое равенство $p_2 p_3 \dots p_k = (sq_2)q_3 \dots q_m$, к которому применимы те же рассуждения. □

Следствие 4.4
Всякое кольцо главных идеалов факториально. □

Пример 4.7 (характеризация областей главных идеалов, продолжение прим. 4.6 на стр. 71)
Покажем, что целостное кольцо K является областью главных идеалов, если и только если на K имеется функция высоты $\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\}$ со следующими двумя свойствами:

1) $\nu(a) = 0 \iff a = 0$; 2) если $a \notin (b)$, то найдутся $x, y \in K$ с $0 < \nu(ax+by) < \nu(b)$.

Действительно, пусть такая высота существует. Тогда в каждом идеале $I \subset K$ есть ненулевой элемент $d \in I$, на котором ν принимает наименьшее в I ненулевое значение. Если $a \in I \smallsetminus (d)$, то найдутся $x, y \in K$ с $0 < \nu(ax+dy) < \nu(d)$, что невозможно, ибо $ax+dy \in I$. Тем самым $I = (d)$ и K является областью главных идеалов. Наоборот, пусть K — область главных идеалов. Выберем в каждом классе ассоциированных простых элементов какого-нибудь представителя p и для каждого $a \in K$ обозначим через $\nu_p(a)$ показатель, с которым p входит в разложение a на простые множители: $a = \prod_p p^{\nu_p(a)}$. Положим $\nu(a) = 2^{\sum_p \nu_p(a)}$. Так как $\nu_p(a) = 0$ для всех p кроме конечного числа, это определение корректно. Если $b \nmid a$, то $\text{нод}(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}$ имеет положительную высоту, строго меньшую, чем $\nu(b)$, и представляется в виде $ax+by$, что и требуется. Более того, построенная высота ν *приведена* в том смысле[1], что $\nu(a) \leqslant \nu(ab)$ для всех a и всех ненулевых b, причём равенство равносильно обратимости b.

[1] Ср. с прим. 4.6 на стр. 71.

Пример 4.8 (гауссовы числа и суммы двух квадратов)
Элементы кольца $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1) \simeq \{x+iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ из упр. 4.13 (в) на стр. 71 называются *целыми гауссовыми числами*.

Упражнение 4.18. Убедитесь, что: а) в $\mathbb{Z}[i]$ обратимы только ± 1 и $\pm i$ б) $z \in \mathbb{Z}$ прост, если и только если прост $\overline{z}$.

Из упражнения вытекает, что разложение вещественного целого числа $n \in \mathbb{Z}$ на простые множители в области $\mathbb{Z}[i]$, будучи инвариантным относительно комплексного сопряжения, вместе с каждым невещественным неприводимым множителем содержит и его сопряжённый. Поэтому вещественное простое $p \in \mathbb{Z}$ становится приводимым в $\mathbb{Z}[i]$, если и только если оно имеет вид $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a, b \in \mathbb{Z}$. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что факторкольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[1], что равносильно неприводимости многочлена x^2+1 над $\mathbb{F}_p$. Последнее равносильно тому, что -1 не является квадратом в $\mathbb{F}_p$, и имеет место если и только если[2] $p = 4k+3$. Мы заключаем, что неприводимость простого $p \in \mathbb{Z}$ в области $\mathbb{Z}[i]$ равносильна тому, что $p = 4k+3$, и тому, что p не представляется в виде суммы двух квадратов целых чисел.

Упражнение 4.19. Покажите, что произвольное $n \in \mathbb{N}$ является квадратом или суммой двух квадратов натуральных чисел, если и только если в его разложении на простые множители в кольце $\mathbb{Z}$ простые числа $p = 4k+3$ присутствуют только в чётных степенях.

4.4.3. НОД в факториальном кольце. В любом факториальном кольце K у любого конечного набора чисел $a_1, \ldots, a_m \in K$ имеется наибольший общий делитель[3]. Он имеет следующее явное описание. Зафиксируем в каждом классе ассоциированных простых элементов кольца K некоторый представитель p и для каждого $a \in K$ обозначим через $\nu_p(a) \in \mathbb{Z}_{\geqslant 0}$ показатель, с которым p входит в разложение a на простые множители[4], как в прим. 4.7 выше. Тогда, с точностью до умножения на обратимые элементы, $\text{нод}(a_1, \ldots, a_m) = \prod_p p^{\min_i \nu_p(a_i)}$.

Упражнение 4.20. Убедитесь, что правая часть делит каждое a_i и делится на любой общий делитель всех a_i.

Отметим, что если K не является областью главных идеалов, то $\text{нод}(a_1, \ldots, a_m)$ может не представляться в виде линейной комбинации элементов a_i с коэффициентами из K. Например, элементы x, y факториального кольца[5] $\mathbb{Q}[x, y]$ имеют $\text{нод}(x, y) = 1$, но нет таких $f, g \in \mathbb{Q}[x, y]$, что $fx + gy = 1$, ибо подставляя в это равенство $x = y = 0$, получим $0 = 1$.

4.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо $K[x]$ является подкольцом в $Q_K[x]$. Назовём *содержанием* многочлена $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ наибольший общий делитель его коэффициентов:

$$\text{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \ldots, a_n)\,.$$

Лемма 4.2
$\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$ для любых $f, g \in K[x]$.

[1] См. предл. 4.2 на стр. 73.
[2] См. прим. 1.8 на стр. 30.
[3] В смысле зам. 1.3. на стр. 26, т. е. число, которое делит все a_i и делится на любой их общий делитель.
[4] Обратите внимание, что для каждого a показатель $\nu_p(a) \neq 0$ только для конечного множества простых чисел p.
[5] См. сл. 4.6 на стр. 77.

Доказательство. Достаточно для каждого простого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg, если и только если q делит все коэффициенты хотя бы одного из многочленов f, g. Для этого положим $R = K/(q)$ и применим к произведению fg гомоморфизм

$$K[x] \to R[x], \quad a_0 + a_1 x + \ldots + a_n x^n \mapsto [a_0]_q + [a_1]_q x + \ldots + [a_n]_q x^n,$$

заменяющий коэффициенты каждого многочлена их вычетами по модулю q.

Упражнение 4.21. Проверьте, что это и в самом деле гомоморфизм колец.

В силу простоты q кольцо R целостное. Поэтому $R[x]$ тоже целостное, и $[fg]_q = [f]_q[g]_q = 0$, если и только если $[f]_q = 0$ или $[g]_q = 0$. □

Лемма 4.3 (приведённое представление)
Каждый $f \in Q_K[x]$ представляется в виде $f(x) = (a\,/\,b) \cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$ и $\operatorname{cont}(f_{\text{red}}) = \text{нод}(a, b) = 1$, причём a, b и f_{red} определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Вынесем из коэффициентов f их общий знаменатель, потом вынесем из всех коэффициентов полученного многочлена их наибольший общий делитель. В результате мы получим многочлен содержания 1, умноженный на число из Q_K, которое запишем несократимой дробью a/b. Докажем единственность такого представления. Если $(a/b) \cdot f_{\text{red}}(x) = (c/d) \cdot g_{\text{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, заключаем, что $ad = bc$, откуда $f_{\text{red}}(x) = g_{\text{red}}(x)$. В виду отсутствия общих неприводимых множителей у a и b и у c и d, равенство $ad = bc$ возможно лишь когда a ассоциирован с c, а b — с d. □

Следствие 4.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в $Q_K[x]$, если и только если он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в приведённом виде из лем. 4.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\text{red}}(x) \cdot h_{\text{red}}(x), \tag{4-5}$$

в котором $g_{\text{red}}, h_{\text{red}} \in K[x]$ имеют содержание 1, и $\text{нод}(a, b) = 1$. По лем. 4.2

$$\operatorname{cont}(g_{\text{red}} h_{\text{red}}) = \operatorname{cont}(g_{\text{red}}) \cdot \operatorname{cont}(h_{\text{red}}) = 1,$$

т. е. правая часть в (4-5) является приведённым представлением многочлена f. В силу единственности приведённого представления элементы a и b обратимы в K, а $f = g_{\text{red}} h_{\text{red}}$ с точностью до умножения на обратимую константу. □

Теорема 4.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Будучи кольцом главных идеалов, кольцо $Q_K[x]$ факториально, и каждый многочлен $f \in K[x] \subset Q_K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в приведённом виде из лем. 4.3 и сокращая возникающую при этом числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\text{red}}$, в котором $a, b \in K$ имеют $\text{нод}(a, b) = 1$, а

все $f_{\nu,\mathrm{red}} \in K[x]$ неприводимы в $Q_K[x]$ и $\mathrm{cont}(f_{\nu,\mathrm{red}}) = 1$. Тогда $\mathrm{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$ по лем. 4.3, и правая часть равенства является приведённым представлением многочлена $f = \mathrm{cont}(f) \cdot f_{\mathrm{red}}$. В силу единственности приведённого представления $b = 1$ и $f = a\prod f_{\nu,\mathrm{red}}$ с точностью до умножения на обратимые константы из K. Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$. Докажем единственность такого разложения. Пусть в $K[x]$

$$a_1 \dots a_k \cdot p_1 \dots p_s = b_1 \dots b_m \cdot q_1 \dots q_r\,,$$

где $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ — неприводимые многочлены. Поскольку неприводимые многочлены имеют содержание 1, сравнивая содержание обеих частей, приходим к равенству $a_1 \dots a_k = b_1 \dots b_m$ в K. Так как K факториально, мы заключаем, что $k = m$ и после надлежащей перенумерации сомножителей $a_i = s_i b_i$, где все $s_i \in K$ обратимы. Следовательно, с точностью до умножения на обратимую константу из K, в кольце $K[x]$ выполняется равенство $p_1 \dots p_s = q_1 \dots q_r$. Так как все p_i и q_i неприводимы в факториальном кольце $Q_K[x]$, мы заключаем, что $r = s$ и после надлежащей перенумерации сомножителей $p_i = q_i$ с точностью до постоянных множителей из поля Q_K. Из единственности приведённого представления[1] вытекает, что эти постоянные множители являются обратимыми константами из кольца K. □

Следствие 4.6
Кольцо многочленов $K[x_1, \dots, x_n]$ над факториальным кольцом[2] K факториально. □

4.6. Разложение многочленов с целыми коэффициентами. Разложение многочлена $f \in \mathbb{Z}[x]$ на множители в $\mathbb{Q}[x]$ разумно начать с отыскания его рациональных корней, что делается за конечное число проб.

Упражнение 4.22. Покажите, что несократимая дробь $p/q \in \mathbb{Q}$ является корнем многочлена $a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ только если $p \mid a_0$ и $q \mid a_n$.

Точное знание комплексных корней многочлена f тоже весьма полезно.

Упражнение 4.23. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения будут исчерпаны, следует подключать более трудоёмкие способы.

4.6.1. Редукция коэффициентов $\mathbb{Z}[x] \to \mathbb{Z}/(m)\,[x]$, $f \mapsto [f]_m$, где

$$[f]_m \stackrel{\text{def}}{=} [a_0]_m + [a_1]_m x + \dots [a_n]_m x^n \text{ для } f = a_0 + a_1 x + \dots + a_n x^n\,, \tag{4-6}$$

приводит коэффициенты всех многочленов по модулю m и является гомоморфизмом колец[3]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$, и из неприводимости многочлена $[f]_m$ хотя бы при одном m вытекает его неприводимость в $\mathbb{Z}[x]$. Если число $m = p$ простое, кольцо коэффициентов $\mathbb{Z}/(m) = \mathbb{F}_p$ является полем, и кольцо многочленов $\mathbb{F}_p[x]$ в этом случае факториально. При малых p разложение многочлена небольшой степени на неприводимые множители в $\mathbb{F}_p[x]$ можно осуществить простым перебором, и анализ такого разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

[1] См. лем. 4.3 на стр. 76.
[2] В частности, над полем или над областью главных идеалов.
[3] Мы уже пользовались этим в доказательстве лем. 4.2 на стр. 75, см. упр. 4.21.

Пример 4.9
Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Сделаем редукцию по модулю 2. Так как у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Но единственный неприводимый многочлен второй степени в $\mathbb{F}_2[x]$ — это $x^2 + x + 1$, и $x^5 + x^2 + 1$ на него не делится. Тем самым, $[f]_2$ неприводим над $\mathbb{F}_2$, а значит, и над $\mathbb{Z}$.

Пример 4.10 (критерий Эйзенштейна)
Пусть все за исключением старшего коэффициенты приведённого многочлена $f \in \mathbb{Z}[x]$ делятся на простое число $p \in \mathbb{N}$, а младший коэффициент, делясь на p, не делится при этом на p^2. Покажем, что f неприводим в $\mathbb{Z}[x]$. В силу сделанных об f предположений при редукции по модулю p от f остаётся только старший моном $[f(x)]_p = x^n$. Если $f(x) = g(x)h(x)$ в $\mathbb{Z}[x]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[x]$ оба сомножителя g, h тоже редуцируются в некоторые степени переменной: $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все коэффициенты многочленов g и h кроме старшего делятся на p. Тогда младший коэффициент многочлена f, будучи произведением младших коэффициентов многочленов g и h, должен делиться на p^2, что не так.

Пример 4.11 (неприводимость кругового многочлена Φ_p)
Покажем, что при простом $p \in \mathbb{N}$ круговой многочлен $\Phi_p(x) = x^{p-1} + \ldots + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = (t+1)^p - 1 \,/\, t = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-1}.$$

Поскольку при простом p все биномиальные коэффициенты $\binom{p}{k}$ с $1 \leqslant k \leqslant p-1$ делятся[1] на p, а свободный член $\binom{p}{p-1} = p$ не делится на p^2, многочлен $f(t)$ неприводим по критерию Эйзенштейна из прим. 4.10. Поэтому и $\Phi_p(x) = f(x-1)$ неприводим.

4.6.2. Алгоритм Кронекера позволяет путём довольно трудоёмкого, но вполне конечного вычисления либо явно разложить многочлен $f \in \mathbb{Z}[x]$ на множители в кольце $\mathbb{Z}[x]$, либо убедиться, что f неприводим в $\mathbb{Z}[x]$. Пусть $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ степень одного из делителей, пусть это будет h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени не выше n, подставим в f произвольные $n+1$ различных чисел $z_0, \ldots, z_n \in \mathbb{Z}$ и выпишем все возможные наборы чисел $d_0, \ldots, d_n \in \mathbb{Z}$, в которых каждое d_i делит соответствующее $f(z_i)$. Таких наборов имеется конечное число, и если искомый многочлен h существует, то набор его значений $h(z_0), \ldots, h(z_n)$ на числах z_i является одним из выписанных наборов $d_0, \ldots, d_n$. Для каждого такого набора в $\mathbb{Q}[x]$ есть ровно один многочлен h степени не выше n с $h(z_i) = d_i$ при всех i — это *интерполяционный многочлен Лагранжа*[2]

$$h(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)}. \tag{4-7}$$

[1] См. сл. 1.1 на стр. 29.
[2] См. прим. 2.5 на стр. 42.

Таким образом, делитель h многочлена f, если он существует, совпадает с одним из тех многочленов (4-7), что имеют целые коэффициенты. Остаётся явно разделить f на все такие многочлены и либо убедиться, что они не делят f, либо обнаружить среди них делитель f.

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 $X \setminus Y = \{1\}$.

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 сюръективное 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 сюръекция $\mathbb{N} \twoheadrightarrow \mathbb{N}$, $n \mapsto \max(1, (n - 1))$, обе не биективны и продолжаются до точно таких же отображений $X \to X$ тождественным действием на $X \setminus \mathbb{N}$.

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 $k = 1, 2, 3, \ldots$ отображает некоторое число $n_k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 0.7. 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 $(k_1, \ldots, k_m)$ 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. 0.8. 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. 0.9. 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. 0.10. Положим $x \sim y$, если существует конечная последовательность точек

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

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

Упр. 0.11. 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. 0.12. 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. 0.14. 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. 0.15. Отношение $n \mid m$ на множестве $\mathbb{Z}$ не кососимметрично: $n \mid m$ и $m \mid n$ если и только если $m = \pm n$. 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. 0.16. 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. 0.17. 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 $y < x_I$. Так как I содержит все интервалы $[y)$ с $y < x_I$, мы заключаем, что $I \supseteq [x_I)$, откуда $I = [x_I)$.

Упр. 0.18. 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 $y < u$.

Если в начальном интервале $[u)$ имеется максимальный элемент u', то $[u) = [u') \sqcup \{u'\}$, и $[u')$ изоморфен некоторому начальному интервалу $[w') \subset W$, отличному от W, поскольку равенство $[w') = W$ означает, что $U \geqslant W$. Тем самым, интервал $[u) = [u') \sqcup \{u'\}$ изоморфен вполне упорядоченному множеству $[w') \sqcup \{w'\}$, которое не совпадает с W по тем же причинам, что и выше, и является начальным интервалом вида $[w) \subset W$, где $w = w(u)$ — наименьший элемент в дополнении к подмножеству $[w') \sqcup \{w'\}$ в W.

Если в начальном интервале $[u)$ нет максимального элемента, то $[u) = \bigcup_{y<u}[y)$ изоморфен объединению вложенных начальных интервалов $\bigcup_{y<u}[w(y)) \subset W$. Это объединение не исчерпывает всё множество W, поскольку в противном случае $W \simeq [y)$ и $W \leqslant U$. 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 с некоторым начальным отрезком множества W.

Упр. 0.19. Пусть рекурсивные подмножества $W_1, W_2 \subset P$ имеют общий начальный элемент. Рассмотрим подмножество $Z \subseteq W_1$, состоящее из всех таких $z \in W_1$, что начальный интервал $[z)_1$ в множестве W_1 совпадает с начальным интервалом $[z)_2$ в множестве W_2. Множество Z не пусто, поскольку содержит общий начальный элемент множеств W_1 и W_2. В силу рекурсивности W_1 и W_2 множество Z содержится в $W_1 \cap W_2$, являясь, по упр. 0.17 на стр. 17, начальным интервалом как в W_1, так и в W_2. Если $Z \neq W_1$ и $Z \neq W_2$, то точные верхние грани Z в W_1 и W_2, с одной стороны, не лежат в Z и поэтому различны, а с другой стороны обе равны $\varrho(Z)$ в силу рекурсивности W_1 и W_2. Тем самым, $Z = W_1$ или $Z = W_2$.

Упр. 0.20. 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. 0.19 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 такого W, что $W \cap S \neq \varnothing$, 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. 0.21. 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. 0.22. 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 $\mu(X \setminus [w)) = w$ 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. 0.23. 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 $\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$ удовлетворяют равенствам $m = xa + by$, $n = as + bt$ и $xt - ys = 1$. Прибавляя к 1-й строке 2-ю, умноженную на k, получаем таблицу $\begin{pmatrix} m' & x' & y' \\ n & s & t \end{pmatrix}$, в которой $m' = m + nk$, $x' = x + ks$, $y' = t + kt$. Тогда

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

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

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

Единственность разложения. Для любого простого числа p и любого целого z имеется альтернатива: либо нод$(z, p) = |p|$, и тогда z делится на p, либо нод$(z, p) = 1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ 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. 1.9. При любом $k \in \mathbb{N}$ умножение на класс $[x]^{-1}[y]$ переводит класс $[a^k x]$ в класс $[a^k y]$, а умножение на класс $[x][y]^{-1}$ переводит класс $[a^k y]$ назад в $[a^k x]$.

Упр. 1.11. Класс $\binom{mp^n}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему после раскрытия скобок и приведения подобных слагаемых в биноме $(1+x)^{mp^n}$ над полем $\mathbb{F}_p$. Последовательно применяя формулу форм. (1-24) на стр. 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. 1.13. Если число $\alpha \in \Bbbk$ является корнем многочлена $f(x)$, то $f(x)$ делится на $(x-\alpha)$ (разделите $f(x)$ на $(x-\alpha)$ с остатком и подставьте $x=\alpha$).

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

Упр. 1.16. 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. 1.17. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

Упр. 2.3. Ответ: $(y^n - x^n)/(y-x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \ldots + yx^{n-2} + x^{n-1}$.

Упр. 2.5. $\left(a_0 + a_1x + a_2x^2 + \ldots\right)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots = a_0 + a_1x^p + a_2x^{2p} + \ldots$ (первое равенство справедливо, поскольку возведение в p-тую степень перестановочно со сложением, второе — по малой теореме Ферма).

Упр. 2.6. Если $f(x) = \sum a_k x^k$, то $f(x+t) = \sum\limits_{k,\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu}t^\nu = \sum\limits_\nu t^\nu \cdot f_\nu(x)$, где

$$f_\nu(x) = \sum_{k\geqslant\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu} = \frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0} a_k x^k\,.$$

Упр. 2.7. Годятся дословно те же аргументы, что и в упр. 1.8.

Существование. Если f неприводим, то сам он и является своим разложением. Если f приводим, то он раскладывается в произведение многочленов строго меньшей степени, которые в свою очередь или неприводимы или являются произведениями многочленов строго меньшей степени и т. д. Поскольку степень не может бесконечно уменьшаться, в конце концов получится требуемое разложение.

Единственность. Для неприводимого $p \in \Bbbk[x]$ и любого $g \in \Bbbk[x]$ имеется следующая альтернатива: либо $\text{нод}(p,g) = \lambda p$, где $\lambda \in \Bbbk^\times$ — ненулевая константа, и в этом случае g делится на p, либо $\text{нод}(p,g) = 1$, и тогда g взаимно прост с p. Пусть все сомножители в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ неприводимы. Поскольку $\prod q_i$ делится на p_1, многочлен p_1, не может быть

[1] См. сл. 1.1 на стр. 29.
[2] См. n° 1.5.4 на стр. 31.

взаимно прост с каждым q_i в силу лем. 1.3 на стр. 26. Поэтому найдётся q_i, делящийся на p_1. После надлежащей перенумерации можно считать, что это q_1. Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.8. При умножении любой из строк таблицы $\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$ на ненулевую константу равенства $p = rf + sg$, $q = uf + wg$ сохраняются, а многочлен $rw - us$ умножается на эту константу. Если заменить любую строку таблицы на её сумму с другой строкой, умноженной на любой многочлен, равенства $p = rf + sg$, $q = uf + wg$ сохранятся, а многочлен $rw - us$ вообще не поменяется (ср. с упр. 1.6 на стр. 25). Пусть в итоговой таблице

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix}$$

$h_1 m_2 - h_2 m_1 = \delta \in \Bbbk^\times$. Умножая это равенство на f и на g и пользуясь тем, что $d' = fh_1 + gh_2$, а $fm_1 = -gm_2$, получаем

$$\delta f = fh_1 m_2 - fh_2 m_1 = fh_1 m_2 + gh_2 m_2 = d' m_2$$
$$\delta g = gh_1 m_2 - gh_2 m_1 = -fh_1 m_1 - gh_2 m_1 = -d' m_1 .$$

Поэтому $f = d' m_2 \delta^{-1}$ и $g = -d' m_1 \delta^{-1}$ делятся на d'. Для любого $q = fs = gt$ из равенства

$$\delta q = qh_1 m_2 - qh_2 m_1 = gth_1 m_2 - fsh_2 m_1 = -c'(th_1 + sh_2),$$

где $c' = fm_1 = -gm_2$, заключаем, что $q = -c'(th_1 + sh_2)\delta^{-1}$ делится на c'.

Упр. 2.9. Если многочлен степени $\leqslant 3$ приводим, то у него есть делитель первой степени, корень которого будет корнем исходного многочлена.

Упр. 2.11. См. упр. 0.9 на стр. 10.

Упр. 2.12. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x-\alpha)$ в качестве констант сюръективно, поскольку число $\alpha \in \Bbbk$ переходит в класс$[x]$, и значит, для любого $g \in \Bbbk[x]$ число $g(\alpha)$ переходит в класс $[g]$.

Упр. 2.13. Обратным элементом к произвольному ненулевому $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ является $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Кольцо в (а) содержит делители нуля: $[t+1]\cdot[t^2-t+1] = [0]$ и, тем самым, не является полем. Кольцо в (б) является полем: многочлен $p = \vartheta^3 + 2$ не имеет корней в $\mathbb{Q}$, и значит, не делится в $\mathbb{Q}[x]$ ни на какой многочлен первой или второй степени; следовательно, p взаимно прост со всеми $g \in \mathbb{Q}[x]$, не делящимися на p, т. е. для любого $[g] \neq [0]$ существуют $h_1, h_2 \in \mathbb{Q}[x]$, такие что $h_1 g + h_2 p = 1$; тем самым, $[h_1] = [g]^{-1}$.

Упр. 2.14. Ответ: $(1+\vartheta)^{-1} = -\vartheta$.

Упр. 2.15. Решение этой задачи опирается на теор. 2.3 на стр. 50 и теор. 2.4 на стр. 51. Обозначим через $\mathbb{F}_q$ конечное поле из q элементов[1]. Пусть $f \in \mathbb{F}_q[x]$ неприводим. Из доказательства теор. 2.1 на стр. 44 вытекает, что существует такое конечное поле $\mathbb{F}_r \supset \mathbb{F}_q$, что f полностью раскладывается на линейные множители в $\mathbb{F}_r[x]$. Так как поле $\mathbb{F}_r$ состоит из корней многочлена $g = x^r - x$, этот многочлен имеет общие корни с f, откуда нод$(f, g) \neq 1$ в $\mathbb{F}_q[x]$. Так как f неприводим, $g \vdots f$ в $\mathbb{F}_q[x]$. А поскольку g сепарабелен, f тоже сепарабелен.

[1] Согласно теор. 2.3 и теор. 2.4 такое поле единственно с точностью до изоморфизма и состоит из корней многочлена $x^q - x$ в таком расширении простого подполя поля $\mathbb{F}_q$, над которым этот многочлен полностью раскладывается на линейные множители.

Упр. 2.17. Число $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$ является корнем многочлена

$$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)\,.$$

Уравнение $z^4 + z^3 + z^2 + z + 1 = 0$ можно решить в радикалах, деля обе части на z^2 и вводя новую переменную $t = z + z^{-1}$.

Упр. 2.18. Пусть $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Так как равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$, среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ, которые делятся на нод(k, n).

Упр. 2.19. См. листок $2\frac{1}{2}$.

Упр. 2.22. Конечное поле $\mathbb{F}$ характеристики p является векторным пространством над своим простым подполем $\mathbb{F}_p \subset \mathbb{F}$, и в нём имеются такие векторы $v_1, \ldots, v_m$, что любой вектор $w \in \mathbb{F}$ линейно выражается через них в виде $w = x_1 v_1 + \ldots + x_m v_m$, где все $x_i \in \mathbb{F}_p$. Удаляя из набора $v_1, \ldots, v_m$ все векторы, которые линейно выражаются через оставшиеся, мы получим такой набор векторов $\{e_1, \ldots, e_n\} \subset \{v_1, \ldots, v_m\}$, через который каждый вектор $w \in \mathbb{F}$ выражается единственным способом, так как равенство $x_1 e_1 + \ldots + x_n e_n = y_1 e_1 + \ldots + y_n e_n$, в котором $x_i \neq y_i$ для какого-нибудь i, позволяет выразить e_i через остальные векторы как $e_i = \sum_{\nu \neq i} e_\nu (y_\nu - x_\nu)/(x_i - y_i)$, что невозможно. Коль скоро каждый элемент поля $\mathbb{F}$ однозначно записывается в виде $x_1 e_1 + \ldots + x_n e_n$, где каждый коэффициент x_i независимо принимает p значений, мы заключаем, что $|\mathbb{F}| = p^n$.

Упр. 2.23. См. доказательство теоремы Эйлера из прим. 1.6 на стр. 28.

Упр. 2.24. Отображение $\mathrm{ev}_\zeta : \mathbb{F}_p[x] \to \mathbb{F}$, $f \mapsto f(\zeta)$, является гомоморфизмом колец. Поскольку поле $\mathbb{F}$ конечно, а кольцо многочленов $\mathbb{F}_p[x]$ бесконечно, у этого гомоморфизма ненулевое ядро. Многочлен g — это приведённый многочлен минимальной степени в $\ker \mathrm{ev}_\zeta$. Если $g(x) = h_1(x)\,h_2(x)$, то $h_1(\zeta) = 0$ или $h_2(\zeta) = 0$, что по выбору g невозможно при $\deg h_1, \deg h_2 < \deg g$. Пусть $f(\zeta) = 0$ для $f = gh + r$, где $\deg r < \deg g$ или $r = 0$. Подставляя $x = \zeta$, получаем $r(\zeta) = 0$, откуда $r = 0$.

Упр. 3.1. Воспользуйтесь лем. 3.1.

Упр. 3.2. По теор. 3.1 на стр. 54 эпиморфизм $\pi : K = \mathbb{Z}/(30) \twoheadrightarrow \mathbb{Z}/(15)$, $[n]_{30} \mapsto [n]_{15}$, раскладывается в композицию гомоморфизма $\iota_S : K \to KS^{-1}$ и гомоморфизма

$$\pi_S : KS^{-1} \twoheadrightarrow \mathbb{Z}/(15)\,, \quad [m]_{30}/[2^k]_{30} \mapsto [m]_{15}[2^k]_{15}^{-1}\,,$$

сюръективного в силу сюръективности π. Если $[m]_{30}/[2^k]_{30} \in \ker \pi_S$, то $[m]_{15} = 0$, а значит, $[m]_{30}/[2^k]_{30} = [2m]_{30}/[2^{k+1}]_{30} = 0$ в KS^{-1}. Тем самым, $\ker \pi_S = 0$ и π_S инъективен.

Упр. 3.4. По правилу дифференцирования композиции $\left(f^m\right)' = m f^{m-1} f'$, откуда

$$\frac{d}{dx}(1-x)^{-m} = \frac{d}{dx}\left(\frac{1}{1-x}\right)^m = m(1-x)^{-(m+1)}\,.$$

Нужная формула получается отсюда по индукции.

Упр. 3.5. Первое равенство вытекает и правила дифференцирования сложной функции[1], второе доказывается дифференцированием обеих частей.

[1] См. формулу (2-8) на стр. 38.

Упр. 3.9. Ответы: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$, $a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30$$
$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12$$
$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500\,.$$

Упр. 3.10. Подставьте $t = 1$ в $(m+1)\,S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}$.

Упр. 4.1. Импликации (а)⇒(б)⇒(в) очевидны. Если I содержит обратимый элемент, то среди его кратных есть единица, кратные которой исчерпывают всё кольцо.

Упр. 4.2. Первое очевидно, второе вытекает из того, что суммы $b_1a_1 + \ldots + b_ma_m$, где $a_i \in M$, $b_i \in K$, лежат во всех идеалах, содержащих M.

Упр. 4.3. Если a и b являются старшими коэффициентами многочленов f и g из идеала I, и $\deg f = m$, а $\deg g = n$, где $m \geqslant n$, то $a + b$ либо нуль, т. е. является старшим коэффициентом нулевого многочлена, либо является старшим коэффициентом многочлена $f + x^{m-n}g \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 4.4. Повторите доказательство теор. 4.1, следя за младшими коэффициентами вместо старших.

Упр. 4.6. Обозначим через I_0 идеал, образованный всеми аналитическими функциями[1], обращающимися в нуль на множестве $\mathbb{Z} \subset \mathbb{C}$, а через I_k — идеал всех функций, обращающихся в нуль на множестве $\mathbb{Z} \smallsetminus \{1,\ 2,\ \ldots\ ,\ k\}$. Убедитесь, что $\sin(2\pi z)/\prod_{\alpha=1}^{k}(z-\alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 4.7. Из того, что I является абелевой подгруппой в K немедленно вытекает, что отношение $a_1 \equiv a_2 \pmod{I}$ рефлексивно, транзитивно и симметрично. Корректность операций проверяется так же, как в упр. 0.9: если $[a']_I = [a]_I$ и $[b']_I = [b]_I$, т. е. $a' = a + x$, $b' = b + y$ с некоторыми $x, y \in I$, то $a' + b' = a + b + (x + y)$ и $a'b' = ab + (ay + bx + xy)$ сравнимы по модулю I с $a + b$ и ab соответственно, поскольку суммы в скобках лежат в I (именно в этот момент мы пользуемся тем, что идеал вместе с каждым элементом содержит и все его кратные); таким образом, $[a' + b']I = [a + b]_I$ и $[a'b']_I = [ab]_I$.

Упр. 4.8. Возьмите в качестве J^* объединение всех идеалов из M.

Упр. 4.9. В (а) всякий идеал в $\mathbb{C}[x]$ является главным. Если факторкольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то многочлен f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. В (б) с помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $[0, 1] \to \mathbb{R}$ найдётся точка $p \in [0, 1]$, в которой все функции из I обращаются в нуль, что даст включение $I \subset \ker \mathrm{ev}_p$. В (в) подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 4.11. Если в каждом идеале I_k есть элемент $x_k \in I_k \smallsetminus \mathfrak{p}$, то произведение этих элементов $x_1 \ldots x_m \in \bigcap I_k \subset \mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

[1] Функция $\mathbb{C} \to \mathbb{C}$ называется *аналитической*, если она задаётся сходящимся всюду в $\mathbb{C}$ степенным рядом из $\mathbb{C}[\![z]\!]$.

Упр. 4.12. Рассмотрим эпиморфизм факторизации $\pi : K \twoheadrightarrow K/I$. Полный прообраз $\pi^{-1}(J)$ любого идеала $J \subset K/I$ является идеалом в K. Классы элементов, порождающих этот идеал в K порождают идеал J в K/I.

Упр. 4.13. В (в) и (г) для любого $z \in \mathbb{C}$ в рассматриваемом кольце существует такой элемент w, что $|z - w| < 1$. Взяв такой w для $z = a/b$, заключаем, что $|a - bw| < |b|$.

Упр. 4.14. Если $\exists\ b^{-1}$, то $\nu(ab) \leqslant \nu(abb^{-1}) = \nu(a)$. Наоборот, если $\nu(ab) = \nu(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $\nu(r) < \nu(ab) = \nu(a)$, либо $r = 0$. Из равенства $r = a(1 - bq)$ вытекает, что либо $\nu(r) \geqslant \nu(a)$, либо $1 - bq = 0$. С учётом предыдущего, такое возможно только при $1 - bq = 0$ или $r = 0$. Во втором случае $a(1 - bq) = 0$, что тоже влечёт $1 - bq = 0$. Следовательно $bq = 1$ и b обратим.

Упр. 4.15. Если $b = ax$ и $a = by = axy$, то $a(1 - xy) = 0$, откуда $xy = 1$.

Упр. 4.16. Многочлены x и y не имеют в $\mathbb{Q}[x, y]$ никаких общих делителей, кроме констант. Общими делителями элементов 2 и x в $\mathbb{Z}[x]$ являются только ± 1.

Упр. 4.17. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a + b\sqrt{5}$ число $\overline{\vartheta} = a - b\sqrt{5}$, а целое число $\|\vartheta\| \stackrel{\text{def}}{=} \vartheta \cdot \overline{\vartheta} = a^2 - 5b^2$ назовём *нормой* числа ϑ. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1 \cdot \overline{\vartheta}_2$, откуда $\|\vartheta_1\vartheta_2\| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = \|\vartheta_1\| \cdot \|\vartheta_2\|$. Поэтому $\vartheta \in \mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $\|\vartheta\| = \pm 1$, и в этом случае $\vartheta^{-1} = \pm\overline{\vartheta}$. Поскольку $\|2\| = 4$, а $\|1 \pm \sqrt{5}\| = -4$, разложение этих элементов в произведение xy с необратимыми x и y возможно только при $\|x\| = \|y\| = \pm 2$. Но элементов нормы ± 2 в $\mathbb{Z}[\sqrt{5}]$ нет, так как равенство $a^2 - 5b^2 = \pm 2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm 2$ в поле $\mathbb{F}_5$, где числа ± 2 не являются квадратами.

Упр. 4.18. Из равенства $z_1 z_2 = 1$ вытекает равенство $|z_1| \cdot |z_2| = 1$. Так как $|z|^2 \in \mathbb{N}$ для всех $z \in \mathbb{Z}[i]$, гауссово число z может быть обратимо только если $|z| = 1$.

Упр. 4.19. Пусть $n = p_1^{\alpha_1} \dots p_s^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}$, где $p_i, q_j \in \mathbb{N}$ — попарно разные простые числа, причём p_i представляются в виде суммы двух квадратов, а q_j — нет, т. е. все $q_j \equiv 3 \pmod 4$, а все p_i — нет. Тогда разложение n на простые множители в области $\mathbb{Z}[i]$ имеет вид

$$n = \prod\nolimits_i (x_i + iy_i)^{\alpha_i}(x_i - iy_i)^{\alpha_i} \prod\nolimits_j q_j^{\beta_j}\,, \text{ где } q_j \in \mathbb{N}\,.$$

Если все β_j чётные, то $n = (a+ib)(a-ib) = a^2+b^2$ для $a+ib = \prod_i (x_i+iy_i)^{\alpha_i} \prod_j q_j^{\beta_j/2}$. Наоборот, пусть $n = a^2 + b^2 = (a + ib)(a - ib)$, и разложение гауссова числа $a + ib$ на простые множители в $\mathbb{Z}[i]$ имеет вид $a + bi = \prod_k \ell_k^{\gamma_k}$. Тогда разложение числа n на простые множители в $\mathbb{Z}[i]$ имеет вид $\prod_k \ell_k^{\gamma_k}\overline{\ell}_k^{\gamma_k}$, и все вещественные простые множители входят в него в чётных степенях.

Упр. 4.22. Это следует из равенства $a_0 q^n + a_1 q^{n-1} p + \ \dots\ + a_{n-1} q p^{n-1} + a_n p^n = 0$

Упр. 4.23. Ответ: $(x^2 - 2x + 2)(x^2 + 2x + 2)$.