А. Л. Городенцев[1]

Курс алгебры для факультета математики ГУ – ВШЭ

Первый курс

Модуль I

Это несколько расширенные записки лекций по алгебре для первого курса, читанных осенью 2008 года в первом учебном модуле на факультете математики ГУ – ВШЭ. Это интенсивный курс, рассчитанный на две пары лекций и две пары упражнений в неделю. Он посвящён знакомству с алгебраическими свойствами отображений, группами преобразований, гомоморфизмами групп, а также с полями, коммутативными кольцами и их гомоморфизмами. Большинство встречающихся в тексте упражнений существенно для понимания и используется в дальнейшем.

Москва,
ноябрь 2008

[1]Факультет математики ГУ – ВШЭ & Группа математической физики ИТЭФ
`mailto: gorod@itep.ru`
`http://wwwth.itep.ru/~gorod`

Содержание

§1. Множества и отображения.

1.1. Символические сокращения. В этих записках мы иногда заменяем стандартные словесные обороты следующими символическими сокращениями:

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ — множества *натуральных*, *целых*, *рациональных*, *действительных* и *комплексных* чисел соответственно.

$\Rightarrow$ и $\iff$ — «влечёт» и «равносильно»; например, $k \in \mathbb{Z} \Rightarrow k(k+1)/2 \in \mathbb{Z}$; или: x — чётно $\iff$ $x = 2k$, где $k \in \mathbb{Z}$.

$\forall$ — «для любого»; например: $\forall\, k \in \mathbb{Z}\;\; k(k+1)/2 \in \mathbb{Z}$.

$\exists$ — «существует»; например: $x \in \mathbb{Z}$ чётно $\iff \exists\, k \in \mathbb{Z}$, такой что $x = 2k$.

: — «такой что»; например: $x \in \mathbb{Z}$ чётно $\iff \exists\, k \in \mathbb{Z} \,:\, x = 2k$.

$\{x \in X \mid \dots\}$ или $\{x \in X : \dots\}$ — множество всех $x \in X$, для которых выполняется свойство « ... »; например, формула $\{x \in \mathbb{Z} \mid \exists\, k \in \mathbb{Z} : 2k = x\}$ задаёт множество чётных чисел.

$\{\dots\}$ — множество чего-то, что описывается текстом « ... »; например: {чётные числа}.

1.2. Множества. В курсе алгебры мы не будем заниматься основаниями теории множеств[1], полагаясь на почерпнутые из школы интуитивные представления о множестве как «абстрактной совокупности произвольных объектов[2]». Множества состоит из *элементов*, которые мы часто будем называть *точками*. Множество задано, как только про любой объект можно сказать, является он точкой данного множества или нет. Принадлежность точки x множеству X записывается как $x \in X$. Все точки в любом множестве, по определению, *различны*. Два множества *равны*, если они состоят из одних и тех же элементов. Кроме того, существует единственное множество, не содержащее ни одного элемента. Оно называется *пустым* и обозначается $\varnothing$. Множество X называется *подмножеством* множества Y (обозначение: $X \subset Y$), если каждый элемент $x \in X$ лежит также и в Y. В частности, пустое множество является подмножеством любого множества.

Упражнение 1.1. Сколько различных подмножеств (включая пустое и всё множество) имеется у множества, состоящего из n элементов?

Для любых двух множеств X и Y множество $X \cup Y$, состоящее из всех элементов, принадлежащих хотя бы одному из них, называется их *объединением*; множество $X \cap Y$, состоящее из всех элементов, принадлежащих одновременно каждому из них, называется их *пересечением*; множество $X \smallsetminus Y$, состоящее из всех элементов множества X, которые не содержатся в Y, называется их *разностью*.

Упражнение 1.2. 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 множеств Y и Z, таких что $Y \cap Z = \varnothing$, то это записывается как $X = Y \sqcup Z$ и называется *дизъюнктным объединением*. Множество $X \times Y$, элементами которого являются, по определению, всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

[1] чуть позже вы познакомитесь с ними в курсе математической логики

[2] на самом деле в теории множеств, как и в программировании, надо зафиксировать некоторый набор выразительных средств («язык») и ограничиться только такими «совокупностями» и «объектами», которые можно описать посредством этого языка; однако прежде, чем придумывать новый язык программирования, разумно спросить себя, чего мы от него хотим; минимальный набор требований к *языку теории множеств*, который вы будете изучать в курсе логики, как раз и состоит в том, чтобы на нём можно было непротиворечиво выразить всё, чему вас обучат в курсах алгебры, геометрии и анализа

1.3. Отображения. Отображение $X \xrightarrow{f} Y$ из множества X в множество Y — это правило, сопоставляющее каждой точке $x \in X$ некоторую точку $f(x) \in Y$, однозначно определяемую по x. Эта точка называется *образом* точки x при отображении f. Множество всех точек x, образ которых равен данной точке $y \in Y$ обозначается

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

и называется *полным прообразом*[1] точки y. Полный прообраз может быть как пустым, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, обозначается

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

и называется *образом отображения* $X \xrightarrow{f} Y$.

Два отображения $X \xrightarrow{f} Y$ и $X \xrightarrow{g} Y$ *равны*, если их значения в каждой точке одинаковы: $f(x) = g(x) \quad \forall\, x \in X$. Множество всех отображений из множества X в множество Y обозначается $\operatorname{Hom}(X, Y)$. При $X = Y$ отображения $X \longrightarrow X$ обычно называют *эндоморфизмами* множества X и пишут $\operatorname{End}(X)$ вместо $\operatorname{Hom}(X, X)$. У всякого множества X имеется *тождественный эндоморфизм* $X \xrightarrow{\operatorname{Id}_X} X$, который переводит каждый элемент в самого себя: $\forall\, x \in X \;\; \operatorname{Id}_X(x) = x$.

Отображение $X \xrightarrow{f} Y$ называется *наложением* (а также *сюрьектцией* или *эпиморфизмом*), если $\operatorname{im}(f) = Y$, т. е. прообраз каждой точки $y \in Y$ не пуст. Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, т. е. прообраз каждой точки $y \in Y$ содержит не более одной точки. При желании подчеркнуть, что отображение инъективно (соотв. сюрьективно), мы будем изображать его стрелкой $X \hookrightarrow Y$ (соотв. $X \twoheadrightarrow Y$).

Упражнение 1.3. Нарисуйте все отображения а) $\{0, 1, 2\} \longrightarrow \{0, 1\}$; б) $\{0, 1\} \longrightarrow \{0, 1, 2\}$. Сколько среди них сюрьективных и сколько инъективных?

Отображение $X \xrightarrow{f} Y$ называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*), если для каждого $y \in Y$ существует единственный $x \in X$, такой что $f(x) = y$. Иными словами, биективность отображения означает, что оно одновременно является вложением и наложением. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$. Изоморфизмы $X \xrightarrow{\sim} X$ иначе называют *автоморфизмами* или *симметриями*. В «житейском» понимании, автоморфизмы — это *перестановки элементов*. Множество всех автоморфизмов множества X обозначается через $\operatorname{Aut}(X)$.

Упражнение 1.4. Какие из отображений: $\mathbb{Z} \xrightarrow{x \mapsto x^2} \mathbb{Z}$; $\mathbb{N} \xrightarrow{x \mapsto x^2} \mathbb{N}$; $\mathbb{Z} \xrightarrow{x \mapsto 7x,} \mathbb{Z}$; $\mathbb{R} \xrightarrow{x \mapsto 7x,} \mathbb{R}$ являются а) биекциями, б) инъекциями, в) сюрьекциями?

1.3.1. Пример: отображения и слова. Пусть $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_m\}$. Сопоставим каждому отображению $X \xrightarrow{f} Y$ выписанный в ряд слева направо набор его значений:

$$w(f) \stackrel{\text{def}}{=} (f(x_1),\, f(x_2),\, \ldots\, ,\, f(x_n)) \tag{1-1}$$

и будем воспринимать его как n-буквенное слово, написанное при помощи m-буквенного алфавита

$$y_1\, y_2\, \cdots\, y_m \,.$$

Например, отображениям $\{1, 2\} \xrightarrow{f} \{1, 2, 3\}$ и $\{1, 2, 3\} \xrightarrow{g} \{1, 2, 3\}$

$$f: \begin{tikzcd}[row sep=tiny] & 1 \\ 1 \arrow[ddr] & \\ & 2 \\ 2 \arrow[ur] & \\ & 3 \end{tikzcd} \qquad g: \begin{tikzcd} 1 \arrow[r] & 1 \\ 2 \arrow[r] & 2 \\ 3 \arrow[ur] & 3 \end{tikzcd}$$

[1] а также *слоем* отображения f над точкой y

отвечают слова $w(f) = (3,2)$ и $w(g) = (1,2,2)$, составленные из букв трёхбуквенного алфавита $\{1,\, 2,\, 3\}$. Очевидно, что построенное нами отображение

$$w : \mathrm{Hom}(X,Y) \xrightarrow{\sim} \{n\text{-буквенные слова в алфавите } y_1\; y_2\; \dots\; y_m\} \tag{1-2}$$

является биекцией.

1.3.2. ПРЕДЛОЖЕНИЕ. *Если множество X состоит из n элементов, а множество Y — из m, то множество $\mathrm{Hom}(X,Y)$ состоит из m^n элементов.*

Доказательство. Обозначим через $W_m(n)$ количество всех n-буквенных слов, которые можно написать при помощи алфавита из m букв. Выпишем все эти слова на m страницах, поместив на i-тую страницу все слова, начинающиеся на i-тую букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Стало быть $W_m(n) = m \cdot W_m(n-1) = m \cdot m \cdot W(n-2) = \dots = m^{n-1} \cdot W(1) = m^n$. □

1.3.3. ПРЕДЛОЖЕНИЕ. *У n-элементного множества имеется ровно $n!$ автоморфизмов.*

Доказательство. Пусть $X = \{x_1, x_2, \dots, x_n\}$. Построенный в n° 1.3.1 изоморфизм (1-2) между отображениями и словами устанавливает взаимно однозначное соответствие между биекциями $X \xrightarrow{f} X$ и n-буквенными словами (в алфавите $x_1, x_2, \dots, x_n$), содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. На каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \dots = n \cdot (n-1) \cdot (n-2) \cdot\; \cdots \;\cdot 2 \cdot 1 = n!\,.$ □

Упражнение 1.5 («принцип Дирихле»). Покажите, что следующие три условия на множество X попарно равносильны друг другу: а) X бесконечно; б) $\exists$ вложение $X \hookrightarrow X$, не являющееся наложением; в) $\exists$ наложение $X \twoheadrightarrow X$, не являющееся вложением.

Упражнение 1.6. Счётно ли множество $\mathrm{Aut}\,(\mathbb{N})$?

1.4. Отображения и разбиения. Со всяким отображением $X \xrightarrow{f} Y$ связано разбиение множества X в объединение непересекающихся подмножеств — полных прообразов различных точек $y \in Y$. Поэтому задать отображение $X \xrightarrow{f} Y$ — это то же самое, что представить X в виде объединения непустых непересекающихся подмножеств и занумеровать эти подмножества точками $y \in \mathrm{im}\,(f)$:

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

Такой взгляд на отображения часто оказывается полезным.

1.4.1. Пример: другое доказательство предложений (n° 1.3.2)–(n° 1.3.3). Обозначим через $\mathrm{Map}_{\,m,n}$ множество всех отображений из n-элементного множества X в m-элементное множество Y, зафиксируем какой-нибудь элемент $x \in X$ и рассмотрим *отображение вычисления*

$$\mathrm{ev}_x : \mathrm{Map}_{\,m,n} \xrightarrow{f \mapsto f(x)} Y_m\;, \tag{1-4}$$

которое сопоставляет каждому отображению $X \xrightarrow{f} Y$ его значение в точке x. Отображение вычисления, очевидно, сюрьективно. Прообраз каждой точки $y \in Y$ находится во взаимно однозначном соответствии с множеством всех отображений из $(n-1)$-элементного множества $X \smallsetminus \{x\}$, получающегося выкидыванием из X точки x, в Y:

$$\mathrm{ev}_x^{-1}(y) = \{X_n \xrightarrow{f} Y \mid f(x) = y\} \simeq \mathrm{Hom}\,(X \smallsetminus \{x\}\,,\, Y) \simeq \mathrm{Map}_{\,m,(n-1)}\;.$$

Разложение (1-3) означает в этом случае, что множество $\mathrm{Map}_{\,m,n}$ распадается в дизъюнктное объединение m подмножеств, каждое из которых изоморфно $\mathrm{Map}_{\,m,(n-1)}$. Поэтому[1]

$$|\mathrm{Map}_{\,m,n}| = m \cdot |\mathrm{Map}_{\,m,(n-1)}| = m \cdot m \cdot |\mathrm{Map}_{\,m,(n-2)}| = \;\cdots\; = m^{n-1} \cdot |\mathrm{Map}_{\,m,1}| = m^n\,.$$

Аналогичным образом, обозначим через $\mathfrak{S}_n$ множество автоморфизмов n-элементного множества X, зафиксируем $x \in X$ и рассмотрим *отображение вычисления*

$$\mathrm{ev}_x : \mathfrak{S}_n \xrightarrow{f \mapsto f(x)} X_n\;.$$

[1] здесь и далее мы обозначаем через $|M|$ число элементов в конечном множестве M

Повторяя предыдущее рассуждение, мы видим, что $\mathfrak{S}_n$ распадается в объединение непересекающихся слоёв отображения ev_x, причём слой $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X$ состоит из всех биекций $X \xrightarrow{\sim} X$, переводящих x в x', и тем самым, находится во взаимно однозначном соответствии с множеством всех биекций между $(n-1)$-элементным множеством $X \smallsetminus \{x\}$ и $(n-1)$-элементным множеством $X' = X \smallsetminus \{x'\}$. Поэтому число элементов во всех слоях одинаково и равно $|\mathfrak{S}_{n-1}|$. Стало быть, $|\mathfrak{S}_n| = n \cdot |\mathfrak{S}_{n-1}| = n \cdot (n-1) \cdot |\mathfrak{S}_{n-2}| = \cdots = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!$.

Внимательно сопоставляя только что проведённые рассуждения с доказательствами из (n° 1.3.2–n° 1.3.3), нетрудно составить «словарик», позволяющий переговаривать одни в другие. Так фраза «зафиксируем какой-нибудь элемент $x \in X$» из нынешнего доказательства на языке (n° 1.3.2–n° 1.3.3) звучала бы как «зафиксируем в слове $w(f)$ какою-нибудь позицию, например, будем смотреть на *самую левую* букву слова». При этом «самую левую» в нынешнем рассуждении означает, что в качестве $x \in X$ фиксируется $x = x_1$, а «смотреть, чему равна самая левая буква в слове $f(w)$» — это «применить к f отображение вычисления ev_{x_1}». Читателю рекомендуется детально проследить это соответствие до конца.

1.4.2. Пример: мультиномиальные коэффициенты. При раскрытии скобок и приведении подобных слагаемых в выражении $(a_1 + a_2 + \cdots + a_k)^n$ будут получаться взятые с некоторыми коэффициентами одночлены $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$, показатели которых принимают любые целые значения $0 \leqslant m_i \leqslant n$ суммарной степени $m_1 + m_2 + \cdots + m_k = n$, т. е.

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{m_1 + m_2 + \cdots + m_k = n} \binom{n}{m_1 \ldots m_k} \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k} , \tag{1-5}$$

где через $\binom{n}{m_1 \ldots m_k}$ обозначен коэффициент, возникающий при соответствующем одночлене[1]. Умножение n скобок $(a_1 + a_2 + \cdots + a_k)$ заключается в выборе внутри каждой из скобок какой-нибудь буквы, перемножении этих букв (визуально эта операция заключается в выписывании выбранных букв слева направо друг за другом в одно n-буквенное слово) и суммировании всех таких слов. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$ — это в точности всевозможные слова из m_1 букв a_1, m_2 букв a_2, … , m_k букв a_k. Чтобы подсчитать их количество, сделаем m_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с m_2 буквами a_2, m_3 буквами a_3 и т. д. В результате получится набор из $n = m_1 + m_2 + \cdots + m_k$ попарно различных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(m_1)}}_{m_1 \text{ меченых букв } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(m_2)}}_{m_2 \text{ меченых букв } a_2}, \ldots \ldots \ldots, \underbrace{a_k^{(1)}, a_k^{(2)}, \ldots, a_k^{(m_k)}}_{m_k \text{ меченых букв } a_k} . \tag{1-6}$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, всего таких слов будет $n!$. Теперь обозначим через Y интересующее нас множество слов из m_1 одинаковых букв a_1, m_2 одинаковых букв a_2, … , m_k одинаковых букв a_k, и рассмотрим отображение $X \xrightarrow{f} Y$, которое стирает верхние индексы у помеченных букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $m_1! \cdot m_2! \cdot \cdots \cdot m_k!$ слов, получающихся всевозможными перестановками m_1 верхних индексов у букв $a_1^{(j)}$, m_2 верхних индексов у букв $a_2^{(j)}$, … , m_k верхних индексов у букв $a_k^{(j)}$ в каком-нибудь одном слове $x \in X$, переходящем в y. Из разложения (1-3) вытекает равенство

$$\binom{n}{m_1 \ldots m_k} = \frac{n!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!} , \tag{1-7}$$

и формула (1-5) приобретает вид

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{m_1 + m_2 + \cdots + m_k = n} \frac{n! \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!} . \tag{1-8}$$

При $k = 2$ она превращается в известную формулу раскрытия бинома с натуральным показателем[2]:

$$(a+b)^n = \sum_{k=0}^{n} \frac{n! \cdot a^k b^{n-k}}{k!(n-k)!} . \tag{1-9}$$

[1] он называется *мультиномиальным коэффициентом*

[2] это частный случай *формулы Ньютона*, которую мы обсудим в полной общности в примере (n° 8.6), когда будем заниматься степенными рядами

Упражнение 1.7. Из скольких слагаемых состоит сумма в правой части формулы (1-8)?

1.4.3. Разбиения и отношения. Альтернативный способ задавать разбиение данного множества X в объединение непересекающихся подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество разбиения «эквивалентными». Формальное описание этой процедуры таково. Назовём *бинарным отношением* на множестве X произвольное подмножество $R \subset X \times X$ в множестве всех упорядоченных пар

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

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

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

$$\underset{R}{\sim} \;:=\; «\leqslant» \qquad (x_1 \leqslant x_2 \text{ означает, что } x_1 \text{ не превосходит } x_2) \tag{1-10}$$

$$\underset{R}{\sim} \;:=\; «\,\vdots\,» \qquad (x_1 \,\vdots\, x_2 \text{ означает, что } x_1 \text{ делится на } x_2) \tag{1-11}$$

$$\underset{R}{\sim} \;:=\; «=» \qquad (x_1 = x_2 \text{ означает, что } x_1 \text{ равен } x_2) \tag{1-12}$$

$$\underset{R}{\sim} \;:=\; «\equiv \pmod n» \qquad (x_1 \equiv x_2 \pmod n \text{ означает}^1\text{, что } (x_1 - x_2) \,\vdots\, n) \tag{1-13}$$

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

$$\forall\, x \in X \;\; x \underset{R}{\sim} x\,; \qquad (\textit{рефлексивность}) \tag{1-14}$$

$$\forall\, x_1, x_2, x_3 \in X \;\; (x_1 \underset{R}{\sim} x_2 \;\&\; x_2 \underset{R}{\sim} x_3) \;\Rightarrow\; x_1 \underset{R}{\sim} x_3\,; \qquad (\textit{транзитивность}) \tag{1-15}$$

$$\forall\, x_1, x_2 \in X \quad x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1\,. \qquad (\textit{симметричность}) \tag{1-16}$$

Так, отношения (1-12) и (1-13) являются эквивалентностями, а (1-10) и (1-11) — нет (они несимметричны).

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, если на множестве X задано какое-нибудь отношение эквивалентности R, назовём *классом эквивалентности* элемента $x \in X$ множество

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

(равенство выполняется благодаря симметричности отношения R). Если пересечение каких-нибудь двух классов $[x]_R$ и $[y]_R$ не пусто, то $x \underset{R}{\sim} z \underset{R}{\sim} y$ для $z \in [x]_R \cap [y]_R$, откуда $x \underset{R}{\sim} y$ и $[x]_R = [y]_R$ в силу (1-15, 1-16). Таким образом, любые два класса эквивалентности или не пересекаются или совпадают, а значит, X разбивается в дизъюнктное объединение различных классов эквивалентности. Итак, разбиение X в объединение непересекающихся подмножеств равносильно заданию на X какого-нибудь отношения эквивалентности.

1.4.4. Отступление: частично упорядоченные множества. Бинарное отношение $\underset{R}{\sim}$ называется *частичным порядком*, если оно рефлексивно и транзитивно, но (в отличие от эквивалентности) не симметрично, а *антисимметрично*, т. е.

$$\forall\, x_1, x_2 \in X \;\; (x_1 \underset{R}{\sim} x_2 \;\&\; x_2 \underset{R}{\sim} x_1) \;\Rightarrow\; x_1 = x_2 \qquad (\textit{антисимметричность}) \tag{1-17}$$

Из бинарных отношений (1-10)–(1-11) на множестве целых чисел $\mathbb{Z}$ частичными порядками являются первые три, а четвёртое — нет[2].

---

[1] обозначение $x_1 \equiv x_2 \pmod n$ читается «x_1 сранимо с x_2 по модулю n»

[2] целые числа -12 и 6 не равны, но $-12 \equiv 6 \pmod 9$ и $6 \equiv -12 \pmod 9$

Упражнение 1.8. Будут ли частичными порядками следующие отношения на множестве минутных делений циферблата механических часов:

а) $x \preccurlyeq y$, если исчисляемый против часовой стрелки угол от x к y меньше $30°$

б) $x \preccurlyeq y$, если после полудня минутная стрелка укажет на x раньше, чем на y

(ответ можно подглядеть в сноске ([1])).

Множество с заданным на нём отношением частичного порядка «$\leqslant$» называется *частично упорядоченным множеством* (сокр. ЧУМом). Если $x \leqslant y$ и одновременно $x \neq y$, то это записывают как $x < y$ и говорят, что x *строго* меньше y в смысле заданного отношения «$\leqslant$» .

Упражнение 1.9. Убедитесь, что единственное бинарное отношение, которое является одновременно эквивалентностью и частичным порядком, — это равенство.

1.4.5. Пример: возрастающие и неубывающие отображения. Рассмотрим $X_m = \{1, 2, \dots, m\}$ как упорядоченное множество (со стандартным отношением порядка $\leqslant$). Отображение $X_m \xrightarrow{\varphi} X_n$ называется *возрастающим* (или *строго сохраняющим порядок*), если

$$\forall\, x_1, x_2 \quad x_1 < x_2 \quad \Rightarrow \quad \varphi(x_1) < \varphi(x_2)\ ,$$

и *неубывающим* (или *нестрого сохраняющим порядок*), если

$$\forall\, x_1, x_2 \quad x_1 \leqslant x_2 \quad \Rightarrow \quad \varphi(x_1) \leqslant \varphi(x_2)\ .$$

Между множеством неубывающими отображений $X_m \xrightarrow{\varphi} X_n$ и множеством возрастающих отображений $X_m \xrightarrow{\psi} X_{n+m-1}$ имеется биекция, которая переводит неубывающее отображение $X_m \xrightarrow{\varphi} X_n$ в строго возрастающее отображение $X_m \xrightarrow{\psi} X_{n+m-1}$, заданное формулой $\psi(k) = \varphi(k) + k - 1$ где $k = 1, 2, \dots, m \in X_m$.

1.5. Композиция отображений. Последовательное выполнение двух отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

называется *композицией*. Получающееся в результате отображение $X \longrightarrow Z$, переводящее каждую точку $x \in X$ в точку $g(f(x)) \in Z$, обозначается $g{\circ}f$ или просто gf.

Упражнение 1.10. Убедитесь, что отображение $X \xrightarrow{g} Y$

а) инъективно тогда и только тогда, когда существует отображение $Y \xrightarrow{f} X$, такое что $fg = \mathrm{Id}_X$ (всякое такое f называется *левым обратным* к g);

б) сюрьективно тогда и только тогда, когда существует отображение $Y \xrightarrow{h} X$, такое что $gh = \mathrm{Id}_Y$ (всякое такое f называется *правым обратным* к g).

Как и умножение чисел, композиция отображений *ассоциативна*[2]:

$$(fg)h = f(gh) \text{ для любой тройки отображений } X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} T \tag{1-18}$$

Упражнение 1.11. Убедитесь, что обе части равенства (1-18) переводят каждый $x \in X$ в $f(g(h(x))) \in T$.

Однако поверхностная аналогия между числами и отображениями на этом кончается. Например, для отображений может не выполняться равенство $fg = gf$ (*коммутативность*, или *переместительный закон*).

Упражнение 1.12. Рассмотрим на плоскости пару разных 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 $\sigma_2\sigma_1$. Когда они равны?

Более того, композиция не всегда определена (нельзя «перемножить» $X \xrightarrow{h} Y$ и $Z \xrightarrow{f} T$, если Y никак не связано с Z), и часто случается, что gf определено, а fg — нет.

Упражнение 1.13. Придумайте соответствующие примеры.

---

[1] ответ: (б) является, а (а) — нет

[2] в начальной школе ассоциативность обычно называют *сочетательным законом*

Отметим, что проблем с неопределённостью композиций не возникает, если $f, g \in \mathrm{End}(X)$ являются эндоморфизмами одного и того же множества X, но сделаем и ещё одно важное предупреждение: даже когда все композиции определены, из равенства $fg_1 = fg_2$, вообще говоря, не следует равенство $g_1 = g_2$, как не следует оно и из равенства $g_1 f = g_2 f$.

Упражнение 1.14. Придумайте соответствующие примеры и покажите, что импликации

$$fg_1 = fg_2 \Rightarrow g_1 = g_2 \quad \text{и} \quad g_1 f = g_2 f \quad \Rightarrow \quad g_1 = g_2$$

имеют место, когда f обладает, соответственно, *левым* и *правым обратным* отображением (что по упр. 1.10 равносильно, соответственно, инъективности и сюрьективности f).

1.5.1. Пример: таблица умножения эндоморфизмов двуэлементного множества. Составим таблицу умножения эндоморфизмов множества $\{1, 2\}$. Будем обозначать эндоморфизмы $\{1, 2\} \xrightarrow{f} \{1, 2\}$ словами $w(f) = ((f(1),\, f(2))$, как в (n° 1.3.1). В этих обозначениях множество $\mathrm{End}(\{1, 2\})$ состоит из четырёх эндоморфизмов $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$ которые перемножаются по правилам:

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

(1-19)

Таблица умножения $\mathrm{End}(\{1, 2\}) \times \mathrm{End}(\{1, 2\}) \xrightarrow{(g,f)\mapsto gf} \mathrm{End}(\{1, 2\})$.

Обратите внимание, что $(2,2)\circ(1,1) \neq (1,1)\circ(2,2)$, а также на то, что в верхней и нижней строках все произведения одинаковы, но «сократить общий множитель» при этом нельзя.

Упражнение 1.15. Для $X = \{1, 2\}$ и $Y = \{1, 2, 3\}$ составьте аналогичные (1-19) таблицы умножения

$$\mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, X) \xrightarrow{(g,f)\mapsto gf} \mathrm{End}(X)$$
$$\mathrm{Hom}(Y, X) \times \mathrm{Hom}(X, Y) \xrightarrow{(f,g)\mapsto fg} \mathrm{End}(Y)\ .$$

1.6. Обратимость. Если отображение $X \xrightarrow{g} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки, и правило $y \mapsto g^{-1}(y)$ задаёт отображение $X \xleftarrow{g^{-1}} Y$, которое называется *обратным* к g. По построению, мы имеем равенства

$$g\circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1}\circ g = \mathrm{Id}_X\ . \tag{1-20}$$

Таким образом, отображение g^{-1} является одновременно и левым и правым обратным к g в смысле упр. 1.10.

1.6.1. ПРЕДЛОЖЕНИЕ. *Следующие условия на отображение $X \xrightarrow{g} Y$ попарно эквивалентны:*

(1) *g взаимно однозначно;*

(2) *существует отображение $X \xleftarrow{g'} Y$, такое что $g\circ g' = \mathrm{Id}_Y$ и $g'\circ g = \mathrm{Id}_X$;*

(3) *g обладает как левым, так и правым обратными отображениями.*

При выполнении этих условий любое отображение g' из (2) и любые левые и правые обратные к g отображения из (3) совпадают друг с другом и с построенным выше отображением g^{-1}.

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была установлена в формуле (1-20). Импликация (2) $\Rightarrow$ (3) очевидна. Докажем, что из (3) вытекают (2) и (1). Если у $X \xrightarrow{g} Y$ есть левое обратное $X \xleftarrow{f} Y$ (такое что $f\circ g = \mathrm{Id}_X$) и правое обратное $X \xleftarrow{h} Y$ (такое что $g\circ h = \mathrm{Id}_Y$), то

$$f = f\circ\mathrm{Id}_Y = f\circ(g\circ h) = (f\circ g)\circ h = \mathrm{Id}_X\circ h = h\ , \tag{1-21}$$

и условие (2) выполняется для $g' = f = h$. Поскольку $g(g'(y)) = y$ для любого $y \in Y$, прообраз $f^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$, и тем самым, не пуст. С другой стороны, для любой точки $x \in g^{-1}(y)$ выполняется равенство $g(x) = y$, а значит, и равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$. Поэтому $f^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, а $g' = g^{-1}$. □

§2. Группы преобразований.

2.1. Группы преобразований. Зафиксируем некоторое множество X. Набор $G \subset \mathrm{Aut}\,(X)$ автоморфизмов множества X называется *группой преобразований* (или просто *группой*), если обратные отображения ко всем преобразованиям из G, а также композиции любых двух преобразований из G тоже лежат в G. Отметим, что при выполнении этих условий G автоматически будет содержать тождественное преобразование $\mathrm{Id}_X = g{\circ}g^{-1}$ (где g — произвольное преобразование из G). Число преобразований, из которых состоит группа G (при условии, что она конечна), называется *порядком группы* и обозначается $|G|$.

2.1.1. Пример: симметрическая группа. Множество $G = \mathrm{Aut}\,(X)$ всех биективных отображений из какого-либо множества X в себя очевидно является группой. Она называется (полной) *симметрической группой* множества X. Симметрическая группа множества $X = \{1, 2, \dots, n\}$ обозначается $\mathfrak{S}_n$ и называется *группой перестановок n элементов*. Согласно n° 1.3.3 она имеет порядок $|\mathfrak{S}_n| = n!$. Мы будем записывать перестановку

$$\{1, 2, \dots, n\} \xrightarrow{\sigma} \{1, 2, \dots, n\}$$

строчкой $(\sigma_1, \sigma_2, \dots, \sigma_n)$ её значений $\sigma_i = \sigma(i)$, как мы это уже делали в примерах (n° 1.3.1) и (n° 1.5.1). В этих обозначениях перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ действуют по правилам

$$\begin{array}{cccccccccccc} & 1 & 2 & 3 & 4 & & & 1 & 2 & 3 & 4 \\ \sigma: & \downarrow & \downarrow & \downarrow & \downarrow & , & \tau: & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 2 & 1 & & & 2 & 3 & 4 & 1 \end{array}$$

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

Упражнение 2.1. Составьте таблицу умножения шести элементов группы $\mathfrak{S}_3$, аналогичную таблице из примера (n° 1.5.1).

2.1.2. Пример: группа поворотов $\boldsymbol{\mu}_n$. Зафиксируем натуральное число $n > 1$. Группа $\boldsymbol{\mu}_n$ состоит из n поворотов координатной плоскости $\mathbb{R}^2$ вокруг начала координат на углы $2\pi k/n$ с $0 \leqslant k \leqslant (n-1)$. Обратным к повороту на угол $2\pi k/n$ является поворот на угол $2\pi(n-k)/n$, равный повороту на угол $-2\pi k/n$. Композиция поворотов на углы $2\pi k/n$ и $2\pi m/n$ является поворотом на угол $2\pi(k+m)/n$. Тождественное преобразование —- это поворот на нулевой угол, отвечающий $k = 0$.

Отметим, что композиция в группе $\boldsymbol{\mu}_n$ *коммутативна*:

$$\forall\, \tau_1, \tau_2 \in \boldsymbol{\mu}_n \quad \tau_1\tau_2 = \tau_2\tau_1\,.$$

Группы, в которых композиция коммутативна, называются *коммутативными* или *абелевыми*.

Элементы группы $\boldsymbol{\mu}_n$ удобно представлять себе в виде циферблата, деления которого изображают углы поворотов, исчисляемые в долях от полного оборота. Скажем, группа $\boldsymbol{\mu}_{12}$ выглядит почти как стандартный 12-часовой циферблат[1] (см. рис. 2◇1). При таком изображении композиции поворотов отвечает последовательное откладывание углов друг за другом, а переходу к обратному повороту — откладывание угла в противоположном направлении.

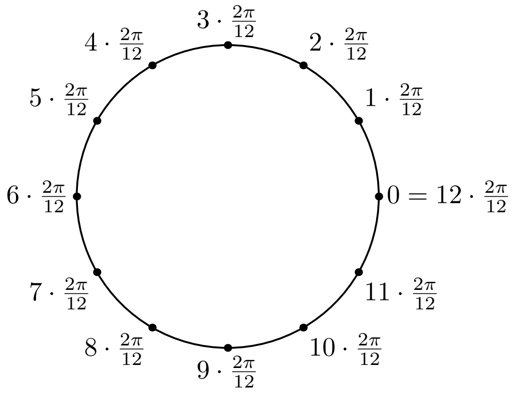


Рис. 2◇1. Циферблат $\boldsymbol{\mu}_{12}$.

Иначе элементы группы $\boldsymbol{\mu}_n$ можно воспринимать как классы целых чисел, дающих одинаковые остатки от деления на n. В самом деле, повороты на $2\pi k/n$ и $2\pi k'/n$ совпадают тогда и только тогда, когда $k' - k$ делится на n, или $k' \equiv k \pmod{n}$ в обозначениях из формулы (1-13). Таким образом, элементы группы $\boldsymbol{\mu}_n$ можно отождествить с остатками от деления на n. Композиция поворотов превратится при этом в известное правило сложения остатков: «остаток суммы двух чисел равен остатку от суммы их остатков».

[1] но с изменённой ориентацией, поскольку увеличению угла отвечает движение против часовой стрелки, и повёрнутый набок, поскольку нулевой угол отвечает направлению горизонтальной координатной оси

2.1.3. Группы движений и группы фигур. Рассмотрим трёхмерное евклидово пространство $\mathbb{R}^3$. Автоморфизмы $f \in \mathrm{Aut}(\mathbb{R}^3)$, которые сохраняют расстояния между точками, называются *движениями*. Движения, очевидно, образуют группу. Собственные движения[1] образуют в группе всех движений подгруппу (она называется *группой собственных движений*).

Если задаться какой-нибудь фигурой $\mathfrak{F} \subset \mathbb{R}^3$, то можно рассмотреть движения, которые переводят $\mathfrak{F}$ в себя. Группа биективных отображений фигуры $\mathfrak{F}$ в себя, определяемых этими движениями, называется (*полной*) *группой фигуры* $\mathfrak{F}$ и обозначается $G(\mathfrak{F}) \subset \mathrm{Aut}(\mathfrak{F})$. Наряду с полной группой фигуры можно рассматривать *собственную* группу фигуры, в которой допускаются только собственные движения. Отметим, что для плоских пространственных фигур собственная группа совпадает с полной: беря композицию любого несобственного движения из группы фигуры с зеркальным отражением относительно содержащей эту фигуру плоскости, мы получим собственное движение, которое действует на фигуру точно также, как и исходное несобственное движение.

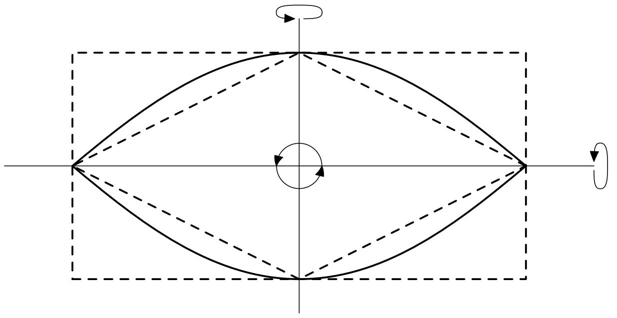


Рис. 2◇2. Группа двуугольника.

Ниже рассматриваются собственные и несобственные группы нескольких известных фигур.

Упражнение 2.2. Изготовьте модели пяти платоновых тел — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра (см. рис. 2◇5 и рис. 2◇9). Все последующие утверждения о движениях этих фигур будут очевидны, если у Вас в руках будет соответствующая модель, но могут показаться «трудными» при попытке постичь их чисто умозрительно.

2.1.4. Пример: группы диэдров $\mathfrak{D}_n$. Группа правильного плоского n-угольника в пространстве называется n-той *группой диэдра*[2] и обозначается $\mathfrak{D}_n$.

Простейший диэдр — двуугольник — это симметричная луночка с двумя сторонами, изображённая на рис. 2◇2. Группа[3] $\mathfrak{D}_2$ состоит из тождественного отображения и трёх поворотов на 180° вокруг перпендикулярных друг другу осей, одна из которых проходит через вершины луночки, другая — через середины её сторон, а третья перпендикулярна плоскости луночки и проходит её центр. Действительно, любое нетождественное преобразование диэдра должно менять местами либо его стороны, либо вершины, либо то и другое сразу, и ровно это и происходит при трёх перечисленных выше поворотах.

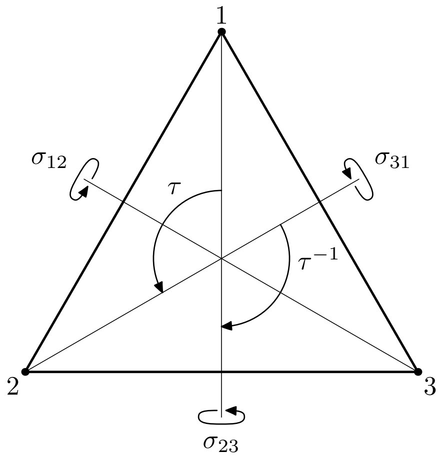


Рис. 2◇3. Группа треугольника.

Упражнение 2.3. Составьте таблицу умножения элементов группы $\mathfrak{D}_2$ и убедитесь, что она коммутативна.

Отметим, что группа $\mathfrak{D}_2$ совпадает как с группой описанного вокруг луночки прямоугольника, так и с группой вписанного в неё ромба, при условии, что оба они не квадраты (см. рис. 2◇2).

Следующий диэдр — правильный треугольник. Покажем, что его группа $\mathfrak{D}_3$ состоит из шести движений (см. рис. 2◇3): тождественного преобразования Id, двух поворотов τ, τ^{-1} на $\pm 120^\circ$ вокруг центра треугольника и трёх осевых симметрий $\sigma_{ij} = \sigma_{ij}^{-1}$ относительно его медиан. Для этого занумеруем вершины треугольника числами 1, 2, 3 и сопоставим каждому движению из группы треугольника осуществляемую им перестановку его вершин. Получим отображение группы диэдра в симметрическую группу:

$$\mathfrak{D}_3 \hookrightarrow \mathfrak{S}_3 = \mathrm{Aut}(\{1, 2, 3\}). \tag{2-1}$$

[1] напомним, что движение называется *собственным*, если оно сохраняет *ориентацию* (говоря наивно, переводит левосторонний винт в левосторонний); например, повороты — это собственные движения, а отражения относительно плоскости и центральная симметрия пространства — нет; если воспользоваться теоремой о том, что любое движение является композицией отражений, то собственные движения — это те, которые можно представить в виде композиции чётного числа отражений

[2] т. е. «двугранника»; имеется в виду, что пространственный многоугольник имеет две визуально неотличимые друг от друга грани — две поверхности плёнки, которую на него можно натянуть

[3] диэдральная группа $\mathfrak{D}_2$ иногда ещё называется *четвертной группой Клейна* и обозначается $\mathfrak{V}_4$

Оно инъективно в силу следующего хорошо известного геометрического факта:

Упражнение 2.4. Докажите, что два движения плоскости совпадают тогда и только тогда, когда они одинаково действуют на вершины какого-нибудь треугольника.

Поскольку группа $\mathfrak{S}_3$ тоже состоит из шести перестановок, отображение (2-1) взаимно однозначно. Повороты на $\pm 120^\circ$ отождествляются им с циклическими перестановками $(2, 3, 1)$ и $(3, 1, 2)$, а осевые симметрии — с транспозициями пар букв $(1, 3, 2)$, $(3, 2, 1)$ и $(2, 1, 3)$.

Упражнение 2.5. Обозначим через $\sigma_{ij} \in \mathfrak{S}_3$ перестановку букв i и j. Убедитесь, что преобразования из группы $\mathfrak{S}_3$ можно записать в виде: Id, σ_{12}, σ_{23}, σ_{13}, $\sigma_{12}\sigma_{23}$, $\sigma_{23}\sigma_{12}$. Где в этом списке повороты $1 \to 2 \to 3 \to 1$ и $3 \to 2 \to 1 \to 3$?

Покажем теперь, что для произвольного $n \geqslant 2$ группа диэдра $\mathfrak{D}_n$ состоит из $2n$ движений: n поворотов вокруг центра многоугольника на углы $2\pi k/n$ с $k = 0, 1, \dots, (n-1)$ (при $k = 0$ получается тождественное преобразование) и n осевых симметрий (т. е. поворотов на 180° в пространстве) относительно прямых, проходящих при нечётном n через вершину и середину противоположной стороны, а при чётном n — через пары противоположных вершин и через середины противоположных сторон (см. рис. 2◇4).

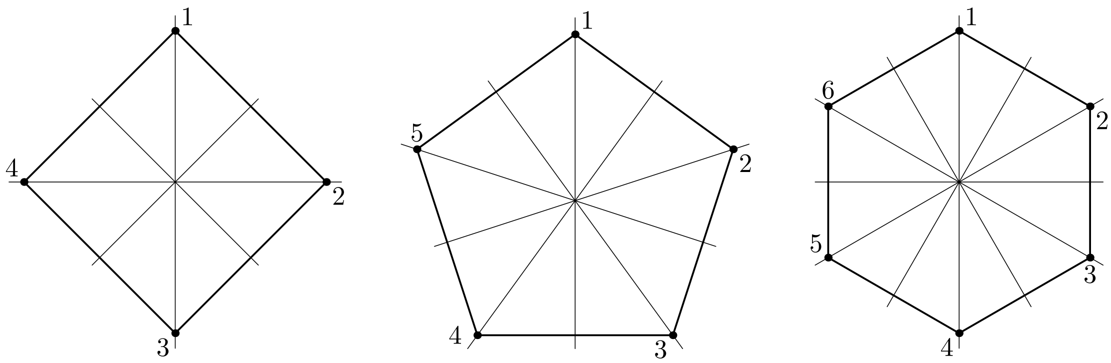


Рис. 2◇4. Оси диэдров для $n = 4, 5, 6$.

Для этого занумеруем вершины диэдра числами $1, 2, \dots, n$ и разобьём все движения из группы диэдра на n непересекающихся классов $C_1, C_2, \dots, C_n$, отнеся в класс C_i все движения, которые переводят вершину 1 в вершину i. Убедимся теперь, что в каждом классе C_i имеется ровно столько же движений, сколько и в классе C_1. Для этого зафиксируем какое нибудь движение $g \in C_i$ и рассмотрим отображения умножения слева на g и на g^{-1}:

$$\gamma : C_1 \xrightarrow{h \mapsto g \circ h} C_i \quad \text{и} \quad \gamma' : C_i \xrightarrow{f \mapsto g^{-1} \circ f} C_1 . \tag{2-2}$$

Легко видеть, что они обратны друг другу:

$$\forall\, f \in C_i \;\; \gamma(\gamma'(f)) = \gamma(g^{-1}f) = gg^{-1}f = f \quad \text{и} \quad \forall\, h \in C_1 \;\; \gamma'(\gamma(h)) = \gamma'(gh) = g^{-1}gh = h ,$$

а значит, в силу предложения (n° 1.6.1), они биективны. Таким образом, $|\mathfrak{D}_n| = n \cdot |C_1|$. Заметим теперь, что согласно упр. 2.4 имеется ровно два движения, переводящих многоугольник в себя и оставляющих на месте вершину 1: тождественное (тождественно действующее на треугольник, образованный вершиной 1 и смежными с ней вершинами 2 и n) и симметрия относительно оси, проходящей через вершину 1 и центр многоугольника (переставляющая вершины 2 и n между собой). Итак, $|C_1| = 2$ и $|\mathfrak{D}_n| = 2n$.

Упражнение 2.6. Составьте таблицы умножения для групп $\mathfrak{D}_3$, $\mathfrak{D}_4$ и $\mathfrak{D}_5$.

2.1.5. Пример: полная и собственная группы правильного тетраэдра. Собственная группа тетраэдра помимо тождественного преобразования содержит $4 \cdot 2 = 8$ поворотов на углы $\pm 120^\circ$ вокруг прямых, проходящих через вершину и центр противоположной грани, а также 3 поворота на 180° вокруг прямых, проходящих через середины противоположных рёбер (см. рис. 2◇5). Отметим, что этих движений достаточно, чтобы перевести любую вершину тетраэдра в любую другую. В несобственной группе, помимо перечисленных поворотов, имеется 6 отражений в плоскостях, проходящих через ребро и середину противоположного к нему ребра. Какие ещё движения есть в группе тетраэдра?

Для ответа на этот вопрос подсчитаем, сколько всего движений имеется в собственной и несобственной группах тетраэдра. Занумеруем вершины числами $1, 2, 3, 4$ и разобьем все движения из (как собственной, так и несобственной) группы тетраэдра на 4 непересекающихся класса C_1, C_2, C_3, C_4, отнеся в класс C_i те движения, которые переводят вершину 1 в вершину i. Зафиксируем какое-нибудь преобразование g, переводящее вершину 1 в вершину i, и рассмотрим, как и в предыдущем примере, отображения

$$\gamma : C_1 \xrightarrow{h \mapsto g \circ h} C_i \quad \text{и} \quad \gamma' : C_i \xrightarrow{f \mapsto g^{-1} \circ f} C_1 , \tag{2-3}$$

умножающие все преобразования из класса C_1 на g, а все преобразований из класса C_i — на g^{-1}.

Упражнение 2.7. Покажите, что γ и γ' являются обратными друг другу биекциями между C_1 и C_i.

Таким образом, все классы C_i состоят из одинакового числа элементов, и порядок группы тетраэдра равен $4 \cdot |C_1|$. Чтобы найти $|C_1|$, заметим, что движения, сохраняющие на месте вершину 1, образуют группу, которую можно отождествить с группой правильного треугольника 234, поскольку она состоит из трёх собственных движений — тождественного отображения и двух поворотов на $\pm 120°$ вокруг оси, соединяющей вершину 1 с центром треугольника 234, а также трёх несобственных движений — отражений в плоскостях[1], проходящих через вершину 1 и медианы треугольника 234. Это вытекает из трёхмерной версии упр. 2.4:

Упражнение 2.8. Докажите, что для совпадения двух движений пространства необходимо и достаточно, чтобы они одинаково действовали на вершины какого-нибудь тетраэдра.

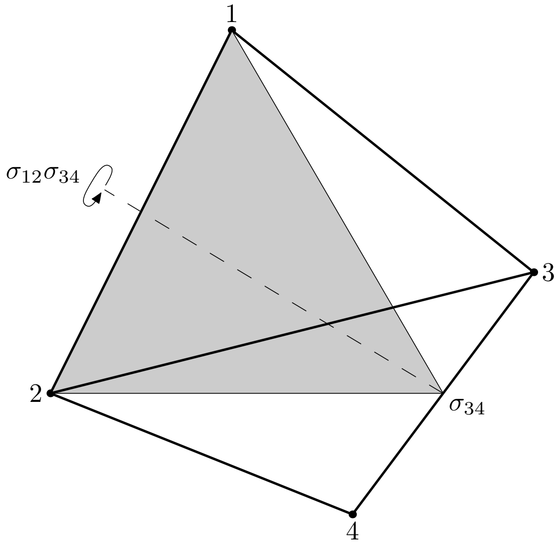


Рис. 2◇5. Плоскость симметрии σ_{34} и ось поворота на $180°$ (равного композиции $\sigma_{12}\sigma_{34}$).

Таким образом, собственная группа тетраэдра состоит из $3 \cdot 4 = 12$ движений, и стало быть, исчерпывается двенадцатью описанными выше поворотами. Полная же группа тетраэдра состоит из $4 \cdot 6 = 24$ движений, а значит, кроме шести описанных выше отражений содержит ещё 6 несобственных движений. Что это за движения?

Для ответа на этот вопрос рассмотрим вложение полной группы тетраэдра в симметрическую группу $\mathfrak{S}_4$, которое сопоставляет каждому движению тетраэдра осуществляемую им перестановку вершин, как в n° 2.1.4 (инъективность этого отображения вытекает из упр. 2.8). Поскольку $|\mathfrak{S}_4| = 24$, это вложение является биекцией. Обозначим через σ_{ij} отражение тетраэдра в плоскости, проходящей через середину ребра $[i, j]$ и противоположное ребро. Шести отражениям σ_{ij} в симметрической группе $\mathfrak{S}_4$ соответствуют транспозиции букв i и j. Поворотам на $\pm 120°$, представляющим собою всевозможные композиции $\sigma_{ij}\sigma_{jk}$ с попарно различными i, j, k, отвечают циклические перестановки трёх букв i, j, k. Трём вращениям на $\pm 180°$ относительно осей, соединяющих середины противоположных рёбер, отвечают одновременные транспозиции непересекающихся пар букв:

$$\begin{aligned} \sigma_{12}\,\sigma_{34} &: \ 1\,2\,3\,4 \longmapsto 2\,1\,4\,3 \\ \sigma_{13}\,\sigma_{24} &: \ 1\,2\,3\,4 \longmapsto 3\,4\,1\,2 \\ \sigma_{14}\,\sigma_{23} &: \ 1\,2\,3\,4 \longmapsto 4\,3\,2\,1\,, \end{aligned}$$

В итоге «недостающие» шесть несобственных преобразований должны отвечать шести возможным циклическим перестановкам вершин:

$$\begin{matrix} 1 \to 2 \to 3 \to 4 \to 1 & 2 \to 3 \to 1 \to 4 \to 2 & 3 \to 1 \to 2 \to 4 \to 3 \\ 2 \to 1 \to 3 \to 4 \to 2 & 1 \to 3 \to 2 \to 4 \to 1 & 3 \to 2 \to 1 \to 4 \to 3 \end{matrix}$$

и их можно реализовать, например, поворотами на $\pm 90°$ относительно прямых, проходящих через середины противоположных рёбер с последующим отражением в плоскости, проходящей через центр тетраэдра и перпендикулярной оси поворота:

$$\begin{aligned} \sigma_{12}\sigma_{23}\sigma_{34} &: \ 1\,2\,3\,4 \longmapsto 4\,1\,2\,3 & \qquad \sigma_{34}\sigma_{23}\sigma_{12} &: \ 1\,2\,3\,4 \longmapsto 2\,3\,4\,1 \\ \sigma_{13}\sigma_{23}\sigma_{24} &: \ 1\,2\,3\,4 \longmapsto 4\,3\,1\,2 & \qquad \sigma_{24}\sigma_{23}\sigma_{13} &: \ 1\,2\,3\,4 \longmapsto 3\,4\,2\,3 \\ \sigma_{14}\sigma_{24}\sigma_{23} &: \ 1\,2\,3\,4 \longmapsto 3\,4\,2\,1 & \qquad \sigma_{23}\sigma_{24}\sigma_{14} &: \ 1\,2\,3\,4 \longmapsto 4\,3\,1\,2\,. \end{aligned}$$

(обратите внимание, что перестановки из правой колонки обратны перестановкам из левой).

2.1.6. Пример: полная и собственная группы додекаэдра. Собственная группа додекаэдра (см. рис. 2◇6) состоит из $6 \cdot 4 = 24$ поворотов на углы $2\pi k/5$ (где $k = 1, 2, 3, 4$) вокруг осей, проходящих через центры противоположных граней додекаэдра, $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины, 15 поворотов на $180°$ вокруг осей, проходящих через середины противоположных рёбер додекаэдра, и тождественного преобразования.

[1] в примере (n° 2.1.4) им соответствовали осевые симметрии треугольника

В полной группе додекаэдра помимо этих 60 движений содержатся их композиции с центральной симметрией относительно центра додекаэдра. Убедиться в том, что никаких других преобразований в группе додекаэдра нет, можно вычислив порядок этой группы тем же методом, что и в предыдущих двух примерах. Для разнообразия мы на этот раз занумеруем не вершины, а грани додекаэдра числами от 1 до 12 и разобьём группу додекаэдра на 12 непересекающихся классов C_i, отнеся в класс C_i все преобразования, переводящие первую грань в i-тую.

Упражнение 2.9. Установите биекцию между классами C_i и C_1.

Класс C_1, переводящий в себя первую грань, можно отождествить с диэдральной группой $\mathfrak{D}_5$. При этом пяти поворотам пятиугольника будут отвечать повороты додекаэдра, вокруг оси, проходящей через центр первой и противоположной к ней грани, а симметриям пятиугольника — несобственные движения, которые можно реализовать отражениями додекаэдра в пяти плоскостях, перпендикулярных первой грани и проходящих через вершину первой грани и середину противоположного ей ребра первой грани. Итого, в собственной группе додекаэдра имеется $12 \cdot 5 = 60$ движений, а в несобственной $12 \cdot 10 = 60$ движений.

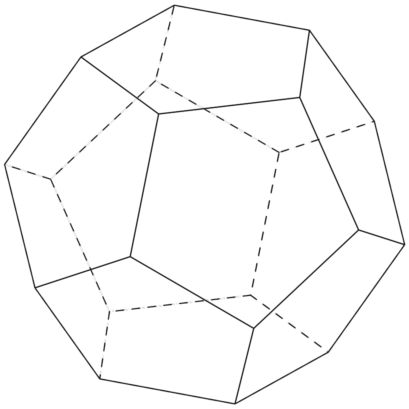


Рис. 2◇6. Додекаэдр.

Упражнение 2.10. Ещё раз подсчитайте число движений в группах тетраэдра и додекаэдра, рассмотрев действие этих групп на рёбра.

Упражнение 2.11. Покажите что полные группы куба (см. рис. 2◇7) и октаэдра (см. рис. 2◇8) состоят из 48 движений, а собственные — из 24.

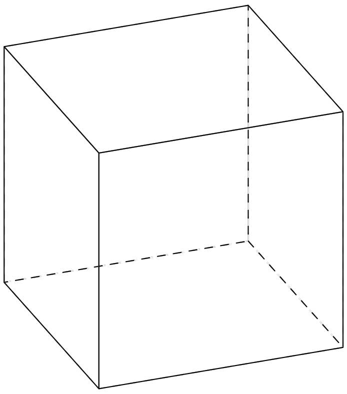


Рис. 2◇7. Куб.

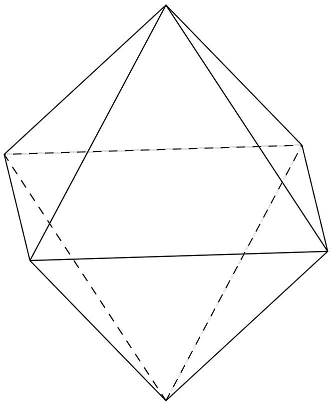


Рис. 2◇8. Октаэдр.

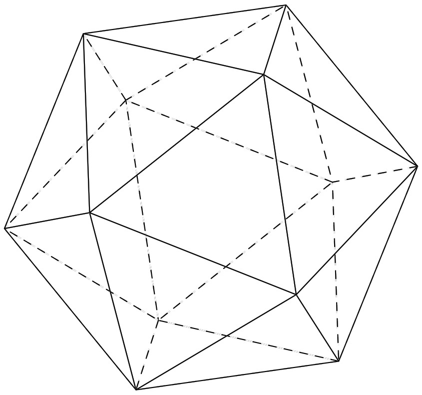


Рис. 2◇9. Икосаэдр.

Упражнение 2.12. Покажите что полная группа икосаэдра (см. рис. 2◇9) состоит из 120 движений, а собственная — из 60.

2.2. Смежные классы. Рассуждение, использованное нами выше для подсчёта количества преобразований в группах фигур путём разбиения этих групп на классы, носит очень общий характер и допускает следующее алгебраическое описание. Пусть в группе G имеется подгруппа[1] $H \subset G$. Для каждого $g \in G$ назовём *левым смежным классом* подгруппы H, отвечающим элементу g, множество преобразований

$$gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}\,, \tag{2-4}$$

получающихся умножением всех преобразований $h \in H$ слева на g. В каждом таком множестве элементов столько же, сколько в подгруппе H, поскольку отображения

$$H \underset{f \mapsto g^{-1} \circ f}{\overset{h \mapsto g \circ h}{\rightleftarrows}} gH$$

[1] т. е. подмножество, также образующее группу; в предыдущих примерах это была подгруппа C_1, состоявшая из преобразований, переводящих в себя вершину или грань, помеченную нами числом 1

задают взаимно обратные биекции между gH и H, как в (2-2, 2-3). С другой стороны, любые два смежных класса g_1H и g_2H либо не пересекаются, либо совпадают. В самом деле, из равенства $g_1h_1 = g_2h_2$ вытекает что $g_1 = g_2h_2h_1^{-1}$, а значит, $g_1H = g_2h_2h_1^{-1}H \subset g_2H$. По тем же причинам $g_2 = g_1h_1h_2^{-1}$ и $g_2H = g_1h_1h_2^{-1}H \subset g_1H$.

Упражнение 2.13. Убедитесь, что отношение принадлежности двух элементов g_1, g_2 к одному смежному классу эквивалентно каждому из условий: а) $g_2^{-1}g_1 \in H$ б) $g_1^{-1}g_2 \in H$ и является *отношением эквивалентности* на группе G в смысле n° 1.4.3 (это даёт другое доказательство того, что любые два смежных классы либо не пересекаются, либо совпадают).

Итак, если в группе G задана произвольная подгруппа H, то группа G распадается в дизъюнктное объединение различных левых смежных классов (2-4), каждый из которых состоит из того же числа элементов, что и подгруппа H. Множество левых смежных классов подгруппы H в группе G обычно обозначается G/H, а число различных смежных классов обозначается $[G : H] = |G/H|$ и называется *индексом* подгруппы H. Мы получаем следующий результат, известный как *теорема Лагранжа о смежных классах*:

2.2.1. ТЕОРЕМА (J. L. LAGRANGE). *Число элементов в любой подгруппе H произвольной конечной группы G делит нацело число элементов в группе G, и частное от этого деления равно количеству различных смежных классов G по H, т. е. $[G : H] = |G| : |H|$.* □

2.2.2. Пример: смежные классы в группе поворотов. Рассмотрим в группе двенадцати поворотов $G = \boldsymbol{\mu}_{12}$ из примера (n° 2.1.2) подгруппу $H \subset G$, образованную четырьмя поворотами на углы, кратные $\pi/2$. Если обозначить поворот на угол $2\pi k/12$ через τ_k (см. рис. 2◇10), то подгруппа H будет состоять из из поворотов τ_0, τ_3, τ_6 и τ_9. Вся группа G распадётся при этом в объединение трёх смежных классов

$$\begin{aligned} H = \tau_0H = \tau_3H = \tau_6H = \tau_9H &= \{\tau_0, \tau_3, \tau_6, \tau_9\} \\ \tau_1H = \tau_4H = \tau_7H = \tau_{10}H &= \{\tau_1, \tau_4, \tau_7, \tau_{10}\} \\ \tau_2H = \tau_5H = \tau_8H = \tau_{11}H &= \{\tau_2, \tau_5, \tau_8, \tau_{11}\}\,, \end{aligned}$$

представители которых обозначены на рис. 2◇10 соответственно точкой, засечкой и двумя засечками. Обратите внимание, что один и тот же смежный класс может быть по разному записан в виде gH — в качестве g в этой записи можно взять любой элемент $g' \in gH$.

В геометрических терминах подгруппа H состоит из всех поворотов, которые переводят в себя один из трёх квадратов с вершинами в делениях изображённого на рис. 2◇10 циферблата (а именно сплошного квадрата), а остальные смежные классы состоят из поворотов, переводящих этот квадрат в два других квадрата.

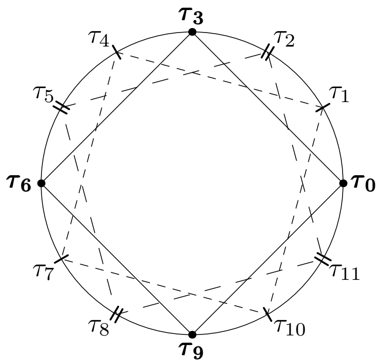


Рис. 2◇10. Смежные классы подгруппы поворотов на углы $\pi k/2$ в группе $\boldsymbol{\mu}_{12}$.

Упражнение 2.14. В собственной группе G каждого из пяти платоновых тел опишите смежные классы подгруппы $H \subset G$, состоящей из всех поворотов вокруг оси, проходящей через центр тела и
а) вершину 1; б) центр грани 1; в) середину ребра 1.

2.2.3. Правые смежные классы. Отметим, что вместо левых смежных классов (2-4) мы могли бы с тем же успехом использовать *правые смежные классы*

$$Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}\,. \tag{2-5}$$

Упражнение 2.15. Повторите для правых смежных классов все предыдущие рассуждения, т. е. покажите, что все они состоят из одинакового числа элементов (равного порядку подгруппы H) и любые два смежных класса или не пересекаются или совпадают; кроме того, сформулируйте и решите «правостороннюю» версию упр. 2.13.

Множество правых смежных классов подгруппы H в группе G обычно обозначается $H\backslash G$. В качестве следствия из теоремы Лагранжа мы получаем, что число левых смежных классов (2-4) равно числу правых смежных классов (2-5):

$$|H\backslash G| = [G : H] = |G|/|H| = |G/H|\,.$$

§3. Орбиты.

3.1. Орбиты. Орбитой $G(x)$ точки $x \in X$ относительно группы преобразований $G \subset \mathrm{Aut}\,(X)$ называется множество всех точек, которые можно получить из точки x, применяя к ней всевозможные преобразования из группы G:

$$G(x) \overset{\text{def}}{=} \{g(x) \mid g \in G\}\ .$$

Орбиты двух различных точек $x_1, x_2 \in X$ или не пересекаются или совпадают. В самом деле, если $g_1(x_1) = g_2(x_2)$ для некоторых $g_1, g_2 \in G$, то $x_1 = g_1^{-1} g_2(x_2)$, и стало быть, $G(x_1) \subset G(x_2)$. Вместе с тем $g_2^{-1} g_1(x_1) = x_2$, и поэтому $G(x_2) \subset G(x_1)$. Мы получаем

3.1.1. ПРЕДЛОЖЕНИЕ. *Всякое множество X представляет собою дизъюнктное объединение орбит любой группы $G \subset \mathrm{Aut}\,(X)$.* □

3.1.2. Длины орбит. Разбиение множества X на орбиты устроено не так регулярно, как разбиение группы на смежные классы, и разные орбиты могут состоять из разного числа точек. Количество точек в орбите (если оно конечно) называется *длиной* этой орбиты.

Чтобы найти длину орбиты $G(x)$ произвольно заданной точки $x \in X$, заметим, что преобразования $g \in G$, которые переводят точку x в себя, образуют в группе G подгруппу. Эта подгруппа называется *стабилизатором* точки x и обозначается

$$\mathrm{Stab}(x) \overset{\text{def}}{=} \{h \in G \mid h(x) = x\}\ .$$

Преобразования, переводящие точку x в точку $y = g(x)$ той же орбиты образуют левый смежный класс стабилизатора:

$$\{f \in G \mid f(x) = g(x)\} = g \cdot \mathrm{Stab}(x)\ .$$

В самом деле, если $h(x) = x$, то $gh(x) = g(x)$, и наоборот, если $f(x) = g(x)$, то f можно записать в виде $g \cdot g^{-1} \cdot f = g(g^{-1} \cdot f)$, где $g^{-1} f \in \mathrm{Stab}(x)$, поскольку $g^{-1} f(x) = g^{-1} g(x) = x$.

Упражнение 3.1. Проверьте, что построенное нами соответствие $g(x) \leftrightarrow g \cdot \mathrm{Stab}(x)$ задаёт биекцию между точками орбиты $G(x)$ и смежными классами подгруппы $\mathrm{Stab}(x)$.

Таким образом, длина орбиты $G(x)$ точки $x \in X$ равна индексу $[G : \mathrm{Stab}(x)]$ её стабилизатора. Из теоремы Лагранжа (n° 2.2.1) вытекает:

3.1.3. СЛЕДСТВИЕ (ФОРМУЛА ДЛЯ ДЛИНЫ ОРБИТЫ). $|G(x)| = |G| : |\mathrm{Stab}(x)|$. □

3.1.4. Пример: ещё раз о порядках групп платоновых тел. Наше вычисление порядков групп пяти платоновых тел, а также порядка общей группы диэдра $\mathfrak{D}_n$ (см. примеры (n° 2.1.4)–(n° 2.1.6), было в сущности ни чем иным, как применением формулы для длины орбиты. В самом деле, все вершины платонова тела образуют одну орбиту группы G этого тела, и стабилизатор $\mathrm{Stab}(в_1)$ вершины 1 — это в точности рассматривавшийся нами класс C_1, откуда $|G| = |\mathrm{Stab}(в_1)| \cdot$ (число вершин). С тем же успехом в качестве точки x, через которую проходит орбита, можно было бы взять не вершину, а центр какой-нибудь грани, скажем, центр $г_1$ первой грани. Тогда мы могли бы вычислить порядок группы как $|G| = |\mathrm{Stab}(г_1)| \cdot$ (число граней). Обратите внимание, что орбиты $G(в_1)$ и $G(г_1)$ имеют разную длину.

Упражнение 3.2. Для каждого из пяти платоновых тел найдите длины орбит всех точек этого тела при действии на них собственной и несобственной группы тела. Есть ли среди орбит такие, длина которых равна порядку группы? Если да, то где располагаются такие точки?

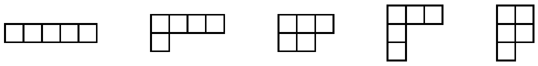
3.1.5. Пример: другой вывод явной формулы для мультиномиального коэффициента. Применим формулу для длины орбиты (n° 3.1.3) для подсчёта количества слов, которые можно получить переставляя буквы в слове

$$w = \underbrace{a_1, a_1, \dots, a_1}_{m_1 \text{ букв } a_1}, \underbrace{a_2, a_2, \dots, a_2}_{m_2 \text{ букв } a_2}, \dots\dots\dots, \underbrace{a_k, a_k, \dots, a_k}_{m_k \text{ букв } a_k}, \tag{3-1}$$

состоящем из $n = m_1 + m_2 + \cdots + m_k$ букв. Симметрическая группа $\mathfrak{S}_n$ действует на всевозможных n-буквенных словах перестановками букв. Искомое число — это в точности длина орбиты $\mathfrak{S}_n(w)$ слова (3-1) относительно этого действия. Стабилизатор $\mathrm{Stab}(w)$ состоит из всевозможных перестановок одинаковых букв друг с другом и имеет порядок $|\mathrm{Stab}(w)| = m_1! \cdot m_2! \cdot \dots \cdot m_k!$. Поэтому

$$|\mathfrak{S}_n(w)| = |\mathfrak{S}_n| / |\mathrm{Stab}(w)| = \frac{(m_1 + m_2 + \dots + m_k)!}{m_1! \cdot m_2! \cdot \dots \cdot m_k!} .$$

3.1.6. Пример: раскладки соломинок по стаканам. Подсчитаем, сколькими способами можно разложить пять разноцветных соломинок по трём одинаковым стаканам, если требуется разложить все пять соломинок, но разрешается, чтобы некоторые из стаканов оставались пустыми. Будем обозначать цвета соломинок цифрами 1, 2, 3, 4, 5. На множестве всех раскладок действует симметрическая группа $\mathfrak{S}_5$, переставляющая соломинки между собою. Это действие не изменяет количества соломинок, находящихся в каждом из стаканов, и его орбиты взаимно однозначно соответствуют различным количественным распределениям соломинок по стаканам. Такое количественное распределение удобно изображать *диаграммой Юнга* — соломинки, находящиеся в одном стакане, рисуются полоской из клеток (число клеток равно числу соломинок), и эти полоски располагаются друг под другом в порядке убывания количества соломинок. В нашем случае получается 5 таких диаграмм[1]:

,

т. е. группа $\mathfrak{S}_5$ имеет 5 орбит, и каждая орбита состоит из всевозможных заполнений клеток соответствующей диаграммы цифрами 1, 2, 3, 4, 5 (каждая цифра используется ровно один раз).

Стабилизатор раскладки, отвечающей тому или иному заполнению фиксированной диаграммы Юнга цифрами, состоит из всевозможных перестановок цифр, стоящих в одной строке (т. е. из произвольных перестановок соломинок внутри одного стакана), а также всевозможных перестановок между собою строк одинаковой длины (т. е. перестановок между собою стаканов, содержащих одинаковое число соломинок). Читателю предлагается убедиться, что

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline\end{array}\right)\right| = 5! = 120 \qquad \left|\mathrm{Stab}\left(\begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = 4! = 24 \cdot 1!$$

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}\right)\right| = 3! \cdot 2! = 12 \qquad \left|\mathrm{Stab}\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4\\\cline{1-1} 5\\\cline{1-1}\end{array}\right)\right| = 3! \cdot 1! \cdot 1! \cdot 2! = 12$$

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = 2! \cdot 2! \cdot 1! \cdot 2! = 8 ,$$

и длины соответствующих орбит, тем самым, равны

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline\end{array}\right)\right| = \frac{120}{120} = 1 \qquad \left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{24} = 5$$

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}\right)\right| = \frac{120}{12} = 10 \qquad \left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4\\\cline{1-1} 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{12} = 10$$

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{8} = 15 .$$

Итого, имеется 41 способ раскладки пяти разных соломинок по трём одинаковым стаканам.

3.2. Цикловой тип перестановки. Пусть $X = \{1, 2, \dots , n\}$ и $g \in \mathfrak{S}_n = \mathrm{Aut}\,(X)$ — какая-то перестановка. Применяя автоморфизм g к произвольному элементу $x \in X$, мы получим последовательность точек

$$x \xmapsto{g} g(x) \xmapsto{g} g^2(x) \xmapsto{g} g^3(x) \xmapsto{g} \cdots .$$

[1] на первой диаграмме все соломинки попали в один стакан; на второй: четыре — в один, и ещё одна — в другой, на третьей: три — в один, две — в другой; на четвёртой: три — в один, и ещё по одной — в два оставшихся стакана; на последней: по две — в два стакана, и одна — в третий

В силу конечности множества X в этой последовательности будут повторяющиеся элементы, и поскольку отображение g биективно, самым первым из повторившихся элементов будет стартовый элемент[1] x :

$$x \longmapsto g(x) \longmapsto g^2(x) \longmapsto \cdots \longmapsto g^{k-1}(x) \longmapsto x = g^k(x) \,. \tag{3-2}$$

Более того, из биективности отображения G вытекает, что любые два таких цикла (начинающиеся из разных точек x и y) либо не пересекаются, либо состоят из одних и тех же элементов.

Таким образом, множество X распадётся в дизъюнктное объединение циклов вида (3-2). Это разбиение можно иначе описать как разбиение множества X на непересекающиеся орбиты группы, состоящей из всевозможных итераций перестановки g и обратной к ней. Эта группа называется *циклической группой*, порождённой перестановкой g и обозначается

$$\langle g\rangle \overset{\text{def}}{=} \{\,\dots\,,\, g^{-2},\, g^{-1}, \mathrm{Id},\, g,\, g^2,\, \dots\,\}\,, \quad \text{где } g^{-k} \overset{\text{def}}{=} \underbrace{g^{-1}g^{-1}\,\cdots\, g^{-1}}_{k \text{ раз}} \text{ при } k\in\mathbb{N}\,. \tag{3-3}$$

Например[2], $g = (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) \in \mathfrak{S}_9$ разбивает множество $\{1,\,2,\,\dots\,,\,9\}$ на три цикла:

$$\begin{gathered} 1 \xmapsto{g} 6 \xmapsto{g} 3 \xmapsto{g} 4 \xmapsto{g} 1 \\ 2 \xmapsto{g} 5 \xmapsto{g} 8 \xmapsto{g} 2 \\ 7 \xmapsto{g} 9 \xmapsto{g} 7\,, \end{gathered} \tag{3-4}$$

представляющие собою орбиты действия группы (3-3), которая в данном случае состоит из 12 преобразований

$$\begin{aligned} g &= (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = g^{-11} \\ g^2 &= (3,\,8,\,1,\,6,\,2,\,4,\,7,\,8,\,9) = g^{-10} \\ g^3 &= (4,\,2,\,6,\,3,\,5,\,1,\,9,\,2,\,7) = g^{-9} \\ g^4 &= (1,\,5,\,3,\,4,\,8,\,6,\,7,\,5,\,9) = g^{-8} \\ g^5 &= (6,\,8,\,4,\,1,\,2,\,3,\,9,\,2,\,7) = g^{-7} \\ g^6 &= (3,\,2,\,1,\,6,\,5,\,4,\,7,\,8,\,9) = g^{-6} \\ g^7 &= (4,\,5,\,6,\,3,\,8,\,1,\,9,\,5,\,7) = g^{-5} \\ g^8 &= (1,\,8,\,3,\,4,\,2,\,6,\,7,\,2,\,9) = g^{-4} \\ g^9 &= (6,\,2,\,4,\,1,\,5,\,3,\,9,\,8,\,7) = g^{-3} \\ g^{10} &= (3,\,5,\,1,\,6,\,8,\,4,\,7,\,5,\,9) = g^{-2} \\ g^{11} &= (4,\,8,\,6,\,3,\,2,\,1,\,9,\,2,\,7) = g^{-1} \\ \mathrm{Id} = g^{12} &= (1,\,2,\,3,\,4,\,5,\,6,\,7,\,8,\,9) \end{aligned} \tag{3-5}$$

(обратите внимание, что циклы (3-4) стоят в правых частях этих формул по столбцам).

Будем называть перестановку, которая переставляет по кругу какие-либо m попарно различных элементов[3]

$$i_1 \longmapsto i_2 \longmapsto i_3 \longmapsto \cdots \longmapsto i_{m-1} \longmapsto i_m \longmapsto i_1\,, \tag{3-6}$$

а все остальные элементы оставляет на месте, *циклом* длины m и обозначать такой цикл через

$$\langle i_1, i_2, \dots, i_m\rangle\,.$$

Упражнение 3.3. Покажите, что два цикла $c_1, c_2 \in \mathfrak{S}_n$ *коммутируют* друг с другом (т. е. удовлетворяют соотношению $c_1c_2 = c_2c_1$) ровно в двух случаях: когда $c_1^m = c_2$ для некоторого $m\in\mathbb{N}$, или когда множества участвующих в них элементов не пересекаются.

---

[1] более формально: если $g^m(x) = g^k(x)$ при $m > k$, то применяя к обеим частям g^{-k} получим $g^{m-k}(x) = x$

[2] мы используем обозначения n° 1.3.1

[3] числа $i_1, i_2, \dots, i_m$ могут быть любыми, не обязательно соседними или возрастающими

Циклы, переставляющие непересекающиеся множества элементов, называются *независимыми*. Из сказанного выше вытекает, что произвольная перестановка g распадается в композицию независимых коммутирующих между собою циклов, причём такое разложение единственно и совпадает с разложением множества X на орбиты циклической группы, порождённой g.

Набор длин циклов, на которые разлагается данная перестановка g называется её *цикловым типом* и обозначается через $\lambda(g)$. Цикловой тип удобно представлять себе в виде *диаграммы Юнга* — выровненного по левому краю набора горизонтальных клетчатых полосок невозрастающей сверху вниз длины, каждая из которых символизирует соответствующий цикл. Например, рассмотренная выше перестановка

$$g = (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = \langle 1,6,3,4\rangle\langle 2,5,8\rangle\langle 7,9\rangle = \begin{array}{|c|c|c|c|}\hline 1&6&3&4\\\hline 2&5&8\\\cline{1-3} 7&9\\\cline{1-2}\end{array}$$

имеет цикловой тип $\lambda(g) = \begin{array}{|c|c|c|c|}\hline \ & \ & \ & \ \\\hline \ & \ & \ \\\cline{1-3} \ & \ \\\cline{1-2}\end{array}$. Вместо того, чтобы полностью рисовать диаграмму Юнга, мы для экономии бумаги иногда будем просто выписывать в строчку длины её строк. Так, запись

$$\lambda(g) = (\lambda_1, \lambda_2, \dots, \lambda_m)\,, \quad \text{где } \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_m \geqslant 0$$

означает, что перестановка g состоит из $\leqslant m$ циклов, длины которых суть $\lambda_1, \lambda_2, \dots, \lambda_m$. Например,

$$\lambda(6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = (4,\,3,\,2)$$

Число клеток, из которого состоит диаграмма Юнга λ, называется её *весом* и обозначается $|\lambda|$. Таким образом, цикловые типы перестановок из $\mathfrak{S}_n$ изображаются диаграммами Юнга веса n. Единственной перестановкой с цикловым типом $\lambda = (1,\,1,\,\dots\,,\,1)$ (он изображается диаграммой-столбцом высоты n и ширины 1) является тождественная перестановка Id. Диаграмме $\lambda = (n)$ (состоящей из одной строки длины n) отвечают всевозможные циклы максимальной длины, переставляющие все элементы множества X по кругу в некотором порядке.

Упражнение 3.4. Сколько имеется в $\mathfrak{S}_n$ различных циклов длины n?

3.2.1. Пример: сколько различных перестановок из $\mathfrak{S}_n$ имеют заданный цикловой тип λ? Пусть диаграмма Юнга λ состоит из m_1 строк длины 1, m_2 строк длины 2, … , m_n строк длины[1] n. Заполним её клетки числами 1, 2, … , n так, чтобы каждое число использовалось ровно один раз, и интерпретируем строки как независимые циклы, слева направо сдвигающие стоящие в них числа.

Симметрическая группа $\mathfrak{S}_n$ действует перестановками цифр на множестве таких заполнений, а значит, и на множестве перестановок заданного циклового типа λ, причём любая перестановка может быть переведена этим действием в любую другую. Иначе говоря, перестановки заданного циклового типа λ образуют одну орбиту симметрической группы $\mathfrak{S}_n$ и их количество равно длине этой орбиты.

Стабилизатор любой перестановки, задаваемой некоторым конкретным заполнением диаграммы λ числами, состоит из всевозможных перестановок циклов одинаковой длины между собою как единого целого, а также циклических перестановок цифр внутри каждого их циклов. Таким образом, порядок стабилизатора зависит только от формы диаграммы и равен

$$|\mathrm{Stab}(\lambda)| = 1^{m_1}\cdot m_1!\cdot 2^{m_2}\cdot m_2!\cdot\,\cdots\,\cdot n^{m_n}\cdot m_n! = \prod_{\alpha=1}^{n} \alpha^{m_\alpha} m_\alpha!\,. \tag{3-7}$$

Стоящее в правой части произведение принято обозначать z_λ. По формуле для длины орбиты (n° 3.1.3) число перестановок, распадающихся в произведение m_1 циклов длины 1, m_2 циклов длины 2, … , m_n циклов длины n (все циклы независимы) равно

$$\frac{n!}{z_\lambda} = \frac{n!}{1^{m_1}\cdot m_1!\cdot 2^{m_2}\cdot m_2!\cdot\,\cdots\,\cdot n^{m_n}\cdot m_n!}\,,$$

[1] отметим, что $m_1\lambda_1 + m_2\lambda_2 + \cdots + m_n\lambda_n = n$ и среди чисел m_i с неизбежностью встречаются нулевые

где $m_1\lambda_1 + m_2\lambda_2 + \cdots + m_n\lambda_n = n$. Отметим, что число $n!/z_\lambda$, тем самым, всегда целое и

$$\sum_{|\lambda|=n} \frac{1}{z_\lambda} = 1$$

(суммирование происходит по всем диаграммам Юнга λ веса n).

3.3. Циклические группы и порядки элементов. Рассмотрим теперь произвольную группу преобразований G и произвольное преобразование $g \in G$. Наименьшая подгруппа группы G, содержащая g, обозначается через $\langle g \rangle$ и называется *циклической подгруппой, порождённой* g. Она состоит из всевозможных целых степеней[1] g^m преобразования g. Если все эти преобразования попарно различны, говорят, что элемент g имеет *бесконечный порядок*. Если среди преобразований вида g^m встречаются одинаковые, скажем, $g^m = g^k$ для некоторых $m > k$, то применяя к обеим частям g^{-k}, мы приходим к равенству $g^{m-k} = \mathrm{Id}$. Наименьшее $n \in \mathbb{N}$, для которого $g^n = \mathrm{Id}$, называется в этом случае *порядком* элемента g.

Элементы бесконечного порядка могут быть только в бесконечных группах G. В конечной группе G всякий элемент $g \in G$ с неизбежностью имеет некоторый конечный порядок n, и порождённая им циклическая группа $\langle g \rangle$ состоит в этом случае в точности n преобразований

$$\mathrm{Id},\, g,\, g^2,\, \dots\,,\, g^{n-1} \tag{3-8}$$

В самом деле, представляя произвольную целую степень m в виде $m = q \cdot n + r$, где остаток r заключён в пределах $0 \leqslant r \leqslant (n-1)$, мы видим, что $g^m = (g^n)^q\, g^r = \mathrm{Id}^q g^r = g^r$. С другой стороны, все преобразования (3-8) попарно различны, поскольку из равенства $g^r = g^s$ с $0 \leqslant r < s < n$ получалось бы равенство $g^{s-r} = \mathrm{Id}$, в котором $0 < (s-r) < n$ вопреки определению порядка n элемента g. Таким образом, порядок любого элемента конечной группы равен порядку порождённой этим элементом циклической подгруппы. Из теоремы Лагранжа вытекает

3.3.1. СЛЕДСТВИЕ. *Порядок любого элемента конечной группы нацело делит порядок группы. В частности* $g^{|G|} = \mathrm{Id} \quad \forall\, g \in G$. □

3.3.2. Пример: порядок перестановки $g \in \mathfrak{S}_n$ циклового типа $\lambda(g) = (\lambda_1, \lambda_2, \dots, \lambda_m)$ равен

$$|\langle g \rangle| = \text{нок}(\lambda_1, \lambda_2, \dots, \lambda_m)\ ,$$

т. е. наименьшему натуральному числу, нацело делящемуся на длины всех независимых циклов, из которых состоит g. Например, порядок перестановки

$$\mathfrak{S}_{12} \ni (3,\, 12,\, 7,\, 9,\, 10,\, 4,\, 11,\, 1,\, 6,\, 2,\, 8,\, 5) = \langle 1,\, 3,\, 7,\, 11,\, 8\rangle\langle 2,\, 12,\, 5,\, 10\rangle\langle 4,\, 9,\, 6\rangle$$

равен $5 \cdot 4 \cdot 3 = 60$.

3.3.3. Циклические группы. Группа G называется *циклической*, если $G = \langle g \rangle$ для некоторого $g \in G$. Примером бесконечной циклической группы является группа T_v параллельных переносов (плоскости или пространства) на всевозможные целые кратные заданного вектора v. Эта группа состоит из тождественного преобразования (сдвига на нулевой вектор $0 = 0 \cdot v$) и бесконечной серии сдвигов на векторы $\pm v$, $\pm 2v$, $\pm 3v$, …

Циклическая группа порядка n — это группа поворотов $\boldsymbol{\mu}_n$ из примеров (n° 2.1.2) и (n° 2.2.2). Ясно, что произвольную циклическую группу порядка n, порождённую элементом g можно отождествить с группой поворотов так, чтобы композиции элементов переходили в композиции — для этого надо отобразить элемент g^k в поворот на угол $2\pi k/n$. Таким образом, все циклические группы порядка n «устроены одинаково». Точный математический смысл этого мы обсудим ниже в §4, а сейчас рассмотрим ещё несколько примеров.

3.3.4. Пример: всякая группа простого порядка является циклической, причём в качестве порождающего её элемента можно взять любое преобразование $g \in G$, отличное от тождественного. В самом деле, в этом

[1] по определению $g^{-m} = \left(g^{-1}\right)^m$ при $m \in \mathbb{N}$, а $g^0 = \mathrm{Id}$

случае $|\langle g\rangle|$ будет больше единицы и по теореме Лагранжа должен нацело делить $|G|$, что возможно только если $|\langle g\rangle| = |G|$, т. е. $\langle g\rangle = G$.

Упражнение 3.5. Является ли циклической группа двуугольника $\mathfrak{D}_2$?

3.3.5. Пример: инволюции. Отличные от тождественного преобразования g порядка 2, т. е. такие что $g \neq \mathrm{Id}$, но $g^2 = \mathrm{Id}$, называются *инволюциями*. Иначе можно сказать, что инволюции — это преобразования, которые обратны сами себе: $g^2 = \mathrm{Id} \iff g = g^{-1}$.

В симметрической группе $\mathfrak{S}_n$ примерами инволюций является циклы длины 2 (или *транспозициии*), меняющие местами какие-нибудь два элемента и оставляющие на месте все остальные. Замечательно, что такие инволюции порождают симметрическую группу.

Упражнение 3.6. Покажите, что произвольная перестановка может быть (многими способами) представлена в виде композиции нескольких (не обязательно независимых) транспозиций.

Для того чтобы перестановка $g \in \mathfrak{S}_n$ была инволюцией необходимо и достаточно, чтобы в её разложении в композицию независимых циклов не было циклов длины $\geqslant 3$. Иначе говоря, инволюции в $\mathfrak{S}_n$ — это в точности композиции *независимых* транспозиций.

Упражнение 3.7. Покажите, что произвольная перестановка может быть представлена в виде композиции двух инволюций.

Подсказка: сначала представьте в виде произведения двух инволюций произвольный цикл[1]

Рассмотрим теперь произвольную конечную группу G и любую пару не равных друг другу инволюций $g_1, g_2 \in G$. Обозначим через $\langle g_1, g_2\rangle$ порождённую ими подгруппу[2] и покажем, что $\langle g_1, g_2\rangle$ можно с сохранением операций отождествить с группой диэдра $\mathfrak{D}_n$, где n — это порядок элемента[3] g_1g_2 в G.

Подгруппа $\langle g_1, g_2\rangle$ состоит из всевозможных чередующихся произведений $g_1g_2g_1g_2 \dots$ и $g_2g_1g_2g_1 \dots$. Домножая равенство

$$\mathrm{Id} = (g_1g_2)^n = \underbrace{g_1g_2g_1g_2 \ \dots \ g_1g_2}_{n \text{ пар}}$$

справа на g_2 и пользуясь тем, что $g_2^2 = \mathrm{Id}$, мы получаем соотношение $g_2 = g_1g_2g_1 \cdots g_1$, которое позволяет переписать любое произведение вида $g_2g_1g_2g_1 \dots$ в виде $g_1g_2g_1g_2 \dots$. Для этого надо подставить вместо самой левой буквы g_2 равное ей слово $g_1g_2g_1 \cdots g_1$ и произвести все возникающие на стыке двух слов сокращения, в результате которых либо полностью сократится исходное слово $g_2g_1g_2g_1 \dots$, что сразу приведёт нас к желаемому результату, либо полностью сократится всё подставленное слово $g_1g_2g_1 \cdots g_1$ и останется слово вида $g_2g_1g_2g_1 \dots$, которое будет строго короче исходного, и к нему по индукции можно будет применить ту же самую процедуру. Итак, любой элемент группы $\langle g_1, g_2\rangle$ записывается в виде произведения $g_1g_2g_1g_2 \dots$, которое при помощи соотношения $(g_1g_2)^n = \mathrm{Id}$ можно редуцировать до произведения, содержащего не более $2n-1$ сомножителей. Все такие редуцированные произведения отличны от Id. Действительно, если бы какое-нибудь редуцированное произведение $g_1g_2g_1 \dots$ равнялось Id, то последний сомножитель в нём был бы равен g_1 (иначе порядок элемента g_1g_2 был бы меньше n, и, умножая обе части равенства $g_1g_2g_1 \cdots g_1 = \mathrm{Id}$ слева и справа на g_1, мы бы получили на 2 множителя меньшее равенство $g_2g_1g_2 \dots g_2 = \mathrm{Id}$, которое можно умножить с двух на g_2 и получить ещё меньшее на 2 множителя равенство и т. д., пока не придём либо к $g_1 = \mathrm{Id}$, либо к $g_2 = \mathrm{Id}$, что не так.

Упражнение 3.8. Покажите аналогичным рассуждением, что все $2n-1$ произведений $g_1g_2g_1g_2 \dots$ попарно различны.

Таким образом, $\langle g_1, g_2\rangle$ состоит из тождественного преобразования и $2n-1$ преобразований $g_1g_2g_1 \dots$. Сопоставим теперь инволюциям g_1 и g_2 симметрии σ_{ℓ_1} и σ_{ℓ_2} относительно двух соседних осей ℓ_1 и ℓ_2 n-угольника (угол между ними при чётном n равен π/n, а при нечётном — $2\pi/n$). Композиции g_1g_2 сопоставим композицию $\sigma_{\ell_1}\sigma_{\ell_2}$, которая согласно упр. 1.12 является поворотом от ℓ_2 к ℓ_1 на угол $2\pi/n$ при чётном n, и на угол $2 \cdot (2\pi/n)$ при нечётном.

Упражнение 3.9. Убедитесь, что отображая $2n-1$ произведений $g_1g_2g_1g_2 \dots$ в соответствующие композиции симметрий n-угольника мы получим сохраняющую композиции биекцию между группой диэдра $\mathfrak{D}_n$ и группой, порождённой инволюциями g_1 и g_2.

[1] это утверждение является аналогом того, что композиция двух осевых симметрий относительно пересекающихся прямых является поворотом вокруг точки пересечения этих прямых на удвоенный угол между прямыми, ср. с упр. 1.12

[2] подгруппой, *порождённой* элементами $g_1, g_2, \dots, g_n \in G$, называется наименьшая по включению подгруппа $H \subset G$, содержащая все эти элементы; такая подгруппа состоит из всевозможных композиций преобразований g_i и обратных к ним преобразований g_i^{-1}

[3] отметим, что $n \geqslant 2$, поскольку $g_1 \neq g_2 = g_2^{-1}$

§4. Абстрактные группы и гомоморфизмы.

4.1. Гомоморфизмы групп. Отображение групп $G \xrightarrow{\varphi} H$ называется *гомоморфизмом*, если оно переводит композицию преобразований в композицию, т. е. для любых двух преобразований $g_1, g_2 \in G_1$ в группе G_2 выполняется соотношение $\varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2)$. Начиная с этого момента термины *эпиморфизм*, *мономорфизм* и *изоморфизм* применительно к отображениям групп будут для нас по умолчанию означать, что отображение, к которому они относятся, является *гомоморфизмом*. В частности, $\mathrm{Aut}\,(G)$ будет обозначать множество всех биективных гомоморфизмов из G в себя, $\mathrm{Hom}(G,H)$ — множество всевозможных гомоморфизмов из G в H и т. д. Если же мы захотим рассматривать не только гомоморфные, но любые отображения, мы будем писать $\mathrm{Aut}_{\,\mathrm{set}}(G)$, $\mathrm{Hom}_{\mathrm{set}}(G,H)$, где индекс set показывает, что в данном контексте группы рассматриваются просто как множества, без учёта композиции.

Наличие между группами изоморфизма означает, что эти группы можно отождествить друг с другом с сохранением таблицы умножения элементов. Простейшими примерами таких изоморфизмов являются построенные в (n° 2.1.4), (n° 2.1.5) отождествления группы треугольника с симметрической группой $\mathfrak{S}_3$ и полной группы тетраэдра с $\mathfrak{S}_4$, а также отождествления бесконечной циклической группы с группой сдвигов, конечной циклической группы — с группой поворотов (n° 3.3.3), а конечной группы, порождённой двумя инволюциями, — с группой диэдра (n° 3.3.5). Рассмотрим ещё несколько примеров гомоморфизмов.

4.1.1. Пример: изоморфизм собственной группы куба с $\mathfrak{S}_4$. Собственная группа куба состоит из 24 поворотов (см. рис. 4◇1): тождественного, $3 \cdot 3 = 9$ поворотов на углы, кратные 90° вокруг осей, проходящих через центры противоположных граней, $4 \cdot 2 = 8$ поворотов на углы, кратные 120° вокруг диагоналей, соединяющих противоположные вершины, и 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер. Чтобы убедиться, что других собственных движений нет, достаточно рассмотреть действие группы куба на восьми его вершинах, составляющих, очевидно, одну орбиту, и воспользоваться формулой для длины орбиты (n° 3.1.3).

Упражнение 4.1. Убедитесь, что стабилизатор вершины в собственной группе куба состоит из трёх поворотов на углы, кратные 120°, вокруг проходящей через эту вершину внутренней диагонали куба.

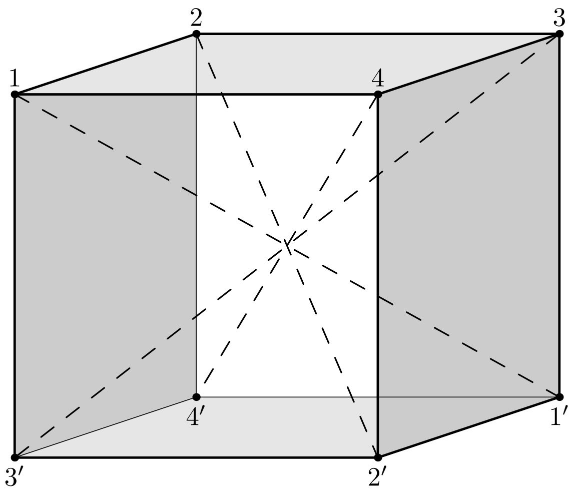
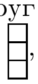


Рис. 4◇1. К действию группы куба на 4 диагонали (1, 2, 3, 4) и 3 пары противоположных граней (прозрачную, светлую, тёмную).

Занумеруем теперь диагонали куба, соединяющие противоположные вершины (помеченные на рис. 4◇1 одинаковыми числами) соответствующими цифрами 1, 2, 3, 4 и сопоставим каждому вращению куба осуществляемую им перестановку диагоналей. Ясно, что мы получим гомоморфизм из собственной группы куба в симметрическую группу $\mathfrak{S}_4$. Он переводит 6 поворотов на $\pm 90°$ в 6 циклов длины 4 циклового типа , 8 поворотов на $\pm 120°$ — в 8 циклов длины 3 циклового типа , 3 поворота на $\pm 180°$ вокруг осей, проходящих через центры противоположных граней, — в 3 пары независимых транспозиций циклового типа , а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер, — в 6 простых транспозиций циклового типа . Тем самым, собственная группа куба, как и полная группа тетраэдра, изоморфна симметрической группе $\mathfrak{S}_4$.

4.1.2. Пример: эпиморфизм $\mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_3$. Если в предыдущем примере вместо четырёх диагоналей куба рассмотреть три пары его противоположных граней (на рис. 4◇1 — прозрачную, светлую и тёмню) или, что то же самое — три отрезка, соединяющие центры противоположных граней, то сопоставляя каждому вращению куба осуществляемую им перестановку этих пар (соотв. отрезков) мы получим гомоморфизм из собственной группы куба в симметрическую группу $\mathfrak{S}_3$, состоящую из 6 элементов. Он эпиморфен, причём прообраз каждой перестановки из $\mathfrak{S}_3$ состоит в точности из четырёх поворотов куба:

тождественное преобразование и 3 поворота на $\pm 180^\circ$ вокруг осей, проходящих через центры противоположных граней, перейдут в тождественное отображение , 8 поворотов на $\pm 120^\circ$ вокруг диагоналей перейдут в 2 цикла различных цикла , а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер и 6 поворотов на $\pm 90^\circ$ перейдут в транспозиции .

Упражнение 4.2. Покажите, что тождественное преобразование куба и 3 поворота на $\pm 180^\circ$ вокруг осей, проходящих через центры противоположных граней, составляют в собственной группе куба подгруппу, изоморфную группе диэдра-двуугольника $\mathfrak{D}_2$, и что полные прообразы всевозможных элементов из $\mathfrak{S}_3$ относительно построенного в предыдущем примере (n° 4.1.2) эпиморфизма — это в точности смежные классы собственной группы куба по этой подгруппе.

4.1.3. Пример: знак перестановки. В этом примере мы построим *гомоморфизм знака*

$$\mathrm{sgn} : \mathfrak{S}_n \xrightarrow{g \mapsto \mathrm{sgn}(g)} \{\pm 1\}\,, \tag{4-1}$$

сопоставляющий каждой перестановке $g \in \mathfrak{S}_n$ её *знак* $\mathrm{sgn}(g) = \pm 1$ так, что

$$\forall\, g_1, g_2 \in \mathfrak{S}_n \quad \mathrm{sgn}(g_1 g_2) = \mathrm{sgn}(g_1)\mathrm{sgn}(g_2)\,. \tag{4-2}$$

Напомним (см. (n° 3.3.5)), что мы называем цикл длины два $\langle i, j\rangle \in \mathfrak{S}_n$ (меняющий местами i-тый и j-тый элементы с сохранением на месте всех остальных) *транспозицией* элементов i и j. Согласно упр. 3.6 всякая перестановка может быть разложена в композицию транспозиций, причём сделать это можно многими разными способами. Нам бы хотелось задать гомоморфизм (4-1) требованиями $\mathrm{sgn}(\mathrm{Id}) = 1$ и $\mathrm{sgn}(\langle i, j\rangle) = -1\ \forall\ i \neq j$, а затем продолжить его на произведения транспозиций по формуле (4-2). Тогда все перестановки, представимые в виде композиции чётного числа транспозиций[1], будут иметь знак $+1$, а перестановки, раскладывающиеся в композицию нечётного числа транспозиций[2], получат знак -1, и свойство (4-2) будет автоматически выполнено. Однако, мы должны проверить, что такое построение не приведёт нас к противоречию: поскольку разложение перестановки в композицию транспозиций не единственно, следует убедиться, что никакая перестановка, являющаяся композицией чётного числа транспозиций, не может одновременно быть композицией нечётного числа транспозиций, и наоборот. Иными словами, нам надо доказать, что чётность числа транспозиций, на которые раскладывается произвольная перестановка $g \in \mathfrak{S}_n$, зависит только от g, но не от способа разложения.

Для этого мы укажем способ отыскания чётности перестановки g, не использующий разложения g в композицию транспозиций. Назовём упорядоченную пару чисел (i, j), такую что $1 \leqslant i < j \leqslant n$, *инверсной парой* перестановки g, если $g(i) > g(j)$. Таким образом, мы разбиваем множество всех упорядоченных пар чисел $\{i < j\} \subset \{1, 2, \dots, n\}$ (состоящее из $n(n-1)/2$ элементов) на два непересекающихся подмножества, образованные, соответственно, инверсными и неинверсными парами, причём это разбиение зависит только от g, «ничего не зная» про то, каким образом g раскладывается в произведение транспозиций.

Покажем теперь, что чётность числа инверсных пар произвольной перестановки совпадает с чётностью количества транспозиций, на которые её можно разложить. Для этого вначале проверим, что при композиции произвольной перестановки g с произвольной транспозицией $\langle i, j\rangle$ чётность числа инверсных пар меняется. Перестановки g и $g \circ \langle i, j\rangle$ отличаются друг от друга перестановкой элементов $g_i = g(i)$ и $g_j = g(j)$, стоящих на i-том и j-том местах в нашей стандартной записи перестановки g словом:

$$\begin{aligned} g &= (g_1, \dots, g_{i-1}, \boldsymbol{g_i}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_j}, g_{j+1}, \dots, g_n) \\ g \circ \langle i, j\rangle &= (g_1, \dots, g_{i-1}, \boldsymbol{g_j}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_i}, g_{j+1}, \dots, g_n)\,. \end{aligned} \tag{4-3}$$

Упражнение 4.3. Проверьте, что у двух перестановок (4-3) инверсность пары (i, j), а также $2(j-i-1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ противоположна[3], а инверсность всех остальных пар одинакова.

Тем самым, количество инверсных пар в этих перестановках разнится на нечётное число, и стало быть, мы показали, что композиция с транспозицией изменяет чётность числа инверсных пар. Если представить теперь перестановку g в виде композиции транспозиций:

$$g = \langle i_1, j_1\rangle \circ \langle i_2, j_2\rangle \circ \cdots \circ \langle i_k, j_k\rangle = \mathrm{Id} \circ \langle i_1, j_1\rangle \circ \langle i_2, j_2\rangle \circ \cdots \circ \langle i_k, j_k\rangle$$

[1] такие перестановки называются *чётными*

[2] такие перестановки называются *нечётными*

[3] т. е. если были инверсными в g, то являются неинверсными в $g \circ \langle i, j\rangle$ и наоборот, если были неинверсными в g, то стали инверсными в $g \circ \langle i, j\rangle$

то чётность числа инверсных пар в ней будет отличаться от нуля (равного чётности числа инверсных пар в тождественной перестановке) в точности на чётность числа k. Следовательно, чётность числа транспозиций, на которые раскладывается g, равна чётности числа инверсных пар перестановки g, и стало быть, не зависит от способа разложения.

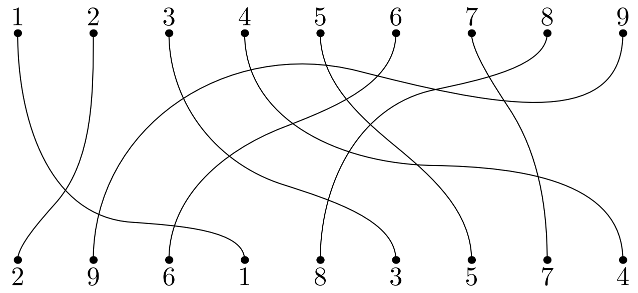


Рис. 4◇2. $\operatorname{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (всего 18 пересечений)

Интерпретация чётности перестановки как чётности числа инверсных пар даёт практический способ отыскания чётности, известный как *правило ниточек*. А именно, напишем друг под другом исходные числа $1, 2, \dots, n$ и их перестановку $g = (g_1, g_2, \dots, g_n)$ и соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала изнутри четырёхугольника $1\, n\, g_n\, g_1$ (см. рис. 4◇2) и чтобы все точки пересечения нитей были простыми двойными[1]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

Упражнение 4.4. Докажите это и найдите при помощи правила ниточек чётность *тасующей перестановки* $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$, в которой наборы номеров $\{i_\nu\}, \{j_\mu\} \subset \{1, 2, \dots, n\}$ не пересекаются, и каждый из них строго возрастают слева направо.

Другим эффективным способом отыскания чётности является разложение перестановки в композицию независимых циклов (см. n° 3.2).

Упражнение 4.5. Докажите, что перестановка чётна тогда и только тогда, когда количество циклов чётной длины в её цикловом типе чётно.

Например для перестановки с рис. 4◇2 получаем $(2, 9, 6, 1, 8, 3, 5, 7, 4) = \langle 1, 2, 9, 4\rangle \circ \langle 3, 6\rangle \circ \langle 5, 8, 7\rangle$, откуда тоже видно, что она чётна.

4.2. Знакопеременные группы $\mathfrak{A}_n \subset \mathfrak{S}_n$.

Чётные перестановки образуют в симметрической группе $\mathfrak{S}_n$ подгруппу порядка $n!/2$. В самом деле, обратная к чётной подстановке подстановка также чётна, поскольку её разложение в произведение транспозиций будет состоять ровно из тех же самых транспозиций, но записанных в обратном порядке:

Упражнение 4.6. Докажите следующую формулу для вычисления обратного элемента к произведению:

$$(g_1 g_2 \cdots g_k)^{-1} = g_k^{-1} \cdots g_2^{-1} g_1^{-1}\,.$$

Композиция чётных перестановок также, очевидно, чётна. Таким образом, чётные перестановки действительно составляют подгруппу. Поскольку для любых двух нечётных перестановок g_1, g_2 перестановка $g_1 g_2^{-1}$ является чётной, все нечётные перестановки лежат в одном смежном классе этой подгруппы. Таким образом, вся группа перестановок представляет собой объединение в точности двух смежных классов, и так как смежные классы состоят из одинакового числа элементов, чётных и нечётных перестановок имеется поровну.

По историческим причинам, которые мы обсудим позже, когда будем изучать теорию Галуа, подгруппа чётных подстановок называется *знакопеременной группой* и обозначается[2] $\mathfrak{A}_n \subset \mathfrak{S}_n$.

Упражнение 4.7. Убедитесь, что при изоморфизме полной группы тетраэдра с $\mathfrak{S}_4$, построенном в примере (n° 2.1.5), собственная подгруппа тетраэдра отождествляется со знакопеременной подгруппой $\mathfrak{A}_4 \subset \mathfrak{S}_4$.

[1]это означает, что в каждой точке пересечения встречается ровно две нити, причём пересечение происходит трансверсально: , а не по касательной:

[2]готическая буква «A», участвующая в этом обозначении, происходит от *alternate*

4.2.1. Пример: эпиморфизм группы додекаэдра на $\mathfrak{A}_5$. Знакопеременная группа $\mathfrak{A}_5$ допускает геометрическую реализацию, похожую на геометрическую реализацию группы $\mathfrak{A}_4$ из упр. 4.7, и основанную на том, что на поверхности додекаэдра (см. рис. 4◇3) имеется ровно 5 кубов с вершинами в вершинах додекаэдра.

Упражнение 4.8. Докажите, что восьмивершинный шестигранник, образованный изображёнными на рис. 4◇3 двенадцатью диагоналями граней додекаэдра, действительно является кубом, и убедитесь, что таких кубов и в самом деле пять.

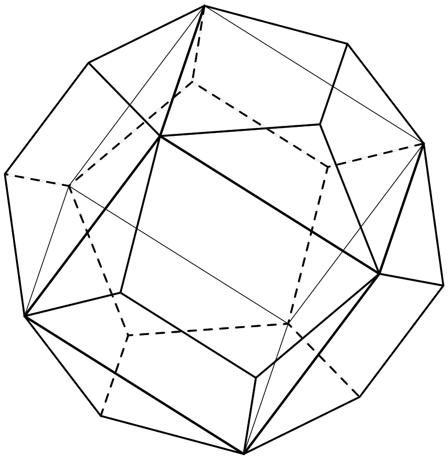


Рис. 4◇3. Один из пяти кубов, лежащих на додекаэдре.

Занумеруем эти кубы цифрами 1, 2, 3, 4, 5 и сопоставим каждому движению из группы додекаэдра осуществляемую им перестановку кубов. Мы получим гомоморфизм из группы додекаэдра в симметрическую группу $\mathfrak{S}_5$. Легко видеть (ср. с (n° 2.1.6)), что образами 60 поворотов при этом будут в точности 60 чётных перестановок: $6 \cdot 4 = 24$ поворота на углы $2\pi k/5$ с $k = 1, 2, 3, 4$ вокруг осей, проходящих через центры противоположных граней додекаэдра, реализуют всевозможные циклы длины 5 (т. е. все 24 перестановки циклового типа), $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины додекаэдра, реализуют всевозможные циклы длины 3 (т. е. все 20 перестановок циклового типа), 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, реализуют всевозможные пары независимых транспозиций (т. е. все 10 перестановок циклового типа); наконец, тождественное преобразование перейдёт в тождественную перестановку. Согласно (n° 2.1.6) собственная группа додекаэдра исчерпывается шестьюдесятью перечисленными поворотами, а значит, построенный нами гомоморфизм устанавливает изоморфизм между собственной группой додекаэдра и знакопеременной группой $\mathfrak{A}_5$.

Отметим, что в отличие от примера (n° 2.1.5) и упр. 4.7 переход от собственной группы додекаэдра к полной не добавляет новых перестановок кубов. В самом деле, по теореме Лагранжа полная группа додекаэдра G представляет собою объединение двух смежных классов: $G = H \sqcup gH$, где $H \subset G$ — подгруппа собственных движений, а $g \in G \smallsetminus H$ — любое несобственное движение. Беря в качестве g центральную симметрию относительно центра додекаэдра, переводящую каждый из кубов в себя, мы заключаем, что образ гомоморфизма $G \longrightarrow \mathfrak{S}_5$ совпадает с образом гомоморфизма $H \longrightarrow \mathfrak{S}_5$ и равен $\mathfrak{A}_5$. При этом прообраз каждой перестановки $g \in \mathfrak{A}_5$ состоит из одного из перечисленных выше поворотов и композиции этого поворота с центральной симметрией додекаэдра.

Упражнение 4.9. Покажите, что симметрическая группа $\mathfrak{S}_5$ не изоморфна полной группе додекаэдра.

4.3. Абстрактные группы. Изоморфные группы преобразований, действующие на разных множествах, имеют одинаковую таблицу умножения, и поэтому любое алгебраическое соотношение на композиции преобразований, справедливое в одной из них, будет справедливо для соответствующих композиций и в другой. Чтобы иметь возможность точно формулировать и изучать такие соотношения не прибегая к явной реализации группы в виде совокупности конкретных симметрий того-или иного объекта, удобно ввести абстрактное понятие группы.

А именно, будем называть (*абстрактной*) *группой* произвольное множество G, на котором задана операция $G \times G \longrightarrow G$, сопоставляющая каждой паре элементов $(g_1, g_2) \in G \times G$ некоторый элемент $g_1 g_2 \in G$, так что при этом выполняются следующие три свойства:

$$(fg)h = f(gh) \quad \forall\, f, g, h \in G \qquad (\textit{ассоциативность}) \tag{4-4}$$

$$\exists\, e \in G \,:\, eg = ge = g \quad \forall\, g \in G \qquad (\textit{существование единицы}) \tag{4-5}$$

$$\forall\, g \in G \quad \exists\, g^{-1} \in G \,:\, gg^{-1} = g^{-1}g = e \quad \forall\, g \in G \qquad (\textit{существование обратного}) \tag{4-6}$$

Элемент e, существование которого постулируется в (4-5), автоматически единственен, поскольку для любых двух таких элементов e' и e'' выполняются равенства $e' = e'e'' = e''$. Как мы видели в n° 1.6.1, свойство (4-6) можно ослабить до требования существования для каждого элемента $g \in G$ левого обратного f: $fg = e$ и правого обратного h: $gh = e$, не требуя при этом, чтобы они совпадали друг с другом — это совпадение доказывается выкладкой

$f = fe = f(gh) = (fg)h = eh = h$, показывающей заодно, что обратный элемент $g^{-1} = f = h$ определяется по g однозначно. Минимизировать условия, определяющие группу можно и дальше.

Упражнение 4.10. Любителям формальных выкладок предлагается убедиться, что в условии (4-5) достаточно требовать существования одной только левой единицы (т. е. такого элемента e, что $eg = g$ $\forall\, g \in G$), а в условии (4-6) — существования одного только левого обратного (решение можно подглядеть в сноске ([1])).

4.4. Реализация абстрактной группы группой преобразований. Всякая группа преобразований, рассматриваемая как множество отображений с операцией композиции, является абстрактной группой. Наоборот, для всякой абстрактной группы G можно строить гомоморфизмы $G \xrightarrow{\varphi} \operatorname{Aut}(X)$ в группы автоморфизмов различных множеств, позволяющие интерпретировать элементы абстрактной группы как преобразования множества X. Всякий такой гомоморфизм φ называется *представлением* абстрактной группы G автоморфизмами множества X или *действием* группы G на множестве X. Представление называется *точным*, если оно инъективно. В этом случае группу G можно отождествить с группой преобразований $\varphi(G) \subset \operatorname{Aut}(X)$.

4.4.1. Левое регулярное представление. Примером точного представления является *левое регулярное представление*, в котором в качестве X выступает сама группа G, рассматриваемая как множество. Это представление сопоставляет каждому элементу $g \in G$ отображение

$$\lambda_g : G \xrightarrow{h \mapsto gh} G\,, \tag{4-7}$$

умножающее все элементы группы G слева на g. Отображение λ_g биективно, поскольку отображение $\lambda_{g^{-1}} : G \xrightarrow{h \mapsto g^{-1}h} G$ является для него двусторонним обратным:

$$\forall\, h \in G \quad \lambda_g\lambda_{g^{-1}}(h) = \lambda_g(g^{-1}h) = gg^{-1}h = h \quad \text{и} \quad \lambda_{g^{-1}}\lambda_g(h) = \lambda_{g^{-1}}(gh) = g^{-1}gh = h\,.$$

Возникающее таким образом отображение[2]

$$\lambda : G \xrightarrow{g \mapsto \lambda_g} \operatorname{Aut}_{\mathrm{set}}(G) \tag{4-8}$$

является гомоморфизмом групп, т. е. удовлетворяет соотношению $\lambda_{g_1g_2} = \lambda_{g_1}\lambda_{g_2}$, т. к.

$$\forall\, h \in G \;\; \lambda_{g_1g_2}(h) = g_1g_2h = \lambda_{g_1}(g_2h) = \lambda_{g_1}(\lambda_{g_2}(h)) = \lambda_{g_1}\lambda_{g_2}(h)\,.$$

Гомоморфизм λ инъективен, ибо при $g_1 \neq g_2$ преобразования λ_{g_1} и λ_{g_2} различны: если $\lambda_{g_1}(h) = \lambda_{g_2}(h)$ хотя бы для одного $h \in G$, то умножая равенство $g_1h = g_2h$ справа на h^{-1}, мы получаем $g_1 = g_2$.

4.4.2. Правое регулярное представление. Наряду с левым регулярным представлением можно рассматривать *правое регулярное представление*

$$\varrho : G \xrightarrow{g \mapsto \varrho_g} \operatorname{Aut}_{\mathrm{set}}(G)\,,$$

которое сопоставляет каждому элементу $g \in G$ отображение ϱ_g правого умножения на g^{-1}:

$$\varrho_g : G \xrightarrow{h \mapsto hg^{-1}} G\,. \tag{4-9}$$

[1] РЕШЕНИЕ: пусть g^{-1} означает (какой-нибудь) левый обратный к g, а e — (какую-нибудь) левую единицу; тогда по их определению $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$; умножая правую и левую часть слева на левый обратный к g^{-1}, получаем $gg^{-1} = e$, т. е. что g^{-1} автоматически является и правым обратным к g элементом; теперь легко увидеть, что e является также и правой единицей: $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$

[2] напомним, что индекс set в обозначении $\operatorname{Aut}_{\mathrm{set}}(G)$ указывает на то, что мы рассматриваем произвольные биекции, не обязательно согласованные с композицией в G; отображение λ_g, как правило, *не является гомоморфизмом*, т. к. $\lambda_g(h_1h_2) = gh_1h_2$ обычно не равно $\lambda_g(h_1)\lambda_g(h_2) = gh_1gh_2$

Появление минус первой степени вызвано тем, что именно именно так заданное отображение ϱ будет являться гомоморфизмом групп, т. е. переводить произведение g_1g_2 в композицию $\varrho_{g_1}\varrho_{g_2}$:

$$\forall\, h\in G \ \ \varrho_{g_1g_2}(h) = h(g_1g_2)^{-1} = hg_2^{-1}g_1^{-1} = \varrho_{g_1}(hg_2^{-1}) = \varrho_{g_1}\left(\varrho_{g_2}(h)\right) = \varrho_{g_1}\varrho_{g_2}(h)\,,$$

тогда как наивное правило, которое мы обозначим $\varrho'_g : h \longmapsto hg$, удовлетворяло бы соотношению

$$\varrho'_{g_1g_2} = \varrho'_{g_2}\varrho'_{g_1}\,, \quad \text{т. к.} \quad \forall\, h\in G \ \ \varrho'_{g_1g_2}(h) = hg_1g_2 = \varrho'_{g_2}(hg_1) = \varrho'_{g_2}\left(\varrho'_{g_1}(h)\right) = \varrho'_{g_2}\varrho'_{g_1}(h)\,,$$

т. е. переводило бы произведение в произведение, записанное в противоположном порядке[1].

Упражнение 4.11. Убедитесь в том, что отображение $G \xrightarrow{\varrho_g} G$ биективно $\forall\, g\in G$ и что $\varrho_{g_1} \neq \varrho_{g_2}$ при $g_1 \neq g_2$.

4.4.3. Отступление об обозначениях. В алгебраической литературе одинаково в ходу две системы обозначений для композиции отображений.

Обозначения, которые мы ввели в (n° 1.5) и которым мы будем следовать практически всюду в этих записках, называются *левым действием*, поскольку в нём отображения применяются к своим аргументам слева и перемножаются справа налево:

$$fg(x) \stackrel{\text{def}}{=} f(g(x))\,, \quad fgh(x) \stackrel{\text{def}}{=} f(g(h(x))) \quad \text{и т. д.}$$

Другой стиль — так называемое *правое действие* — записывает композицию так, что отображения применяются к своим аргументам справа и перемножаются слева направо:

$$[fg]_{\text{прав}} : x \xmapsto{f} f(x) \xmapsto{g} g(f(x))\,, \quad [fgh]_{\text{прав}} : x \xmapsto{f} f(x) \xmapsto{g} g(f(x)) \xmapsto{h} f(g(f(x))) \quad \text{и т. д.}$$

В «правой» системе обозначений левое и правое регулярные представления пришлось бы задавать формулами, противоположными нашим, т. е. обращать g в левом регулярном представлении, и использовать само g, а не g^{-1} в правом. Читатель, который помимо настоящих записок пользуется и другими учебниками, должен следить за тем, какой стиль в них принят, и при необходимости переводить с правого языка на левый и наоборот.

4.4.4. Пример: числовые группы. Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ являются абстрактными группами относительно операции сложения[2]. При помощи левого регулярного представления из n° 4.4 мы можем воспринимать эти группы как группы сдвигов числовой прямой: каждое число $g \in \mathbb{R}$ в левом регулярном представлении превращается в преобразование сдвига $g : \mathbb{R} \xrightarrow{x\mapsto g+x} \mathbb{R}$. Множества ненулевых чисел $\mathbb{Q}^* = \mathbb{Q} \smallsetminus \{0\}$ и $\mathbb{R}^* = \mathbb{R} \smallsetminus \{0\}$ являются также группами относительно операции умножения (ненулевые целые числа такой группы не образуют). Левое регулярное представление умножения чисел интерпретирует каждое ненулевое число g как гомотетию $g : \mathbb{R} \xrightarrow{x\mapsto gx} \mathbb{R}$. Множество знаков $\{\pm 1\}$ из примера (n° 4.1.3) также является группой относительно умножения. Все рассмотренные в этом примере группы коммутативны (или *абелевы*), т. е. помимо свойств (4-4)–(4-6) обладают дополнительным свойством:

$$\forall\, g_1, g_2 \in G \quad g_1g_2 = g_2g_1 \qquad (\textit{коммутативность}) \tag{4-10}$$

Упражнение 4.12. Проверьте, что из диэдральных групп и групп правильных многогранников коммутативна только группа двуугольника $\mathfrak{D}_2$ (ср. с упр. 4.2).

4.5. Подгруппы абстрактных групп. Непустое подмножество $H \subset G$ (абстрактной) группы G называется *подгруппой* в G, если обратные ко всем элементам из H, а также произведения любых двух элементов из H тоже лежат в H. Как и в (n° 2.1) из этих условий вытекает, что единица группы G лежит в H, поскольку $e = hh^{-1}$ для произвольно взятого $h \in H$.

Упражнение 4.13. Докажите, что подмножество H в группе G является подгруппой тогда и только тогда, когда $\forall\, h_1, h_2 \in H \ \ h_1h_2^{-1} \in H$.

[1] Отображение групп $G \xrightarrow{\psi} G'$, удовлетворяющее $\forall\, g_1, g_2 \in G_1$ условию $\psi(g_1g_2) = \psi(g_2)\psi(g_1)$ называется *антигомоморфизмом*

[2] отметим, что натуральные числа такой группы не образуют

Для подгрупп абстрактных групп справедливы все факты, установленные нами в §2 для подгрупп групп преобразований. А именно, с каждой подгруппой $H \subset G$ можно связать два разбиения группы G: в дизъюнктное объединение левых смежных классов[1] $gH = \{gh \mid h \in H\}$ и в дизъюнктное объединение правых смежных классов[2] $Hg = \{hg \mid h \in H\}$, причём каждый из этих классов будет биективен подгруппе H. Для любой конечной группы G выполняется теорема Лагранжа:

$$|G/H| = [G : H] = |G|/|H| = |H\backslash G| \,,$$

где через G/H и $H\backslash G$ обозначены множества левых и правых смежных классов соответственно. С каждым элементом $g \in G$ можно связать циклическую подгруппу, образованную всеми целыми степенями g. Для конечной группы G эта подгруппа также будет конечна: $\langle g\rangle = \{1, g, g^2, \dots, g^{n-1}\} \subset G$, где $n = |\langle g\rangle|$ равно наименьшему натуральному числу, для которого $g^n = e$. Это число называется *порядком* элемента g. По теореме Лагранжа порядок любого элемента нацело делит порядок группы $|G|$. В частности, $\forall\, g\in G \;\; g^{|G|} = e$. Всё это доказывается либо непосредственным повторением рассуждений из предыдущего параграфа, либо точным представлением абстрактной группы G автоморфизмами какого-нибудь множества[3].

Упражнение 4.14. Обязательно ещё раз переговорите для себя все доказательства из §2.

[1] напомним (см. n° 2.2 и упр. 2.13), что любые два левых смежных класса либо не пересекаются, либо совпадают

[2] напомним (см. n° 2.2.3), что любые два правых смежных класса также либо не пересекаются, либо совпадают

[3] любое гомоморфное вложение $G \hookrightarrow \mathrm{Aut}\,(X)$ (скажем, левое регулярное представление (n° 4.4.1)) превращает все перечисленные выше факты в уже доказанные нами в §2 результаты о подгруппах групп преобразований

§5. Строение гомоморфизмов, фактор группы и нормальные подгруппы.

5.1. Строение гомоморфизмов. Любой гомоморфизм групп $G \xrightarrow{\varphi} G'$ переводит единицу e группы G в единицу e' группы G'. В самом деле, $\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e)$ и, умножая обе части на $\varphi(e)^{-1}$, получаем $\varphi(e) = e'$. Далее, поскольку $\varphi\left(g^{-1}\right)\varphi(g) = \varphi\left(g^{-1}g\right) = \varphi(e) = e'$, для любого $g \in G$ выполняется равенство $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$. Поэтому образ гомоморфизма $G \xrightarrow{\varphi} G'$

$$\mathrm{im}\,(\varphi) = \varphi(G) = \{g' \in G' \mid \exists\, g \in G : \varphi(g) = g'\}$$

является подгруппой в $G' : \forall\, \varphi(g), \varphi(f) \in \mathrm{im}\,(\varphi) \quad \varphi(g)\varphi(f)^{-1} = \varphi(g)\varphi(f^{-1}) = \varphi(gf^{-1}) \in \mathrm{im}\,(\varphi)$.

Полный прообраз единицы $e' \in G'$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi \overset{\text{def}}{=} \varphi^{-1}\left(e'\right) = \left\{g \in G \;\middle|\; \varphi(g) = e'\right\} \;.$$

Ядро является подгруппой в $G : \forall\, g, f \in \ker(\varphi) \quad gf^{-1} \in \ker(\varphi)$, поскольку

$$\varphi(g) = \varphi(f) = e' \;\Rightarrow\; \varphi(gf^{-1}) = \varphi(g)\varphi(f^{-1}) = \varphi(g)\varphi(f)^{-1} = e'\left(e'\right)^{-1} = e' \,.$$

Полный прообраз произвольного элемента $g' = \varphi(g) \in \mathrm{im}\,(\varphi)$ представляет собою смежный класс ядра, отвечающий элементу $g \in G$, причём этот смежный класс одновременно является как левым, так и правым смежным классом подгруппы $\ker(\varphi)$, т. е.

$$\varphi^{-1}(\varphi(g)) = g \cdot \ker(\varphi) = \ker(\varphi) \cdot g \;. \tag{5-1}$$

В самом деле, умножая обе части $\varphi(g) = \varphi(f)$ слева на $\varphi(g)^{-1}$, мы получаем равносильное равенство $e' = \varphi(g)^{-1}\varphi(f) = \varphi\left(g^{-1}f\right)$, которое означает, что $g^{-1}f \in \ker(\varphi)$, или $f \in g \cdot \ker(\varphi)$. Аналогично, умножая обе части $\varphi(g) = \varphi(f)$ на $\varphi(g)^{-1}$ справа, мы получаем $e' = \varphi(f)\varphi(g)^{-1} = \varphi\left(fg^{-1}\right)$, что означает, что $fg^{-1} \in \ker(\varphi)$, т. е. $f \in \ker(\varphi) \cdot g$.

Суммируем всё сказанное в виде следующей *теоремы о строении гомоморфизма групп*.

5.1.1. ТЕОРЕМА. *Образ любого гомоморфизма групп $G \xrightarrow{\varphi} G'$ является подгуппой в G', а ядро — подгруппой в G. Левые и правые смежные классы ядра совпадают друг с другом и являются слоями эпиморфизма $G \xrightarrow{\varphi} \mathrm{im}\,(\varphi) : \;\; \forall\, g \in G \quad g \cdot \ker(\varphi) = \ker(\varphi) \cdot g = \varphi^{-1}\big(\varphi(g)\big)$.*

В частности, $|\mathrm{im}\,(\varphi)| = [G : \ker(\varphi)] = |G| : |\ker(\varphi)|$. □

5.1.2. СЛЕДСТВИЕ. *Для того, чтобы гомоморфизм групп был инъективен необходимо и достаточно, чтобы его ядро состояло только из единичного элемента.* □

5.1.3. Пример: ядро эпиморфизма $\mathfrak{S}_4 \xrightarrow{\varphi} \mathfrak{S}_3$ из примера (n° 4.1.2) совпадает с множеством вращений, переводящих в себя каждую из трёх пар противоположных граней куба[1], и потому изоморфно группе двуугольника $\mathfrak{D}_2$, состоящей из тождественного преобразования и трёх поворотов на 180° вокруг осей, проходящих через центры противоположных граней куба. В терминах группы $\mathfrak{S}_4$

$$\ker(\varphi) = \{(1,\,2,\,3,\,4)\,,\; (2,\,1,\,4,\,3)\,,\; (3,\,4,\,1,\,2)\,,\; (4,\,3,\,2,\,1)\} \tag{5-2}$$

состоит из тождественного преобразования и всех перестановок циклового типа $\boxplus$. Сделанное нами в примере (n° 4.1.2) наблюдение, что все слои эпиморфизма φ состоят ровно из четырёх поворотов, объясняется предложением (n° 5.1.1). Читателю настоятельно рекомендуется явно проследить, что эти слои являются как левыми, так и правыми смежными классами подгруппы (5-2).

5.1.4. Пример: ядро эпиморфизма $\mathfrak{S}_n \xrightarrow{\text{sgn}} \{\pm 1\}$ из примера (n° 4.1.3) совпадает со *знакопеременной группой* $\mathfrak{A}_n$. Из предложения (n° 5.1.1) немедленно следуют сделанные в (n° 4.2) наблюдения, что чётные

[1] или, если угодно, каждый из трёх отрезков, соединяющих центры противоположных граней

перестановки образуют в $\mathfrak{S}_5$ подгруппу индекса 2, а нечётные перестановки составляют смежный класс этой подгруппы (одновременно как левый, так и правый).

5.1.5. Пример: ядро гомоморфизма полной группы додекаэдра в $\mathfrak{S}_5$, построенного в примере (n° 4.2.1), изоморфно группе $\{\pm 1\}$ и состоит из тождественного преобразования и центральной симметрии, а образ является знакопеременной подгруппой $\mathfrak{A}_5 \subset \mathfrak{S}_5$. Прообраз каждой чётной перестановки пяти кубов представляет собою смежный класс подгруппы $\{\pm 1\}$ и состоит из одного из описанных в (n° 2.1.6), (n° 4.2.1) поворотов, а также его композиции с центральной симметрией. Отметим, что центральная симметрия коммутирует с любым вращением, поэтому всё равно, в каком порядке эту композицию брать — это ещё раз показывает, что левый смежный класс является в данном случае также и правым, а заодно указывает способ решения упр. 4.9).

5.1.6. Пример: универсальное накрытие единичной окружности числовою прямою. Рассмотрим группу всех преобразований плоскости, задаваемых поворотами вокруг начала координат на произвольные вещественные углы, и будем обозначать через ϑ_α поворот на угол α. Эта группа коммутативна. Её элементы можно отождествить с точками единичной окружности $S^1 = \{(x,y) \mid x^2+y^2=1\}$ (см. рис. 5◇1). А именно, поместим тождественное преобразование $\mathrm{Id} = \vartheta_0$ в точку $(1,0)$ (единичный направляющий вектор оси абсцисс), а поворот ϑ_α — в точку $(\cos\alpha, \sin\alpha)$, для попадания в которую из точки $\vartheta_0 = \mathrm{Id}$ надо пройти по единичной окружности дугу длины α против часовой стрелки, если $\alpha > 0$, и по часовой стрелке, если $\alpha < 0$. При этом композиции поворотов $\vartheta_{\alpha_1}\vartheta_{\alpha_2}$ отвечает сложение соответствующих им ориентированных дуг единичной окружности. Имеется замечательный гомоморфизм из группы вещественных чисел $\mathbb{R}$ с операцией сложения в группу поворотов S^1. Этот гомоморфизм называется *универсальным накрытием* и сопоставлят каждому вещественному числу $\alpha \in \mathbb{R}$ поворот ϑ_α на угол α:

$$u : \mathbb{R} \xrightarrow{\alpha \mapsto \vartheta_\alpha} S^1 , \tag{5-3}$$

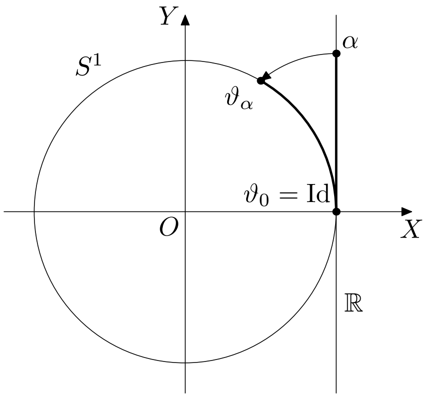


Рис. 5◇1. Накрытие $\mathbb{R} \twoheadrightarrow S^1$.

что можно представлять себе как «наматывание» ориентированной снизу вверх вертикальной числовой прямой $\mathbb{R}$, приставленной своим нулём к точке ϑ_0 (см. рис. 5◇1), на единичную окружность, как нерастяжимая нить наматывается на катушку. Универсальное накрытие сюрьективно, а его ядро состоит из всех углов, поворот на которые является тождественным преобразованием плоскости:

$$\ker(u) = 2\pi \cdot \mathbb{Z} = \{\alpha = 2\pi n \mid n \in \mathbb{Z}\} .$$

Прообраз каждого поворота $\vartheta_\alpha \in S^1$ является смежным классом этой подгруппы и состоит из всех углов, поворот на которые совпадает с поворотом ϑ_α. Все такие углы отличаются от α на произвольное целое число оборотов. Множество этих углов называется *аргументом* поворота $\vartheta_a \in S^1$ и обозначается

$$\mathrm{Arg}\,(\vartheta_\alpha) \stackrel{\text{def}}{=} u^{-1}(\vartheta_\alpha) = \{\alpha + 2\pi n \mid n \in \mathbb{Z}\} .$$

Упражнение 5.1. Пусть $H \subset G$ — произвольная подгруппа абелевой группы G. Убедитесь, что $\forall\, g \in G$ $gH = Hg$.

5.1.7. Пример: эпиморфизм $\mathbb{Z} \twoheadrightarrow \boldsymbol{\mu}_n$ и группа вычетов $\mathbb{Z}/(n)$. Это дискретная версия предыдущего примера. Зафиксируем натуральное $n > 1$ и рассмотрим гомоморфизм из группы целых чисел $\mathbb{Z}$ с операцией сложения в группу поворотов $\boldsymbol{\mu}_n$ из примера (n° 2.1.2)

$$u_n : \mathbb{Z} \xrightarrow{k \mapsto \tau_k} \boldsymbol{\mu}_n , \tag{5-4}$$

который сопоставляет каждому целому числу k поворот $\tau_k = \vartheta_{2\pi k/n}$ на угол $2\pi k/n$. Обозначим ядро этого гомоморфизма через

$$(n) \stackrel{\text{def}}{=} \ker(u_n) = \{zn \mid z \in \mathbb{Z}\} \subset \mathbb{Z} .$$

Оно состоит из всех целых чисел, кратных n. Смежные классы $k + (n)$ называются *классами вычетов по модулю* n и обозначаются $[k]_n$ или $k \,(\mathrm{mod}\ n)$, а принадлежность двух чисел $k, m \in \mathbb{Z}$ одному и тому же классу $[k]_n = [m]_n$ традиционно записывается в виде $k \equiv m \,(\mathrm{mod}\ n)$ (читается: «k сравнимо с m по модулю n»). Композиция в группе $\boldsymbol{\mu}_n$ может восприниматься как сложение классов вычетов, задаваемое правилом $[k]_n + [m]_n \stackrel{\text{def}}{=} [k+m]_n$.

Упражнение 5.2. Убедитесь прямым вычислением, что это правило *корректно* в том смысле, что выбирая в классах вычетов другие элементы k' и m', так что $[k']_n = [k]_n$ и $[m']_n = [m]_n$, мы получим тот же самый результат $[k' + m']_n = [k + m]_n$.

Таким образом, на множестве классов вычетов имеется аддитивная групповая структура. Возникающая таким образом *группа классов вычетов по модулю* n обозначается $\mathbb{Z}/(n)$. По построению, она изоморфна группе поворотов $\boldsymbol{\mu}_n$.

5.2. Нормальные подгруппы. Согласно теореме о строении гомоморфизма (n° 5.1.1) подгруппа $H \subset G$, являющаяся ядром гомоморфизма $G \xrightarrow{\varphi} G'$, обладает замечательным свойством — всякий её левый смежный класс одновременно является и правым смежным классом, т. е. $\forall\, g \in G$ $gH = Hg$, что можно иначе переписать как

$$\forall\, g \in G \;\; gHg^{-1} = H \; . \tag{5-5}$$

Подгруппы $H \subset G$, обладающие этим свойством, называются *нормальными* (или *инвариантными*) подгруппами, что обозначается как $H \lhd G$.

Упражнение 5.3. Покажите, что в абелевой группе любая подгруппа нормальна.

В некоммутативной группе нормальность является существенным ограничением на подгруппу.

5.2.1. Пример: неинвариантность стабилизатора точки с нетривиальной орбитой. Рассмотрим в симметрической группе $G = \mathfrak{S}_4$ подгруппу $H = \mathrm{Stab}(1)$, состоящую из всех перестановок, переводящих элемент 1 в себя. Эта подгруппа не инвариантна.

Упражнение 5.4. Пусть $g = g^{-1} = \langle 1,\, 2 \rangle$ (транспозиция элементов 1 и 2). Убедитесь, что

$$g \cdot \mathrm{Stab}(1) \cdot g^{-1} = \mathrm{Stab}(2) \neq \mathrm{Stab}(1) \; .$$

Отметим, что из теоремы о строении гомоморфизма вытекает, что на множестве смежных классов $\mathfrak{S}_4/H$, которое по (n° 3.1.2) можно отождествить с орбитой $\{1, 2, 3, 4\}$ элемента 1, не существует групповой структуры, в которой отображение

$$\mathrm{ev}_1 : \mathfrak{S}_4 \xrightarrow{g \mapsto g(1)} \{1, 2, 3, 4\}$$

являлось бы гомоморфизмом групп.

Упражнение 5.5. Убедитесь в этом.

5.2.2. ПРЕДЛОЖЕНИЕ. *Подгруппа $H \subset G$ тогда и только тогда является ядром какого-нибудь гомоморфизма $G \xrightarrow{\varphi} G'$, когда она нормальна.*

Доказательство. Необходимость уже была установлена в (n° 5.1.1). Докажем достаточность. Возьмём в качестве G' множество G/H всех различных левых смежных классов gH подгруппы H и зададим на нём структуру группы так, чтобы сюрьекция

$$G \xrightarrow{g \mapsto gH} G/H \; , \tag{5-6}$$

сопоставляющая каждому $g \in G$ смежный класс gH, в котором он лежит, была гомоморфизмом групп. Это требование не оставляет иного выбора, как задать операцию на смежных классах формулой

$$(g_1H) \cdot (g_2H) \stackrel{\text{def}}{=} g_1g_2H \; . \tag{5-7}$$

Неприятность заключается в том, что один и тот же смежный класс может по-разному записываться в виде gH — в качестве g можно взять *любой* из элементов этого класса. Заменяя g_1 и g_2 на f_1 и f_2, такие что $f_1H = g_1H$ и $f_2H = g_2H$, мы не изменим левой части формулы (5-7), но в правой части получим класс f_1f_2H, который, вообще говоря, может отличаться от g_1g_2H, что, собственно, и происходило в предыдущем примере (n° 5.2.1).

Покажем, что если подгруппа H нормальна в G, то из равенств $f_1H = g_1H$ и $f_2H = g_2H$ вытекает равенство $g_1g_2H = f_1f_2H$, и тем самым, формула (5-7) корректно определяет операцию над классами. Равенства $f_1H = g_1H$ и $f_2H = g_2H$ означают, что $g_1^{-1}f_1$ и $g_2^{-1}f_2$ оба лежат в H. Поскольку для всех $g \in G$ и $h \in H$ в силу нормальности H имеется включение $ghg^{-1} \in H$, элемент $g_2^{-1}\left(g_1^{-1}f_1\right)g_2$ (который получается если в предыдущем равенстве положить $g = g_2^{-1}$, $h = g_1^{-1}f_1$) лежит в H. Умножая его справа на $g_2^{-1}f_2 \in H$, мы видим, что $g_2^{-1}\left(g_1^{-1}f_1\right)g_2\left(g_2^{-1}f_2\right) = g_2^{-1}g_1^{-1}f_1f_2 = (g_1g_2)^{-1}(f_1f_2) \in H$. Следовательно, $(g_1g_2)\,H = (f_1f_2)\,H$, что и требовалось.

Итак, мы задали множестве левых смежных классов G/H умножение, для которого отображение (5-6) является гомоморфизмом. Остаётся проверить, что это умножение превращает G/H в группу, т. е. удовлетворяет свойствам (4-4)–(4-6). Ассоциативность умножения (5-7) вытекает из ассоциативности умножения в G:

$$((g_1H)\cdot(g_2H))\cdot(g_3H) = (g_1g_2H)\cdot(g_3H) = (g_1g_2)g_3H = \\ = g_1(g_2g_3)H = (g_1H)\cdot(g_2g_3H) = (g_1H)\cdot((g_2H)\cdot(g_3H))\ .$$

Из правила (5-7) немедленно вытекает, что единичным элементом в G/H является класс единицы $eH = H$, а обратным к произвольному классу gH является класс $g^{-1}H$. Предложение полностью доказано. $\square$

5.3. Факторизация. Построенная в доказательстве предложения (n° 5.2.2) группа G/H, образованная левыми смежными классами gH нормальной подгруппы $H \lhd G$ с умножением (5-7) :

$$(g_1H)\cdot(g_2H) \overset{\text{def}}{=} g_1g_2H \tag{5-8}$$

называется *фактор группой* G по подгруппе $H \lhd G$, а гомоморфизм (5-6) , отображающий каждый элемент группы в содержащий его смежный класс

$$G \xrightarrow{g\mapsto gH} G/H\ ,$$

называется *гомоморфизмом факторизации*. Иными словами, гомоморфизм факторизации «склеивает» каждый смежный класс подгруппы H в одну точку, а формула (5-8) задаёт на этих точках структуру группы. Отметим, что *корректность* формулы (5-8), т. е. независимость результата от выбора представителей g_1, g_2 в смежных классах, *равносильна* тому, что подгруппа H нормальна в G. В самом деле, если формула (5-8) корректна, то G/H, как мы видели, автоматически является группой, а отображение (5-6) — гомоморфизмом групп с ядром H. Поэтому по теореме о строении гомоморфизма (n° 5.1.1) подгруппа H *должна быть* нормальной.

5.4. Разложение гомоморфизма. Теорема о строении гомоморфизма (n° 5.1.1) утверждает, что образ $\mathrm{im}\,(\varphi) \subset G_2$ произвольного гомоморфизма групп $G \xrightarrow{\varphi} G'$ изоморфен фактор группе $G_1/\ker(\varphi)$. В самом деле, непустыми слоями гомоморфизма φ являются в точности смежные классы ядра. В результате любой гомоморфизм φ можно разложить в композицию эпиморфизма факторизации $G \xrightarrow{\varphi''} G/\ker(\varphi)$, отображающего каждый элемент $g \in G$ в его смежный класс $g\cdot\ker(\varphi) = \ker(\varphi)\cdot g$, и мономорфизма $G/\ker(\varphi) \simeq \mathrm{im}\,(\varphi) \xhookrightarrow{\varphi'} G'$, отображающего класс $g\cdot\ker(\varphi) = \ker(\varphi)\cdot g$ в элемент $\varphi(g) \in \mathrm{im}\,(\varphi) \subset G'$. Иными словами, мы имеем *коммутативную диаграмму*[1] гомоморфизмов групп

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\varphi''"'] & & G' \\ & G/\ker(\varphi) \simeq \mathrm{im}\,(f) \arrow[ur, hook, "\varphi'"'] & \end{tikzcd} \tag{5-9}$$

Диаграмма (5-9) называется *каноническим разложением* гомоморфизма $G \xrightarrow{\varphi} G'$.

5.5. Внутренние автоморфизмы. Чтобы прояснить смысл условия $gHg^{-1} = H$, свяжем с каждым элементом $g \in G$ отображение

$$\mathrm{Ad}_g : G \xrightarrow{h\mapsto ghg^{-1}} G\ , \tag{5-10}$$

[1] диаграмма, состоящая из множеств и отображений между ними, называется коммутативной, если композиция отображений вдоль любых двух путей, ведущих из любого узла этой диаграммы в любой другой её узел одинакова; в нашем случае коммутативность диаграммы (5-9) означает, что $\varphi = \varphi'\varphi''$

которое называется *сопряжением*[1] при помощи g (или *внутренним автоморфизмом*, ассоциированным с g).

Упражнение 5.6. В группе G всех движений плоскости обозначим через σ_ℓ и $\tau_O^{(\alpha)}$ осевую симметрию относительно прямой ℓ и поворот на угол α вокруг точки O. Убедитесь, что сопрягая их произвольным собственным движением g мы получим $g\sigma_\ell g^{-1} = \sigma_{g(\ell)}$ и $g\tau_O^{(\alpha)}g^{-1} = \tau_{g(O)}^{(\alpha)}$. Что изменится, если движение g будет несобственным?

Упражнение 5.7. Покажите, что для любой подгруппы $H \subset G$ и любого элемента $g \in G$ множество

$$\mathrm{Ad}_g(H) = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

также является подгруппой в G (она называется *сопряжённой* к H посредством g).

Отображение Ad_g является биективным гомоморфизмом из группы G в себя:

$$\mathrm{Ad}_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \mathrm{Ad}_g(h_1)\mathrm{Ad}_g(h_2)\,,$$
$$\mathrm{Ad}_g^{-1} = \mathrm{Ad}_{g^{-1}}\,,\ \text{т.к.}\ \forall\, h\in G\ \mathrm{Ad}_{g^{-1}}\mathrm{Ad}_g(h) = \mathrm{Ad}_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}g = h\,.$$

Кроме того, оно гомоморфно зависит от g, т.е. $\mathrm{Ad}_{g_1g_2} = \mathrm{Ad}_{g_1}\mathrm{Ad}_{g_2}$, поскольку

$$\forall\, h\in G\ \mathrm{Ad}_{g_1g_2}(h) = g_1g_2h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = \mathrm{Ad}_{g_1}(g_2hg_2^{-1}) = \mathrm{Ad}_{g_1}\left(\mathrm{Ad}_{g_2}(h)\right)\,.$$

Таким образом, сопоставление элементу $g \in G$ автоморфизма сопряжения $G \xrightarrow{\mathrm{Ad}_g} G$ является гомоморфизмом

$$\mathrm{Ad} : G \xrightarrow{g\mapsto \mathrm{Ad}_g} \mathrm{Aut}\,(G)\,. \tag{5-11}$$

Этот гомоморфизм называется *присоединённым представлением* группы G. В отличие от левого и правого регулярных представлений присоединённое представление, вообще говоря, не является точным. Например, если группа G абелева, все внутренние автоморфизмы (5-10) будут тождественными, и ядро присоединённого представления в этом случае совпадает со всей группой. В общем случае $\ker(\mathrm{Ad})$ состоит из всех элементов $g \in G$, которые удовлетворяют условию $ghg^{-1} = h\ \forall\, h \in G$ или, что равносильно, $gh = hg$. Подгруппа элементов, перестановочных со всеми элементами группы G называется *центром* группы G и обозначается

$$Z(G) \stackrel{\text{def}}{=} \{g \in G \mid\ \forall\, h\in G\ \ gh = hg\}\,.$$

Таким образом, $\ker(\mathrm{Ad}) = Z(G)$ — это центр группы G. Образ присоединённого представления $\mathrm{im}\,(\mathrm{Ad}) = \mathrm{Ad}_G \subset \mathrm{Aut}\,(G)$ называется *группой внутренних автоморфизмов* группы G и обозначается $\mathrm{Int}(G)$. Автоморфизмы $\varphi \in \mathrm{Aut}\,(G) \smallsetminus \mathrm{Int}(G)$ называются *внешними*.

Упражнение 5.8. Покажите, что $Z(\mathfrak{S}_n) = \{e\}$, и тем самым, присоединённое представление симметрической группы является точным.

Орбиты присоединённого представления группы G называются *классами сопряжённости*. Иными словами, класс сопряжённости

$$\mathrm{Ad}_G(f) = \{gfg^{-1} \mid g \in G\}$$

данного элемента $f \in G$ представляет собою множество всех элементов, получающихся при сопряжении элемента f всевозможными элементами $g \in G$. Стабилизатором элемента $f \in G$ относительно присоединённого действия является подгруппа

$$C(f) \stackrel{\text{def}}{=} \{g \in G \mid gfg^{-1} = f\} = \{g \in G \mid gf = fg\} = \{g \in G \mid fgf^{-1} = g\}\,,$$

которую можно иначе описать как множество всех элементов, коммутирующих с f, или как множество всех элементов, остающихся на месте при сопряжении элементом f. Эта подгруппа

[1] обозначение Ad является сокращением от *adjunction*

также называется *централизатором* элемента f. Из формулы для длины орбиты вытекает, что число элементов, сопряжённых f, равно отношению

$$|\mathrm{Ad}_G(f)| = |G|/|C(f)| \tag{5-12}$$

5.5.1. Пример: сопряжения в группе перестановок. При сопряжении цикла $\tau = \langle i_1, i_2, \dots, i_k \rangle \in \mathfrak{S}_n$ перестановкой $g = (g_1, g_2, \dots, g_n)$ получится цикл

$$g \cdot \langle i_1, i_2, \dots, i_k \rangle \cdot g^{-1} = \langle g(i_1),\, g(i_2),\, \dots\,,\, g(i_k) \rangle\ , \tag{5-13}$$

переставляющий g-образы тех элементов, которые переставлялись исходным циклом. В самом деле, если элемент $m \in \{1, 2, \dots, n\}$ лежит в множестве $\{g(i_1), g(i_2), \dots, g(i_k)\}$ — скажем, $m = g(i_\nu)$, то левая часть формулы (5-13) действует на него как

$$g(i_\nu) \xmapsto{g^{-1}} i_\nu \xmapsto{\tau} i_{\nu+1} \xmapsto{g} g(i_{\nu+1})\ ,$$

т. е. в точности как правая. Если же $m \notin \{g(i_1), g(i_2), \dots, g(i_k)\}$, и тем самым, $g^{-1}(m) \notin \{i_1, i_2, \dots, i_k\}$, то левая часть (5-13), так же как и правая, оставит элемент m на месте:

$$m \xmapsto{g^{-1}} \underset{\substack{\not\ni\\ \{i_1,i_2,\dots,i_k\}}}{g^{-1}(m)} \xmapsto{\tau} g^{-1}(m) \xmapsto{g} m\ .$$

Поскольку сопряжение является гомоморфизмом, действие Ad_g на произвольную перестановку $\sigma \in \mathfrak{S}_n$, распадающуюся в произведение независимых циклов $\tau_1, \tau_2, \dots, \tau_s$, будет состоять в применении перестановки g к элементам каждого из циклов: $g\tau_1\tau_2\ \cdots\ \tau_s g^{-1} = g\tau_1 g^{-1} \cdot g\tau_2 g^{-1} \cdot\ \cdots\ \cdot g\tau_s \cdot g^{-1}$. Например, результатом сопряжения перестановки

$$\sigma = (6,\, 5,\, 4,\, 1,\, 8,\, 3,\, 9,\, 2,\, 7) = \langle 1,6,3,4 \rangle \langle 2,5,8 \rangle \langle 7,9 \rangle = \begin{array}{|c|c|c|c|}\hline 1&6&3&4\\ \hline 2&5&8\\ \cline{1-3} 7&9\\ \cline{1-2}\end{array}$$

перестановкой $g = (2,\, 1,\, 5,\, 4,\, 3,\, 9,\, 8,\, 7,\, 6)$ будет перестановка

$$\mathrm{Ad}_g(\sigma) = g\sigma g^{-1} = \begin{array}{|c|c|c|c|}\hline 2&9&5&4\\ \hline 1&3&7\\ \cline{1-3} 8&6\\ \cline{1-2}\end{array} =$$
$$= \langle g(1), g(6), g(3), g(4) \rangle \cdot \langle g(2), g(5), g(8) \rangle \cdot \langle g(7), g(9) \rangle = (3,\, 9,\, 7,\, 2,\, 4,\, 8,\, 1,\, 6,\, 5)\ .$$

Иными словами, присоединённое действие группы перестановок на себе совпадает с действием, которое мы рассматривали в примере (n° 3.2.1), когда подсчитывали число перестановок заданного циклового типа: если разложить произвольную перестановку $\sigma \in \mathfrak{S}_n$ в произведение независимых циклов и записать элементы этих циклов по строкам диаграммы Юнга, изображающей цикловой тип перестановки σ, то переход от σ к $g\sigma g^{-1}$ будет заключаться в применении перестановки g ко всем элементам диаграммы.

Таким образом, класс сопряжённости $\mathrm{Ad}_{\mathfrak{S}_n}(\sigma)$ перестановки σ состоит из всех перестановок, имеющих тот же цикловой тип, что и σ, и орбиты присоединённого представления симметрической группы $\mathfrak{S}_n$ взаимно однозначно соответствуют диаграммам Юнга λ веса n. Орбита $\mathrm{Ad}_{\mathfrak{S}_n}(\lambda)$, отвечающая диаграмме λ с m_1 строками длины 1, m_2 строками длины 2, … , m_n строками длины n состоит из

$$|\mathrm{Ad}_{\mathfrak{S}_n}(\lambda)| = \frac{n!}{z_\lambda} = \frac{n!}{1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot\ \cdots\ \cdot n^{m_n} \cdot m_n!}$$

перестановок, а центализатор $C(\lambda)$ каждой перестановки из этой орбиты состоит из

$$|C(\lambda)| = z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot\ \cdots\ \cdot n^{m_n} \cdot m_n! = \prod_{\alpha=1}^{n} \alpha^{m_\alpha} m_\alpha!$$

перестановок.

Упражнение 5.9. Убедитесь, что перестановку $g\sigma g^{-1}$, сопряжённую перестановке $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n) \in \mathfrak{S}_n$, можно также описать как перестановку, переводящую каждый элемент $g(i) \in \{1, 2, \dots, n\}$ в элемент[1] $g(\sigma_i)$.

Упражнение 5.10. Покажите, что стабилизаторы любых двух точек, лежащих в одной орбите группы преобразований $G \subset \mathrm{Aut}\,(X)$, сопряжены посредством произвольного элемента, переводящего одну из этих точек в другую: если $y = g(x)$, то $\mathrm{Stab}(y) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

5.5.2. Пример: сопряжения в группах фигур. Если движение g переводит точки A, B в точки $C = g(A)$ и $D = g(B)$, то преобразование $g\tau g^{-1}$, сопряжённое к повороту τ вокруг оси AB на угол α против часовой стрелки (если смотреть в направлении вектора $\overrightarrow{AB}$), представляет собою поворот вокруг оси CD на угол α против часовой стрелки (если смотреть в направлении вектора $\overrightarrow{CD}$), когда движение g собственное, и на угол $-\alpha$, когда g несобственное. Таким образом, сопряжение элементом g в собственной группе фигуры переводит каждый поворот τ в поворот на такой же угол, но относительно оси, получающейся применением g к оси поворота τ.

5.5.3. Геометрическая характеризация нормальности. Рассмотренные выше примеры показывают, что условие $gHg^{-1} = H$ для подгруппы H какой-либо группы преобразований $G \subset \mathrm{Aut}\,(X)$ означает, что H «симметрична» по отношению ко всем преобразованиям из G в том смысле, что если в H имеется преобразование, как-то специально ведущее себя по отношению к какому-либо набору точек $x_1, x_2, \dots, x_m$, то в H должны быть и преобразования, столь же специально ведущие себя по отношению ко всем наборам точек вида $g(x_1)$, $g(x_2)$, … , $g(x_m)$ с любыми $g \in G$. Рассмотренная в примере (n° 5.3) подгруппа $H = \mathrm{Stab}(1) \subset \mathfrak{S}_4$ не была инвариантной, поскольку задавалась свойством, привязанным к конкретной точке 1. Сопряжение транспозицией $g = \langle 1, 2\rangle$ переводило все перестановки из H в перестановки, обладающие тем же свойством, но уже по отношению к точке 2. Напротив, диэдральная подгруппа $\mathfrak{D}_2 \subset \mathfrak{S}_4$, состоящая из четырёх перестановок $(1, 2, 3, 4)$, $(2, 1, 4, 3)$, $(3, 4, 1, 2)$, $(4, 3, 2, 1)$ и являющаяся ядром эпиморфизма $\mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_3$ из (n° 4.1.2), задаётся условием, симметричным по отношению ко всем перестановкам чисел $1, 2, 3, 4$, а именно, она состоит из тождественного отображения и всех перестановок циклового типа $(2, 2)$.

Увидеть, что подгруппа $H \subset G$ инвариантна, в простых случаях помогает следующая геометрическая переформулировка предложения (n° 5.2.2):

Упражнение 5.11. Покажите, что подгруппа $H \subset G$ нормальна тогда и только тогда, когда существует действие группы G на некотором множестве X, в котором H совпадает с подгруппой всех пребразований, оставляющих каждую точку множества X на месте.

5.6. Простые группы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G. Например, любая группа простого порядка проста, поскольку по теореме Лагранжа вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно предложению (n° 5.2.2) простота группы G равносильна тому, что всякий гомоморфизм $G \longrightarrow G'$ либо является вложением, либо отображает всю группу G в единицу $e' \in G'$.

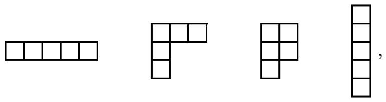
Одним из крупных достижений математики XX века было создание полного списка всех конечных простых групп. В этом курсе мы обсудим многие из идей, использовавшихся при построении этого списка, а также выясним, каким образом произвольные группы можно «собирать» из простых. Однако, это будет чуть позже, а пока что мы закончим наше первое знакомство с группами указанием одной бесконечной серии простых конечных групп, играющей важную роль в теории алгебраических уравнений.

5.6.1. ПРЕДЛОЖЕНИЕ. *Знакопеременная группа $\mathfrak{A}_5$ проста.*

Доказательство. Пусть $H \lhd \mathfrak{A}_5$. Тогда вместе с каждой перестановкой $g \in H$ в подгруппу H войдут и все перестановки сопряжённые g в $\mathfrak{A}_5$. Перестановки, сопряжённые g в полной симметрической группе $\mathfrak{S}_5$ — это все перестановки того же циклового типа, что и g (см. пример (n° 5.5.1)). Так как g чётна, её

[1] поскольку $g(i)$, так же как и i, перебирает без повторов все элементы множества $\{1, 2, \dots, n\}$, описание $g(i) \longmapsto g(\sigma_i)$ «ничем не хуже» описания $i \longmapsto \sigma_i$ — оно отличается от него «переобозначением» элементов в соответствии с перестановкой g

цикловой тип представляет собою диаграмму Юнга веса 5 с чётным количеством строк чётной длины (см. (n° 4.1.3)). Всего имеется 4 таких диаграммы



отвечающие, соответственно, циклам длины 5, циклам длины 3, парам независимых транспозиций и тождественному преобразованию. Если воспользоваться изоморфизмом $\mathfrak{A}_5$ с группой вращений додекаэдра (см. пример (n° 4.2.1)), то можно описать эти классы, соответственно, как повороты на углы $2\pi k/5$ вокруг осей, проходящих через центры противоположных граней, повороты на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины, и повороты на 180° вокруг осей, проходящих через середины противоположных рёбер. Поскольку любая упорядоченная пара противоположных вершин A, B может быть переведена вращением додекаэдра в любую другую такую пару (в том числе и в пару B, A), все повороты на $\pm 2\pi/3$ сопряжены между собою в собственной группе додекаэдра, а стало быть, все циклы длины 3 образуют один класс сопряжённости не только в $\mathfrak{S}_5$, но и в $\mathfrak{A}_5$. По тем же причинам сопряжены между собою в $\mathfrak{A}_5$ и все пары независимых транспозиций. А вот вращения пятого порядка очевидным образом распадаются на два разных класса: 12 сопряжённых вращений на углы $\pm\pi/5$ и 12 сопряжённых вращений на углы $\pm 2\pi/5$.

Упражнение 5.12. Не прибегая к изоморфизму $\mathfrak{A}_5$ с собственной группой додекаэдра, а пользуясь только явными вычислениями в группе перестановок в стиле примера (n° 5.5.1), дайте другое доказательство тому, что в $\mathfrak{A}_5$ все циклы длины 3, а также все пары независимых транспозиций сопряжены между собою, а циклы длины 5 распадается на два класса сопряжённости, содержащие по 12 элементов и состоящие, соответственно, из циклов, сопряжённых $\langle 1, 2, 3, 4, 5\rangle$, и циклов, сопряжённых $\langle 2, 1, 3, 4, 5\rangle$.

Итак, в знакопеременной группе $\mathfrak{A}_5$ имеется ровно 5 классов сопряжённости: класс единицы, содержащий 1 элемент, класс циклов длины 3, содержащий 20 элементов, класс пар независимых транспозиций, содержащий 15 элементов, и два класса циклов длины 5, содержащие по 12 элементов. Поскольку $e \in H$, а каждый из четырёх оставшихся классов либо входит в H целиком, либо не пересекается с H, порядок подгруппы H равен

$$|H| = 1 + 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 \,, \tag{5-14}$$

где каждый из коэффициентов ε_k равен либо 1, либо 0. С другой стороны, по теореме Лагранжа (n° 2.2.1) $|H|$ является делителем $|\mathfrak{A}_5| = 3 \cdot 4 \cdot 5$.

Упражнение 5.13. Убедитесь, что правая часть формулы (5-14) делит $3 \cdot 4 \cdot 5$ ровно в двух случаях: когда все $\varepsilon_k = 1$ и когда все $\varepsilon_k = 0$

Таким образом, нормальные подгруппы в $\mathfrak{A}_5$ исчерпываются единичной подгруппой и всей группой $\mathfrak{A}_5$, что и требовалось установить. $\square$

Упражнение 5.14. Докажите, что все знакопеременные группы $\mathfrak{A}_n$ с $n > 5$ тоже просты.

Указание. Воспользуйтесь индукцией. Вложите $\mathfrak{A}_{n-1}$ в $\mathfrak{A}_n$ как стабилизатор символа n, и докажите, что нетривиальная нормальная подгруппа в $\mathfrak{A}_n$ обязана иметь нетривиальное пересечение с $\mathfrak{A}_{n-1}$ (автоматически нормальное в $\mathfrak{A}_{n-1}$, что противоречит индуктивному предположению о простоте $\mathfrak{A}_{n-1}$).

Упражнение 5.15. Докажите, что внутренние автоморфизмы составляют подгруппу индекса 2 в группе всех автоморфизмов группы $\mathfrak{A}_5$.

Указание. Всякий автоморфизм $\mathfrak{A}_5$ переводит цикл длины 5 в цикл длины 5 и является внутренним тогда и только тогда, когда переводит циклы длины 5 в сопряжённые циклы длины 5.

Упражнение 5.16*. Постройте внешний автоморфизм симметрической группы $\mathfrak{S}_6$.

Указание. Найдите в $\mathfrak{S}_6$ два разных класса сопряжённости, состоящие из одинакового числа элементов, и попытайтесь «переставить» их друг с другом.

§6. Коммутативные кольца и поля. Комплексные числа.

6.1. Коммутативная и некоммутативная алгебра. Своё знакомство с алгеброй мы начали с формул и структур, относившихся к отображениям множеств. С известной долей условности эту часть алгебры можно назвать *некоммутативной алгеброй*, поскольку основная операция, которая в ней используется — композиция отображений — некоммутативна. В этом разделе мы познакомимся с *коммутативной алгеброй* — формулами и структурами, главными действующими лицами в которых являются объекты типа чисел и числовых функций, которые можно складывать и перемножать друг с другом так, что обе эти операции коммутативны. Простейшие алгебраические структуры, аксиоматизирующие свойства чисел и числовых функций — это коммутативные кольца и поля. Примерами полей являются числовые поля $\mathbb{Q}$ и $\mathbb{R}$, а примерами коммутативных колец — целые числа $\mathbb{Z}$, а также многочлены $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ и $\mathbb{R}[x]$ с целыми, рациональными и вещественными коэффициентами.

Оговоримся, что деление алгебры на «коммутативную» и «некоммутативную» довольно искусственно. Мы уже видели в примере (n° 4.4.4), что числовые группы можно воспринимать как группы преобразований числовой прямой. Важнейшим источником информации о коммутативных кольцах и полях являются сохраняющие операции отображения между ними (*гомоморфизмы*), которые сами по себе живут в некоммутативном мире. С другой стороны, представление какой-нибудь группы преобразований как группы автоморфизмов некоторой коммутативной алгебраической структуры часто позволяет увидеть такие свойства этой группы, которые были совершенно не очевидны при другом её представлении. Так что коммутативный и некоммутативный миры тесно переплетаются друг с другом.

Следующее далее определение формализуют стандартные свойства сложения и умножения чисел.

6.2. Определение поля. Множество $\mathbb{F}$ называется *полем*, если на нём заданы две операции

$$\mathbb{F}\times\mathbb{F}\longrightarrow\mathbb{F}\ :$$

сложение $(a,b)\longmapsto a+b$ и умножение $(a,b)\longmapsto ab$ со свойствами:

1) аксиомы сложения
   а) коммутативность (переместительный закон): $a+b=b+a \quad \forall\, a,b\in\mathbb{F}$
   б) ассоциативность (сочетательный закон): $a+(b+c)=(a+b)+c \quad \forall\, a,b,c\in\mathbb{F}$
   в) существование нейтрального элемента (нуля): $\exists\, 0\in\mathbb{F}: \quad a+0=a \quad \forall\, a\in\mathbb{F}$
   г) существование противоположного: $\forall\, a\in\mathbb{F} \quad \exists\,(-a)\in\mathbb{F}: \quad a+(-a)=0$
2) аксиомы умножения
   а) коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$
   б) ассоциативность: $a(bc)=(ab)c \quad \forall\, a,b,c\in\mathbb{F}$
   в) существование нейтрального элемента (единицы): $\exists\, 1\in\mathbb{F}: \quad a\cdot 1=a \quad \forall\, a\in\mathbb{F}$
   г) существование обратного: $\forall\, a\in\mathbb{F},\ a\neq 0 \quad \exists\, a^{-1}\in\mathbb{F}: \quad a\cdot a^{-1}=1$
3) аксиома дистрибутивности (распределительный закон): $a(b+c)=ab+ac \quad \forall\, a,b\in\mathbb{F}$
4) аксиома нетривиальности: $0\neq 1$

Первые два набора аксиом утверждают, что всё поле $\mathbb{F}$ является абелевой группой относительно сложения[1], а множество $\mathbb{F}^*\overset{\text{def}}{=}\mathbb{F}\smallsetminus\{0\}$ всех ненулевых элементов поля $\mathbb{F}$ представляет собою

[1] групповая структура, операцией в которой является сложение, называется *аддитивной* групповой структурой; единицей аддитивной группы служит элемент 0 (в аддитвной структуре он называется *нейтральным элементом*), аддитвно обратные элементы называются *противоположными*; новые названия необходимы для того, чтобы отличать аддитивную групповую структуру от *мультипликативной* групповой структуры, операцией в которой служит умножение; стандартные названия из теории групп («единица», «обратный элемент») используются для мультипликативной групповой структуры

абелеву группу относительно умножения. Последние две аксиомы регулируют взаимодействие этих двух структур между собой. Как мы уже видели в (n° 4.3), из аксиом группы вытекает, что единица и нуль единственны, а противоположный и обратный элементы $-a$ и a^{-1} к данному элементу $a \in \mathbb{F}$ однозначно определяются по a.

Из аксиом поля автоматически следуют и некоторые другие интуитивно ожидаемые свойства действий.

Упражнение 6.1. Покажите, что в любом поле $\mathbb{F}$ для любого $a \in \mathbb{F}$ выполняются равенства $0 \cdot a = 0$ и $(-1) \cdot a = (-a)$ (последнее означает, что умножая a на число, противоположное единице, мы получим число противоположное a, чего *a priori* не требовалось; решение можно подглядеть в сноске ([1])).

Отметим, что требование $a \neq 0$ в аксиоме (2г) необходимо, поскольку иначе мы имели бы $1 = 0 \cdot 0^{-1} = 0$, что противоречит последней аксиоме[2].

Простейшим полем является поле $\mathbb{F}_2$, состоящее из двух элементов 0 и 1, таких что $0 + 1 = 1 \cdot 1 = 1$, а все остальные суммы и произведения равны нулю (включая $1 + 1 = 0$). Элементы этого поля можно интерпретировать как «ложь» и «истину», после чего сложение и умножение превращаются, соответственно, в логические операции «исключающее или» и «и». Таким образом, формулы и вычисления в поле $\mathbb{F}_2$ — это то, что называется «алгеброй высказываний».

Упражнение 6.2. Проверьте, что $\mathbb{F}_2$ действительно является полем и напишите многочлен от x, равный «не x», а также многочлен от x и y, равный «x или[3] y».

Примером поля, послужившим первоисточником для введения этого понятия, является поле рациональных чисел $\mathbb{Q}$, которое можно определить как множество классов эквивалентности выражений вида p/q с $p, q \in \mathbb{Z}$ и $q \neq 0$, где два выражения p/q и r/s считаются эквивалентными тогда и только тогда, когда $ps = qr$ в $\mathbb{Z}$. Сложение и умножение классов определяется формулами

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}\,, \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \tag{6-1}$$

Упражнение 6.3. Проверьте, что эти определения корректны (не зависят от выбора представителей в классе эквивалентных дробей) и удовлетворяют аксиомам поля.

Более сложным примером поля является поле действительных чисел $\mathbb{R}$. У множества $\mathbb{R}$ имеется несколько различных определений[4]. Мы будем предполагать, что читатель знаком с этими определениями и понимает, почему они эквивалентны друг другу. Отметим, что какое бы из определений множества $\mathbb{R}$ не использовалось, задание на $\mathbb{R}$ операций сложения и умножения требует достаточно серьёзной работы, и проверка выполнения аксиом поля для этих двух операций составляет стандартный набор теорем из начального курса анализа. Мы полагаем, что читатель знает эти теоремы.

6.3. Поле комплексных чисел (геометрическое определение). Рассмотрим вещественную координатную плоскость $\mathbb{R}^2$ с фиксированной прямоугольной системой координат OXY с началом в точке $O = (0, 0)$ и координатными осями OX и OY, направленными вдоль векторов $(1, 0)$ и $(0, 1)$, которые мы будем обозначать символами 1 И i (см. рис. 6◇1). Точки z этой плоскости мы будем называть *комплексными числами*, а саму плоскость обозначим через $\mathbb{C}$.

Координаты (x, y) комплексного числа z обозначаются через $\operatorname{Re}(z) = x$, $\operatorname{Im}(z) = y$ и называются *действительной* и *мнимой* частями комплексного числа. Каждому комплексному числу z можно сопоставить его *радиус-вектор* $x \cdot 1 + y \cdot i$ — это вектор с началом в точке O и концом

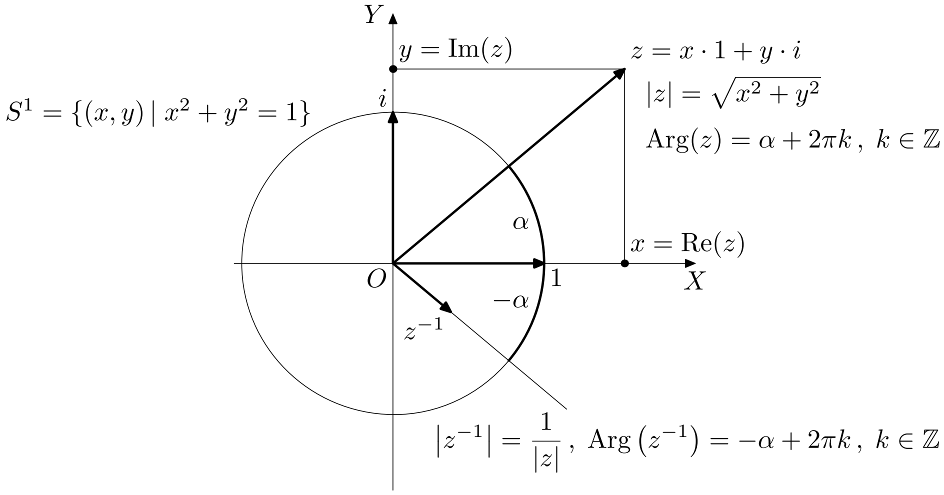
[1] РЕШЕНИЕ: обозначая $a \cdot 0$ через b, будем иметь $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0 + 1) = a \cdot 1 = a$; прибавляя к обеим частям этого равенства $(-a)$, получаем $b = 0$; наконец, $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$, откуда $(-1) \cdot a = -a$

[2] на самом деле аксиома (4) равносильна требованию $\mathbb{F} \neq \{0\}$: при $0 = 1$ мы имели бы $\forall\, a \in \mathbb{F}\ \ a = a \cdot 1 = a \cdot 0 = 0$

[3] здесь имеется в виде «не исключающее или», т. е. многочлен должен принимать значение 1 тогда и только тогда, когда *хотя бы одна* из переменных равна 1

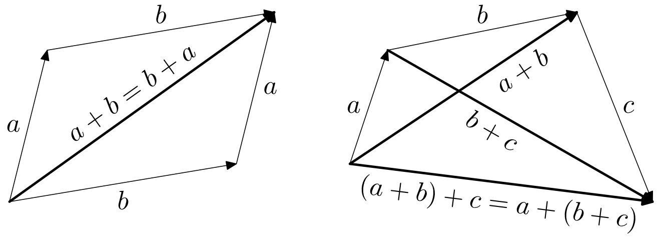
[4] три наиболее употребительных: множество классов эквивалентности десятичных (или привязанных к любой другой позиционной системе счисления, например, двоичных) дробей, множество дедекиндовых сечений множества $\mathbb{Q}$, а также множество классов эквивалентности рациональных последовательностей Коши

в точке z, который мы будем обозначать тем же символом z, что и саму точку. Точке $O = (0, 0)$ при этом сопоставляется нулевой вектор 0.



6◇1. Атрибуты комплексного числа $z = x \cdot 1 + y \cdot i$.

Каждый радиус-вектор $z = x \cdot 1 + y \cdot i$ имеет длину $|z| = \sqrt{x^2 + y^2}$, также называемую *модулем* числа z, и *аргумент* $\mathrm{Arg}\,(z) \overset{\text{def}}{=} \{\alpha + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}$, представляющий собою множество всех углов[1], поворот на которые совмещает направление оси OX с направлением радиус-вектора z (все такие углы отличаются на целое число полных оборотов и образуют смежный класс подгруппы $2\pi\mathbb{Z} \subset \mathbb{R}$ из примера (n° 5.1.6)).



6◇2. Коммутативность и ассоциативность сложения векторов.

Сложение комплексных чисел определяется как сложение отвечающих им радиус-векторов: суммой двух точек z_1 и z_2 называется точка, радиус вектор которой равен сумме $z_1 + z_2$ радиус-векторов точек z_1 и z_2. В координатах это описывается формулой

$$(x_1 \cdot 1 + y_1 \cdot i) + (x_2 \cdot 1 + y_2 \cdot i) = (x_1 + x_2) \cdot 1 + (y_1 + y_2) \cdot i\,.$$

Сложение векторов, как известно, коммутативно и ассоциативно (см. рис. 6◇2), обладает нейтральным элементом $z = 0$, и у всякого вектора есть противоположный. Таким образом, комплексные числа образуют абелеву группу относительно сложения.

[1] напомним, что углы в математике измеряются действительными числами (ср. с примером (n° 5.1.6)), а именно *ориентированный угол* луча OZ с осью OX по определению равен длине пути, который надо пройти по единичной окружности с центром в O от точки её пересечения с лучём OX до точки её пересечения с лучём OZ, причём длина берется со знаком «+», если движение происходит против часовой стрелки, и со знаком «−», если по часовой стрелке; существенно, что такая дуга *не единственна* — она определена с точностью до *любого целого числа оборотов*; поэтому угол не есть конкретное число, но целое счётное множество действительных чисел, составляющих арифметическую прогрессию с разностью 2π; множество всех этих чисел принято обозначать $\mathrm{Arg}\,(\measuredangle XOZ) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где α — какое-то одно из значений угла, и называть *аргументом* луча OZ (в старину сказали бы, что аргумент является *многозначной функцией* от луча OZ, а сейчас мы говорим, что это смежный класс ядра универсального накрытия единичной окружности числовою прямою, описанного в примере (n° 5.1.6))

Произведением комплексных чисел z_1 и z_2 называется число z_1z_2, радиус-вектор которого задаётся условиями

$$|z_1z_2| \stackrel{\text{def}}{=} |z_1| \cdot |z_2| \,, \quad \mathrm{Arg}\,(z_1z_2) \stackrel{\text{def}}{=} \mathrm{Arg}\,(z_1) + \mathrm{Arg}\,(z_2) \tag{6-2}$$

(иными словами, при умножении комплексных чисел их модули перемножаются, а аргументы складываются). Это умножение очевидно коммутативно и ассоциативно. Единичным элементом для него является число $1 \in \mathbb{C}$ (единичный направляющий вектор оси OX), а умножение на нулевой вектор обладает свойством $0 \cdot z = 0 \quad \forall\, z \in \mathbb{C}$. Обратным к ненулевому элементу z является число z^{-1} с

$$|z^{-1}| = 1/|z| \,, \quad \mathrm{Arg}\,(z^{-1}) = -\mathrm{Arg}\,(z) \tag{6-3}$$

(см. рис. 6◇1). Таким образом, относительно умножения ненулевые комплексные числа также образуют коммутативную группу.

Левое регулярное представление мультипликативной группы комплексных чисел (см. n° 4.4.1) имеет простую геометрическую интерпретацию: умножение на фиксированное число $a \in \mathbb{C}$

$$\lambda_a : \mathbb{C} \xrightarrow{z \mapsto az} \mathbb{C}$$

представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{C}$ относительно начала координат на угол $\mathrm{Arg}\,(a)$ с коэффициентом $|a|$. Таким образом устанавливается биекция между отличными от нуля точками $a \in \mathbb{C}$ и поворотными гомотетиями относительно начала координат с ненулевым коэффициентом. Эта биекция является изоморфизмом мультипликативных групп — композиция поворотных гомотетий λ_a и λ_b это в точности поворотная гомотетия λ_{ab} (где под ab понимается произведение комплексных чисел, вычисленное по формуле (6-2)) с коэффициентом $|a||b|$ на угол $\mathrm{Arg}\,(a) + \mathrm{Arg}\,(b)$.

6.3.1. ПРЕДЛОЖЕНИЕ. *Комплексные числа образуют поле.*

Доказательство. Из всех свойств поля нам осталось проверить только дистрибутивность (3). На геометрическом языке формула $a(b+c) = ab + ac$ переписывается как $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$ и означает, что поворотные гомотетии перестановочны со сложением векторов, или — что то же самое — что любая поворотная гомотетия λ_a переводит параллелограмм в параллелограмм. Но это действительно так, поскольку всякий поворот и всякая гомотетия переводят параллелограмм в параллелограмм. □

6.3.2. Алгебраическое представление комплексных чисел. Прежде всего заметим, что ось OX в поле $\mathbb{C}$ можно отождествить с полем вещественных чисел $\mathbb{R}$ — сложение и умножение комплексных чисел, лежащих на оси OX, в точности совпадает со сложением и умножением чисел вещественной числовой прямой. Поэтому разложение $z = x \cdot 1 + y \cdot i$ радиус-вектора z по базисным векторам $1 = (1,0)$ и $i = (0,1)$ с вещественными коэффициентами $x = \mathrm{Re}\,(z)$ и $y = \mathrm{Im}\,(z)$ является *верным равенством в поле* $\mathbb{C}$ — сложение и умножение в этой формуле могут восприниматься как сложение и умножение комплексных чисел. Следуя обычной традиции опускать знаки произведений и умножение на единицу, формулу $z = x \cdot 1 + y \cdot i$ обычно сокращают до $z = x + iy$.

Пользуясь аксиомой дистрибутивности и равенством $i^2 = -1$, мы можем вычислить произведение комплексных чисел $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, изначально определённое нами геометрически формулой (6-2), по обычным правилам раскрытия скобок:

$$z_1z_2 = (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \,. \tag{6-4}$$

Обратное к числу $z = x + iy$ число z^{-1} так же легко выражается через x и y:

$$z^{-1} = \frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2+y^2} = \frac{x}{|z|^2} - \frac{iy}{|z|^2} \,, \tag{6-5}$$

[1] напомним, что *поворотной гомотетией* относительно точки O на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки O и растяжения в ϱ раз относительно O (поскольку растяжения коммутируют с поворотами, всё равно, в каком порядке эта композиция выполняется)

откуда $\mathrm{Re}\,\left(z^{-1}\right)=\mathrm{Re}\,(z)/|z|^2$ и $\mathrm{Im}\,\left(z^{-1}\right)=-\mathrm{Im}\,(z)/|z|^2$. Число $\overline{z}\overset{\text{def}}{=}x-iy$ называется *комплексно сопряжённым* к числу $z=x+iy$. В терминах комплексного сопряжения формулу для обратного числа можно записать в виде $z^{-1}=\overline{z}/|z|^2$. Геометрически, комплексное сопряжение

$$\mathbb{C}\xrightarrow{z\mapsto\overline{z}}\mathbb{C}$$

представляет собою симметрию комплексной плоскости относительно вещественной оси OX. С алгебраической точки зрения сопряжение является инволютивным автоморфизмом поля $\mathbb{C}$, т. е. $\forall\, z\in\mathbb{C}\ \ \overline{\overline{z}}=z$ и $\forall\, z_1,z_2\in\mathbb{C}\ \overline{z_1+z_2}=\overline{z}_1+\overline{z}_2$, $\overline{z_1z_2}=\overline{z}_1\overline{z}_2$.

6.3.3. Пример: тригонометрия. Рассмотрим комплексные числа

$$z_1=\cos\varphi_1+i\sin\varphi_1\ ,\quad z_2=\cos\varphi_2+i\sin\varphi_2\ ,$$

лежащие на единичной окружности $S^1=\{z\,:\,|z|=1\}$. Тогда произведение z_1z_2, вычисленное по формуле (6-2) и вычисленное по формуле (6-4), имеют вид

$$\cos(\varphi_1+\varphi_2)+i\sin(\varphi_1+\varphi_2)=z_1z_2=\Big(\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2\Big)+i\Big(\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2\Big)\ ,$$

откуда $\cos(\varphi_1+\varphi_2)=\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2$ и $\sin(\varphi_1+\varphi_2)=\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2$. Тем самым, нами *доказаны* тригонометрические формулы сложения аргументов. На самом деле не только эти формулы, но и всё казуистическое изобилие формул школьной тригонометрии есть не что иное, как бесформенный шлейф случайных следствий того простого факта, что комплексные числа образуют поле и вычислять с ними можно по обычным правилам «раскрытия скобок».

Вот ещё один пример. Пусть $z=\cos\varphi+i\sin\varphi$. Тогда $z^n=\cos(n\varphi)+i\sin(n\varphi)$ можно вычислить, раскрывая скобки в $(\cos\varphi+i\sin\varphi)^n$ по формуле (1-9) из §1. Мы получаем равенство

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

которое заключает в себе тригонометрические формулы для кратных углов:

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

Упражнение 6.4. Докажите, что при нечётном n функция $\sin(n\varphi)/\sin\varphi$ является многочленом от $\sin^2\!\varphi$. Найдите его степень, корни и старший коэффициент. Выпишите этот многочлен явно для $n=3$ и $n=5$. Наконец, докажите для нечётных n тождество

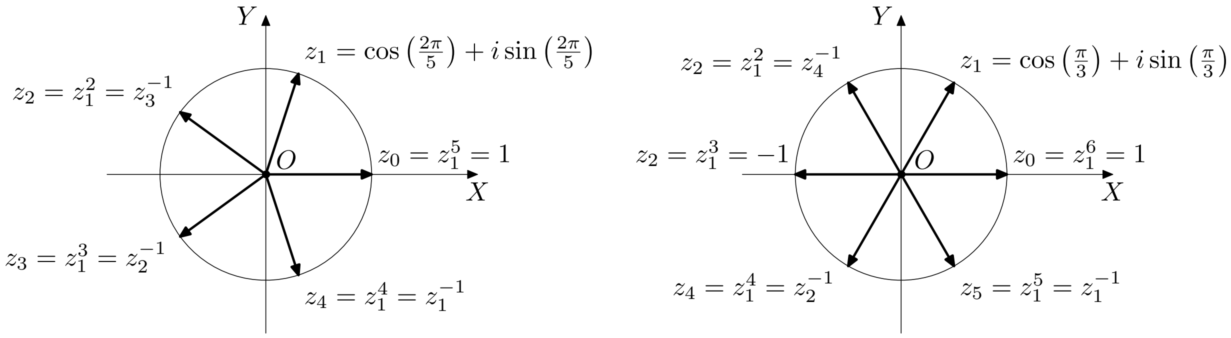
$$\frac{\sin(n\varphi)}{\sin\varphi}=(-4)^{\frac{n-1}{2}}\prod_{\nu=1}^{\frac{n-1}{2}}\left(\sin^2\!\varphi-\sin^2\frac{2\pi\nu}{n}\right)$$

6.3.4. Пример: корни из единицы и уравнение $z^n=a$. Решим в поле $\mathbb{C}$ уравнение $z^n=1$. Сравнивая модули левой и правой части, получаем $|z^n|=|z|^n=1$, откуда $|z|=1$. Обозначая через φ угол радиус-вектора z с осью OX и сравнивая аргументы левой и правой части уравнения, получаем

$$n\varphi\in\mathrm{Arg}\,(1)=\{2\pi k\mid k\in\mathbb{Z}\}\ ,$$

откуда $\varphi\in\{2\pi k/n\mid k\in\mathbb{Z}\}$. Таким образом, уравнение $z^n=1$ имеет ровно n корней $z_0,z_1,\dots,z_{n-1}$, которые располагаются в вершинах правильного n-угольника, вписанного в единичную окружность так, что вершина z_0 находится в точке 1 (см. рис. 6◇3, где $n=5$, 6):

$$z_k=\cos(2\pi k/n)+i\sin(2\pi k/n)\ ,\quad \text{где } k=0,\,1,\,\dots\,,\,(n-1)\ .$$



6◇3. Корни уравнений $z^5 = 1$ и $z^6 = 1$.

В частности, мы видим, что корни образуют циклическую группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-той степени из* 1. Мы уже встречались с нею в примерах (n° 2.1.2), (n° 2.2.2) и (n° 5.1.7). В качестве образующей этой группы можно взять, например, корень $z_1 = \cos(2\pi/n) + i\sin(2\pi/n)$. Тогда $z_k = z_1^k$ для всех $k = 0, 1, \dots, (n-1)$. Образующие группы $\boldsymbol{\mu}_n$ называются *первообразными корнями* степени n из единицы. На рис. 6◇3 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, а среди корней 6-той степени из единицы первообразными являются только z_1 и $z_5 = z_1^{-1}$.

Многочлен, корнями которого являются первообразные корни n-той степени из 1 и только они, называется *многочленом деления круга на n частей* (или *n-тым циклотомическим многочленом*). Например, пятый и шестой циклотомические многочлены равны

$$f_5(z) = (z-z_1)(z-z_2)(z-z_3)(z-z_4) = z^4 + z^3 + z^2 + z + 1$$
$$f_6(z) = (z-z_1)(z-z_4) = z^2 - z + 1 .$$

Упражнение 6.5*. Покажите, что при любом $n \in \mathbb{N}$ циклотомический многочлен $f_n(z)$ является неприводимым[1] над $\mathbb{Q}$ многочленом с целыми коэффициентами степени $\varphi(n)$ (где $\varphi(n)$ — это количество натуральных чисел, меньших n и взаимно простых с n).

Комментарий: Эта задача вместе с другими полезными фактами о циклотомических многочленах (включая несколько более или менее явных формул для них) содержится в «задачах семинаров» в дополнительном листке $6\frac{1}{2}$.

Упражнение 6.6. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ в радикалах от натуральных чисел.

Подсказка: для этого достаточно решить в радикалах уравнение деления круга $z^4 + z^3 + z^2 + z + 1 = 0$, которое сводится к квадратному уравнению делением обеих частей на z^2 и заменой $t = z + z^{-1}$.

Рассмотрим теперь уравнение $z^n = a$. Рассуждая как и выше, получаем

$$|z| = \sqrt[n]{|a|}\,, \quad n\varphi \in \operatorname{Arg}(a) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}\,,$$

где α — угол радиус-вектора a с осью OX. Таким образом, $\varphi \in \left\{ \frac{\alpha}{n} + \frac{2\pi k}{n} \;\middle|\; k \in \mathbb{Z} \right\}$, т. е. корни уравнения $z^n = a$ располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|a|}$ с центром в нуле так, что радиус-вектор одной из его вершин располагается под углом α/n к оси OX.

Упражнение 6.7. Явно выразите действительные и мнимые части корней квадратного уравнения $z^2 = a$ через действительную и мнимую части числа a при помощи четырёх арифметических операций и извлечения квадратных корней из вещественных чисел.

6.4. Определение коммутативного кольца. Множество K с двумя операциями, удовлетворяющими всем аксиомам поля, за исключением требования существования обратного элемента, называется *коммутативным кольцом с единицей*. Если, кроме аксиомы существования обратного, из списка аксиом поля исключить ещё аксиому существования единицы, а с нею и аксиому $0 \neq 1$, множество K, удовлетворяющее оставшимся аксиомам, будет называется просто *коммутативным кольцом*. Модельные примеры колец с единицами, не являющихся полями — это кольцо целых чисел $\mathbb{Z}$, а также кольца многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные

[1] т. е. не раскладывающимся в произведение двух многочленов строго меньшей степени с рациональными коэффициентами

целые числа, многочлены с чётными целыми коэффициентами и многочлены с нулевым свободным членом и коэффициентами в любом коммутативном кольце.

Упражнение 6.8. Покажите, что свойства из упр. 6.1 остаются в силе в любом коммутативном кольце с единицей.

Как явствует из определения, основным отличием колец от полей является возможное отсутствие для некоторых элементов кольца обратных к ним элементов относительно умножения. Элемент a коммутативного кольца называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*. Так, 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). Как следствие, между элементами коммутативного кольца возникает нетривиальное *отношение делимости*. Говорят, что элемент a *делится* на элемент b, если в кольце существует элемент q, такой что $a = bq$. Это обстоятельство записывается как $b|a$ (читается «b делит a») или как $a \vdots b$ (читается «a делится на b»).

6.4.1. Пример: гауссовы целые числа. Рассмотрим в поле комплексных чисел подмножество

$$\mathbb{Z}[i] \overset{\text{def}}{=} \{z = x + iy \mid x, y, \in \mathbb{Z}\} .$$

Числа этого множества располагаются на комплексной плоскости в точках с целочисленными координатами и называются *гауссовыми целыми числами*. Они образуют коммутативное кольцо с единицей относительно операций сложения и умножения комплексных чисел. В $\mathbb{Z}[i]$ имеется ровно 4 обратимых элемента: ± 1 и $\pm i$.

Кольцо $\mathbb{Z}[i]$ имеет много арифметических приложений. Например, вычисления в этом кольце существенно проясняют классическую задачу об описании всех натуральных чисел, представимых в виде суммы двух квадратов целых чисел (нуль при этом тоже допускается в качестве одного из квадратов). Связано это с тем, что квадратичная форма $x^2 + y^2$ над кольцом $\mathbb{Z}[i]$ разлагается в произведение двух линейных множителей: $x^2+y^2 = (x+iy)(x-iy)$, и задача представления натурального числа в виде суммы квадратов двух целых чисел сводится к задаче разложения натурального числа (рассматриваемого как элемента $\mathbb{Z}[i]$) в произведение двух комплексно сопряженных множителей, также лежащих в $\mathbb{Z}[i]$. Отсюда немедленно вытекает, что составное число $m = m_1 m_2$, оба сомножителя в котором представимы в виде суммы двух квадратов:

$$m_1 = a_1^2 + b_1^2 = (a_1 + ib_1)(a_1 - ib_1) = z_1\overline{z}_1 \ , \quad m_2 = a_2^2 + b_2^2 = (a_2 + ib_2)(a_2 - ib_2) = z_2\overline{z}_2 \ ,$$

также может быть представлено в виде суммы двух квадратов:

$$m = z_1 z_2 \cdot \overline{z_1 z_2} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \, .$$

Если доказать для кольца $\mathbb{Z}[i]$ аналог теоремы об однозначности разложения на простые множители (что вскоре будет нами сделано), то предыдущее вычисление полностью сведёт задачу о разложении натурального числа в сумму двух квадратов к вопросу о том, какие *простые* натуральные числа остаются простыми в $\mathbb{Z}[i]$, а какие начинают раскладываться на множители. Мы ещё вернёмся к этой задаче в примере[1] (n° 10.3.8).

Упражнение 6.9. Докажите, что для представимости числа $n \in \mathbb{N}$ в виде суммы двух квадратов целых чисел необходимо и достаточно, чтобы это число имело вид $n = p_1 \cdot p_2 \cdot \dots \cdot p_s \cdot k^2$, где $k \in \mathbb{Z}$ — любое, а $p_1, p_2, \dots, p_s$ — натуральные простые числа, представимые в виде суммы двух квадратов.

Упражнение 6.10*. Докажите, что простое $p \in \mathbb{N}$ тогда и только тогда представимо в виде суммы двух квадратов, когда оно имеет остаток 1 от деления на 4.

6.5. Гомомрфизмы. Отображение колец $A \xrightarrow{\varphi} B$ называется *гомоморфизмом*, если для любой пары элементов $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{gathered} f(a_1 + a_2) = f(a_1) + f(a_2) \\ f(a_1 a_2) = f(a_1) f(a_2) \, . \end{gathered} \tag{6-6}$$

[1] любознательный читатель также может обратиться к замечательной книжке: *К. Айэрленд, М. Роузен. Классическое введение в современную теорию чисел.* М., «Мир», 1987 (или любое другое издание), где найдёт как завершение этой истории, так и разные другие изящные вычисления с гауссовыми числами

Отметим, что этим условиям, в частности, удовлетворяет *нулевой* (или *тривиальный*) гомоморфизм, отображающий все элементы из A в нуль кольца B.

Любой гомоморфизм колец, будучи гомоморфизмом аддитивных групп, обладает всеми свойствами, установленными нами в (n° 5.1). Например, из первого соотношения (6-6) автоматически следует, что $\varphi(0) = 0$ и $\forall\, a \in A\ \ \varphi(-a) = -\varphi(a)$.

Образ гомоморфизма колец является подкольцом в B. Прообраз нулевого элемента

$$\ker(\varphi) \stackrel{\text{def}}{=} \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}$$

называется *ядром* гомоморфизма колец. Ядро является подкольцом в A и вместе с каждым элементом $a \in \ker(\varphi)$ содержит также и все кратные ему элементы ab (с любыми $b \in A$) :

$$\varphi(a) = 0 \quad \Rightarrow \quad \forall\, b \in A\ \ \varphi(ab) = \varphi(a)\varphi(b) = 0\ .$$

Как мы видели в (n° 5.1), прообраз произвольного элемента $\varphi(a) \in \operatorname{im}(\varphi)$ является смежным классом аддитивной группы $\ker(\varphi) \subset A$:

$$\varphi^{-1}\left(\varphi(a)\right) = a + \ker(\varphi) = \{b \in A \mid b - a \in \ker(\varphi)\}\ .$$

Иными словами, два элемента $a, b \in A$ тогда и только тогда переходят в один и тот же элемент кольца B , когда $a - b \in \ker(\varphi)$:

$$\varphi(a) = \varphi\,(b) \quad \Longleftrightarrow \quad \varphi\,(b - a) = \varphi\,(b) - \varphi(a) = 0\ .$$

В частности, для того чтобы гомоморфизм колец был вложением, необходимо и достаточно, чтобы $\ker(\varphi = \{0\}$ (в этом случае говорят, что φ *имеет нулевое ядро*).

6.5.1. ПРЕДЛОЖЕНИЕ. *Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.*

Доказательство. Если $\varphi(a) = 0$ для какого-нибудь $a \neq 0$, то $\forall\, b \in A\ \ \varphi\,(b) = \varphi\left(ba^{-1}a\right) = \varphi\left(ba^{-1}\right)\varphi(a) = 0\,.$ Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. $\square$

§7. Целые числа и вычеты.

7.1. Кольцо вычетов $\mathbb{Z}/(n)$. Элементом этого кольца является *класс вычетов* по модулю n, т. е. *подмножество* в $\mathbb{Z}$, образованное всеми числами, дающими один и тот же остаток от деления на n. Мы уже встречались с классами вычетов в примере (n° 5.1.7), где они интерпретировались как смежные классы аддитивной группы $\mathbb{Z}$ по подгруппе $(n) = \{nk \mid k \in \mathbb{Z}\}$, состоящей из чисел, кратных n. Всего имеется n таких классов, взаимно однозначно соответствующих n различным остаткам:

$$[0]_n,\, [1]_n,\, \dots\, ,\, [(n-1)]_n\ , \quad \text{где} \quad [a]_n = a \pmod{n} = a + (n) = \{a + kn \mid k \in \mathbb{Z}\}\, .$$

Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a+b]\ , \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\ . \tag{7-1}$$

Упражнение 7.1. Проверьте корректность этого определения (т. е. независимость классов $[a+b]$ и $[ab]$ от выбора представителей $a \in [a]$ и $b \in [b]$), а также выполнение в $\mathbb{Z}/(n)$ всех аксиом коммутативного кольца.

Независимость результатов сложения и умножения от выбора представителей в классе иногда позволяет значительно упростить вычисления. Например, для того чтобы вычислить сотую степень класса $2007 \pmod{2008}$ нет нужды возводить в 100-ю степень число 2007, поскольку $[2007]_{2008} = [-1]_{2008}$ и согласно упр. 7.1 мы имеем $2007^{100} \equiv (-1)^{100} \equiv 1 \pmod{2008}$.

7.2. Делители нуля и нильпотенты. В кольцах $\mathbb{Z}/(n)$ мы сталкиваемся с рядом явлений, которые не наблюдаются ни в полях, ни в кольце целых (или гауссовых целых) чисел. Так, в кольце $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(27)$ ненулевой класс $[3]$ имеет нулевой куб $[3]^3 = [27] = [0]$.

Ненулевой элемент a кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Ненулевой элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Отметим, что всякий нильпотент автоматически является делителем нуля.

Кольцо с единицей без делителей нуля называется *целостным*. Кольцо с единицей без нильпотентов называется *приведённым*. Всякое целостное кольцо автоматически приведено.

Упражнение 7.2. Составьте таблицы сложения и умножения в кольцах $\mathbb{Z}/(n)$ для $n = 3, 4, 5, 6, 7, 8$. Найдите в этих кольцах все делители нуля, все нильпотенты, и все обратимые элементы. Для обратимых элементов составьте таблицу обратных. Какие из этих колец являются полями?

Наличие делителей нуля является простейшим препятствием к тому, чтобы кольцо было полем. В самом деле, никакой делитель нуля a не может быть обратим, поскольку система условий

$$\begin{cases} b \neq 0 \\ ab = 0 \\ aa^{-1} = 1 \end{cases}$$

несовместна: умножая обе части второго равенства на a^{-1} мы получаем $b = 0$, что противоречит первому равенству. Отметим, что написанным выше условиям удовлетворяет, в частности, нулевой элемент $a = 0$. Именно поэтому «на ноль делить нельзя», и в аксиоме существования обратного элемента в поле накладывается требование $a \neq 0$ (см. аксиому (2г) на стр. 37).

7.2.1. Пример: действие гомоморфизма колец на единицу. Поскольку кольцо не является группой относительно операции умножения, гомоморфизм коммутативных колец с единицами $A \xrightarrow{\varphi} B$, вообще говоря, не обязан переводить единицу в единицу. Например, отображение $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/(6)$, отправляющее все чётные числа в нулевой класс, а все нечётные — в класс $[3]_6$, является гомоморфизмом колец, и $\varphi(1) = [3]_6 \neq [1]_6$. Тем не менее, вычисление из (n° 5.1) : $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ влечёт в кольце равенство $\varphi(1)(\varphi(1) - 1) = 0$. Если в кольце B нет делителей нуля, из этого равенства следует, что либо $\varphi(1) = 0$, и тогда $\forall a\in A \ \ \varphi(a)=\varphi(1\cdot a)=\varphi(1)\varphi(a)=0$, либо $\varphi(1)=1$. Таким образом, любой нетривиальный гомоморфизм в в целостное кольцо с единицей всё-таки переводит единицу в единицу.

7.3. Обратимые элементы кольца $\mathbb{Z}/(n)$. Класс $[m]_n$ обратим в кольце $\mathbb{Z}/(n)$ тогда и только тогда, когда в кольце целых чисел $\mathbb{Z}$ разрешимо относительно x и y уравнение

$$mx+ny=1\,. \tag{7-2}$$

В самом деле, обратимость класса $[m]_n$ означает существование такого класса $[x]_n$, что

$$[m]_n[x]_n=[mx]_n=[1]_n\ ,$$

а это, в свою очередь, равносильно соотношению (7-2). Чтобы понять, для каких $m,n\in\mathbb{Z}$ уравнение (7-2) обладает целочисленными решениями, зафиксируем какие-нибудь m и n и рассмотрим всю совокупность целых чисел, представимых в виде $mx+ny$ с целыми x, y. Обозначим её через

$$(m,n)\overset{\text{def}}{=}\{mx+by\mid x,y\in\mathbb{Z}\}\,. \tag{7-3}$$

Упражнение 7.3. Покажите, что подмножество $(m,n)\subset\mathbb{Z}$ обладает следующими свойствами:
а) любое число $z\in(m,n)$ делится на каждый общий делитель чисел m и n
б) $m,n\in(m,n)$ в) $z\in(m,n)\Rightarrow kz\in(m,n)\ \forall k\in\mathbb{Z}$ г) $z_1,z_2\in(m,n)\Rightarrow z_1\pm z_2\in(m,n)$

Обозначим через d наименьшее положительное число в (m,n). Отметим, что d, как и все числа в (m,n), представляется в виде $d=mx+ny$ и делится на каждый общий делитель чисел m и n. С другой стороны, любое $z\in(m,n)$ (в частности, $z=m,n$) делится на d. В самом деле, деля $z\in(m,n)$ на d с остатком, мы получаем равенство $z=kd+r$, в котором остаток $r=z-kd$ лежит в (m,n) по упр. 7.3 и находится в пределах $0\leqslant r\leqslant(d-1)$. В силу выбора d мы должны иметь $r=0$. Таким образом, $(m,n)=(d)$ совпадает с множеством чисел, кратных d, и $d=\text{нод}(m,n)$ является *наибольшим общим делителем*[1] m и n.

Итак, уравнение (7-2) разрешимо тогда и только тогда, когда $d=\text{нод}(a,n)=1$, а значит, обратимыми элементами кольца $\mathbb{Z}/(n)$ являются классы $[m]_n$ с $\text{нод}(m,n)=1$.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют группу относительно умножения. Эта группа называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Порядок этой группы обозначается через $\varphi(n)$ и называется *функцией Эйлера* числа $n\in\mathbb{N}$. Иначе можно сказать, что $\varphi(n)$ равно количеству натуральных чисел, меньших n и взаимно простых с n. Из следствия (n° 3.3.1) теоремы Лагранжа мы заключаем, что для любого обратимого вычета $[a]\in\mathbb{Z}/(n)^*$ выполняется равенство $[a^{\varphi(n)}]=[a]^{\varphi(n)}=[1]$. Иными словами, справедливо

7.3.1. ПРЕДЛОЖЕНИЕ (ТЕОРЕМА ЭЙЛЕРА). *Если* $\text{нод}(a,n)=1$, *то* $a^{\varphi(n)}\equiv 1\,(\mathrm{mod}\, n)$. □

7.3.2. СЛЕДСТВИЕ (МАЛАЯ ТЕОРЕМА ФЕРМА). *Если p простое, то* $a^p\equiv a\,(\mathrm{mod}\, p)\ \ \forall a\in\mathbb{Z}$.

Доказательство. Если a делится на p, то обе части сравнения $a^p\equiv a\,(\mathrm{mod}\ p)$ нулевые. Если a не делится на p, мы можем применить предыдущее предложение. Так как $\varphi(p)=p-1$ для простого p, мы получим $a^{p-1}\equiv 1\,(\mathrm{mod}\, p)$, а значит, $a^p\equiv a\,(\mathrm{mod}\, p)$. □

Упражнение 7.4. Вычислите остаток от деления $2007^{2008^{2009}}$ на 11.

7.4. Алгоритм Евклида. Практическое отыскание решений уравнения (7-2) производится следующим образом. Пусть $n\geqslant m$. Положим

$$E_0=n\,,\quad E_1=m\,,\quad E_k=\text{остатку от деления } E_{k-2} \text{ на } E_{k-1} \text{ (при } k\geqslant 1). \tag{7-4}$$

Числа E_k строго убывают до тех пор, пока какое-то E_r не разделит нацело предыдущее E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой элемент E_r последовательности

[1] заметим, что по ходу дела мы доказали, что наибольший общий делитель нацело делится на любой другой общий делитель

E_k и будет наибольшим общим общим делителем чисел (m,n), причём он автоматически получится представленным в виде $E_r = x \cdot E_0 + y \cdot E_1$, если при вычислении каждого E_k мы будем представлять его в виде $E_k = x \cdot E_0 + y \cdot E_1$.

Упражнение 7.5. Индукцией по k убедитесь, что все числа E_k представляются в виде $E_k = x \cdot E_0 + y \cdot E_1$ (и стало быть, делятся на любой общий делитель чисел m и n), а затем, убывающей индукцией по k, начинающейся с $k = r+1$ убедитесь, что все числа E_k (включая $E_0 = n$ и $E_1 = m$) делятся на E_r (и стало быть, $E_r = \text{нод}(m,n)$).

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

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

(взятая в скобки последняя строка служит для проверки), и мы заключаем из него, что

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

откуда вытекает, в частности, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и

$$[10\,203]^{-1} = [147]\,(\mathrm{mod}\ 4\,687)\,,$$

а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $[4\,687]^{-1} = -[320]\,(\mathrm{mod}\ 10\,203)$.

Упражнение 7.6. Докажите, что представление первого нулевого числа $E_{r+1} = q_0E_0 + q_1E_1 = 0$, получающееся согласно алгоритму Евклида, содержит в себе *наименьшее общее кратное* чисел $E_0 = m$ и $E_1 = n$, а именно $\text{нок}(m,n) = |q_0E_0| = |q_1E_1|$ (т. е. «дополнительные множители» q_0, q_1 таковы, что $\text{нод}(q_0,q_1) = 1$).

Отметим, что с вычислительной точки зрения нахождение наибольшего общего делителя пары чисел при помощи алгоритма Евклида является *несопоставимо* менее трудоёмкой задачей, чем разложение этих чисел на простые множители[1], в чём читатель может убедиться, попробовав разложить на простые множители предыдущие числа $n = 10\,203$ и $m = 4\,687$.

7.5. Прямые произведения групп и колец. Из любого набора групп $G_1, G_2, \dots, G_m$ можно изготовить новую группу

$$\prod_\nu G_\nu = G_1 \times G_2 \times \cdots \times G_\nu = \{(g_1, g_2, \dots, g_m) \mid g_\nu \in G_\nu \; \forall\, \nu\}\,,$$

которая называется *прямым произведением* групп G_ν и состоит из упорядоченных наборов $(g_1, g_2, \dots, g_m)$ операция на которых определяется покомпонентно:

$$(g_1, g_2, \dots, g_m) \cdot (h_1, h_2, \dots, h_m) = (g_1 \cdot h_1,\ g_2 \cdot h_2,\ \cdots,\ g_m \cdot h_m)\,. \tag{7-5}$$

Упражнение 7.7. Проверьте, что так определённая операция ассоциативна и обладает единицей $e = (e_1, e_2, \dots, e_m)$ (где каждое e_ν — это единица группы G_ν), а также что у каждого элемента $g =$

[1]найти два больших простых числа, если известно их произведение, за разумное время невозможно даже на мощном компьютере; это обстоятельство лежит в основе большинства используемых в настоящее время систем шифрования данных

$(g_1, g_2, \dots, g_m)$ имеется обратный $g^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_m^{-1})$. Кроме того, убедитесь, что если все группы G_ν коммутативны, то группа $\prod G_\nu$ тоже получится коммутативная.

Отметим, что эта конструкция работает не только для конечных наборов групп, но и для любых семейств групп G_ν, занумерованных элементами $\nu \in X$ произвольного множества X. Соответствующее произведение обозначается тогда $\prod\limits_{\nu \in X} G_\nu$. Отметим также, что если все группы $G_1, G_2, \dots, G_m$ конечны, то произведение тоже конечно и имеет порядок $|\prod G_\nu| = \prod |G_\nu|$.

Аналогичным образом, для любого множества колец $\{K_\nu\}_{\nu \in X}$ можно образовать прямое произведение $\prod K_\nu$, представляющее собою множество упорядоченных наборов элементов

$$(\dots, a_\nu, \dots)\,, \quad \text{где } a_\nu \in K_\nu$$

и покомпонентными операциями, заданными формулой (7-5):

$$(\dots, a_\nu, \dots) + (\dots, b_\nu, \dots) \stackrel{\text{def}}{=} (\dots, a_\nu + b_\nu, \dots)$$
$$(\dots, a_\nu, \dots)(\dots, b_\nu, \dots) \stackrel{\text{def}}{=} (\dots, a_\nu b_\nu, \dots)\,.$$

Упражнение 7.8. Проверьте, что $\prod K_\nu$ является кольцом, причём если все K_ν были кольцами с единицей, то $\prod K_\nu$ также будет кольцом с единицей.

Отметим, что элемент кольца-произведения $a = (a_1, a_2, \dots, a_m) \in K_1 \times K_2 \times \cdots \times K_m$ обратим тогда и только тогда, когда каждая его компонента $a_\nu \in K_\nu$ обратима в своём кольце K_ν. Поэтому группа обратимых элементов кольца $\prod K_\nu$ будет прямым произведением групп обратимых элементов колец K_ν:

$$\left(\prod K_\nu\right)^* = \prod K_\nu^* \tag{7-6}$$

Отметим также, что в прямом произведении колец всегда имеются делители нуля: любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0, 1, 1, \dots, 1)$ является делителем нуля, поскольку

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

Таким образом, произведение колец никогда не является полем. В частности, полем не является и произведение полей. Скажем, если $\mathbb{F}_p$ и $\mathbb{F}_q$ — конечные поля, состоящие соответственно из p и q элементов, то в их произведении $\mathbb{F}_p \times \mathbb{F}_q$ будет ровно $(p-1)(q-1)$ обратимых элементов (a, b), образующих мультипликативную группу $\mathbb{F}_p^* \times \mathbb{F}_q^*$ и $p + q - 2$ делителя нуля, имеющих вид $(a, 0)$ и $(0, b)$ с $a, b \neq 0$.

7.6. Взаимная простота. Сделаем несколько важных замечаний о делимости, относящихся к произвольному коммутативному кольцу K с единицей. Элементы $a, b \in K$ называются *взаимно простыми*, если

$$ax + by = 1 \quad \text{для некоторых } x, y \in K\,. \tag{7-7}$$

Если элементы a и b взаимно просты, то произведение mb с произвольным $m \in K$ делится на a только тогда, когда m делится на a. В самом деле, умножая равенство (7-7) на m, мы получаем

$$m = amx + bmy\,, \tag{7-8}$$

и если mb делится на a, то и m делится на a. Это же вычисление показывает, что если m делится на a и на b, то m делится и на произведение ab (поскольку оба слагаемых в правой части (7-8) делятся в этом случае на ab).

Далее, если элемент $a \in K$ взаимно прост с каждым из элементов $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением. В самом деле, если для каждого i мы можем подобрать такие $x_i, y_i \in K$, что $ax_i + b_i y_i = 1$, то, перемножив все эти равенства, мы получим равенство вида[1]

$$a \cdot x + (b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) = 1\,,$$

[1] в первом слагаемом собраны все члены, содержащие сомножитель a, во втором — единственный член не содержащий такого сомножителя

устанавливающее взаимную простоту a и $b_1 b_2 \cdots b_n$.

7.6.1. Пример: китайская теорема об остатках. Пусть число $n \in \mathbb{Z}$ является произведением m попарно взаимно простых сомножителей: $n = n_1 n_2 \cdots n_m$. Покажем, что в этом случае кольцо вычетов $\mathbb{Z}/(n)$ изоморфно прямому произведению колец вычетов $\mathbb{Z}/(n_i)$, т. е. построим такое взаимно однозначное отображение

$$\mathbb{Z}/(n) \xrightarrow{\varphi} (\mathbb{Z}/(n_1)) \times (\mathbb{Z}/(n_2)) \times \cdots \times (\mathbb{Z}/(n_m)) ,$$

что $\forall\, a, b \in \mathbb{Z}/(n)$ $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ в $\prod \mathbb{Z}/(n_i)$. Зададим φ правилом

$$\varphi([z]_n) \stackrel{\text{def}}{=} ([z]_{n_1}, [z]_{n_2}, \ldots, [z]_{n_m}) \qquad \forall\, z \in \mathbb{Z} .$$

Это правило корректно (не зависит от выбора числа $z \in \mathbb{Z}$ в классе $[z]_n \subset \mathbb{Z}$), поскольку равенство $[z_1]_n = [z_2]_n$ означает, что разность $z_1 - z_2$ делится на $n = n_1 n_2 \cdots n_m$, а значит, она делится и на каждое n_i, и стало быть, для каждого i мы будем иметь равенство $[z_1]_{n_i} = [z_2]_{n_i}$. Очевидно, также, что φ является гомоморфизмом:

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

и ровно то же самое произойдёт с умножением. Покажем, что φ, рассматриваемый как гомоморфизм аддитивных групп, имеет нулевое ядро. В самом деле, рассмотрим класс $[z]_n \in \ker(\varphi)$. Поскольку для любого i класс $[z]_{n_i}$ нулевой, z делится на каждое n_i, а так как все n_i попарно взаимно просты, то z должен делиться и на их произведение (см. n° 7.6), которое равно n. Тем самым $[z]_n = 0$, что и требовалось.

Из следствия (n° 5.1.2) теоремы о строении гомоморфизма групп мы заключаем, что φ является вложением. А так как оба кольца $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ состоят из одинакового числа элементов $n = \prod n_i$, гомоморфизм φ должен быть биекцией. Этот факт известен как *китайская теорема об остатках*, поскольку на классическом языке он утверждает, что для любого набора остатков $r_1, r_2, \ldots, r_m$ от деления на попарно взаимно простые числа $n_1, n_2, \ldots, n_m$ можно подобрать такое целое число z, которое даёт остаток r_i от деления *на каждое* из n_i, причём любые два числа z_1, z_2, решающие эту задачу, различаются на целое кратное числа $n = n_1 n_2 \cdots n_k$.

Для практического отыскания такого числа z полезно установить сюрьективность гомоморфизма φ непосредственно, не прибегая к теореме о гомоморфизме групп. Для этого заметим, что из взаимной простоты числа n_i с остальными n_ν вытекает, что n_i взаимно просто и с их произведением $m_i = \prod\limits_{\nu \neq i} n_\nu$ (см. n° 7.6), т. е. для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Числа $b_i = m_i y_i$ обладают, таким образом, следующим замечательным свойством:

$$[b_i]_{n_i} = [1]_{n_i} \quad \text{и} \quad \forall\, \nu \neq i \;\; [b_i]_{n_\nu} = [0]_{n_\nu} . \tag{7-9}$$

Поэтому в качестве числа z, отображающегося в заданные классы $[r_i]_{n_i}$ при всех i, можно взять

$$z = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m .$$

Для демонстрации эффективности этого алгоритма найдём, к примеру, наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$. Сначала найдём $y_1 \in \mathbb{Z}$, такое что $91 \cdot 179 \cdot y_1 \equiv 1 \pmod{57}$. Поскольку $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, достаточно применить алгоритм Евклида к $E_0 = 57$ и $E_1 = 13$. В результате получим $22 \cdot 13 - 5 \cdot 57 = 1$. 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). Аналогичным образом находим числа

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

дающие при делении на 57, 91 и 179 остатки (0, 1, 0) и (0, 0, 1) соответственно. Тогда остатки (2, 7, 43) будет иметь число

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

а все остальные числа с такими остатками будут отличаться от z на целые кратные числа

$$n = 57 \cdot 91 \cdot 179 = 928\,473\,.$$

Наименьшим положительным среди них является $z + 15\,n = 816\,641$.

7.7. Наибольший общий делитель. Рассмотрим произвольное целостное[1] кольцо K. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Из равенств $a = mb$ и $b = na$ вытекает равенство $a - mb = a - mna = a(1 - mn) = 0$, откуда[2] $mn = 1$. Таким образом, ассоциированность элементов a и b равносильна тому, что a и b получаются друг из друга умножением на обратимый элемент кольца. Например, в кольце целых чисел $\mathbb{Z}$ числа a и b ассоциированы тогда и только тогда, когда $a = \pm b$.

Всякое $d \in K$, делящее a и b и делящееся на любой другой элемент, делящий a и b, называется *наибольшим общим делителем* элементов a и b и обозначается $\text{нод}(a, b)$. Отметим, что применительно к произвольному целостному кольцу K это определение никоим образом не гарантирует ни существования, ни единственности наибольшего общего делителя. Если наибольшие общие делители существуют, то все они ассоциированы друг с другом. Поэтому запись $\text{нод}(a, b) = d$ не вполне корректна, но ей всё-таки принято пользоваться, имея в виду, что d в правой части определено с точностью до умножения на любой обратимый элемент. Для некоторых специальных колец K наибольший общий делитель можно зафиксировать однозначно, используя особые свойства кольца K. Так, в кольце целых чисел $\mathbb{Z}$ из двух ассоциированных чисел $\text{нод}(a, b) = \pm d$ наибольшим общим делителем принято называть *положительный* наибольший общий делитель.

Подчеркнём, что в общем случае из условия $\text{нод}(a, b) = 1$ *не вытекает*, что a и b взаимно просты. Например, в кольце $\mathbb{Q}[t_1, t_2]$ многочленов с рациональными коэффициентами от переменных t_1, t_2 элементы $a = t_1$ и $b = t_2$ таковы, что $\text{нод}(t_1, t_2) = 1$, однако $t_1 \cdot x + t_2 \cdot y \neq 1$ ни при каких $x, y \in \mathbb{Q}[x, y]$, т. е. одночлены t_1 и t_2 *не взаимно просты*. Этот же пример показывает, что в произвольном кольце $\text{нод}(a, b)$ (даже если он существует) вовсе не обязан представляться в виде $ax + by$.

Рассуждение из (n° 7.3) и (n° 7.4) *доказывают* следующее предложение:

7.7.1. ПРЕДЛОЖЕНИЕ. *В кольце целых чисел $\mathbb{Z}$ любые два числа a, b обладают наибольшим общим делителем*[3]*, причём он может быть представлен в виде $\text{нод}(a, b) = ax + by$. Взаимная простота чисел $a, b \in \mathbb{Z}$ равносильна условию $\text{нод}(a, b) = 1$.* □

7.8. Разложение на неприводимые множители. Элемент q произвольного коммутативного кольца K называется *неприводимым*, если он не обратим, и из равенства $q = mn$ вытекает, что один из множителей m, n обратим. Если элемент $q \in K$ неприводим, то $\text{нод}(a, q) = 1$ для любого $a \in K$, не делящегося на q. Неприводимые элементы кольца целых чисел $\mathbb{Z}$ — это простые числа. Из предложения (n° 7.7.1) вытекает, что любое простое число p взаимно просто с любым целым числом a, не делящимся на p. В частности, произведение нескольких целых чисел делится на простое число p только при условии, что хотя бы один из множителей делится на p, и если какое-то целое число n делится на каждое из m различных простых чисел $p_1, p_2, \dots, p_m$, то n делится и на их произведение. Из этих двух свойств вытекает, что разложение произвольного целого числа n в произведение простых множителей *единственно* с точностью до выбора знаков у этих множителей.

7.8.1. ПРЕДЛОЖЕНИЕ. *Каждое целое число $n \neq \pm 1$ представляется в виде произведения простых чисел, причём любые два таких представления $p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_m$ состоят из одинакового числа сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $p_i = \pm q_i$ для всех i.*

[1] напомним (см. n° 7.2) что кольцо называется *целостным*, если в нём нет делителей нуля

[2] здесь мы пользуемся тем, что в K нет делителей нуля

[3] и единственен с точностью до знака; обычно этот знак выбирают положительным и называют наибольшим общим делителем целых чисел их *натуральный* наибольший общий делитель

Доказательство. Докажем вначале существование разложения. Если n простое, то доказывать нечего. Если нет, представим его в виде $n = m_1 m_2$ с $|m_1|, |m_2| < |n|$. Если среди сомножителей имеются составные, также разложим их в произведение меньших по абсолютной величине сомножителей и т. д. Поскольку абсолютная величина непростых сомножителей всё время уменьшается, этот процесс когда-то должен закончиться и мы получим требуемое разложение. Докажем теперь единственность. Пусть $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, где все сомножители просты. Как мы уже говорили, из простоты p_1 вытекает, что хотя бы один из сомножителей в правой части делится на p_1. Пусть это $q_1 = s p_1$. Поскольку q_1 неприводим, s обратим, т. е. $q_1 = \pm p_1$. Вынося p_1, получим $p_1(p_2 \cdots p_k \pm q_2 \cdots q_m) = 0$, откуда следует более короткое равенство $p_2 p_3 \cdots p_k = (\pm q_2) q_3 \cdots q_m$ и т. д. □

7.9. Поле $\mathbb{F}_p = \mathbb{Z}/(p)$. Из данного в (n° 7.3) описания обратимых элементов кольца $\mathbb{Z}/(n)$ вытекает, что это кольцо является полем тогда и только тогда, когда $n = p$ является *простым числом*. В самом деле, если $n = mk$ составное, ненулевые классы $[m], [k] \in \mathbb{Z}/(n)$ будут делителями нуля, что противоречит их обратимости. Напротив, если p простое число, $\text{нод}(m, p) = 1$ для всех m не кратных p, а значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим. Обратный класс $[m]^{-1}$ находится применением алгоритма Евклида к $E_0 = p$ и $E_1 = m$.

Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$. В поле $\mathbb{F}_p$ выполняется замечательное равенство

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

В результате $\forall\ a, b \in \mathbb{F}_p$ имеет место тождество $(a + b)^p = a^p + b^p$. В самом деле, при раскрытии скобок в биноме $(a + b)^p$ одночлены $a^k b^{p-k}$ возникают в виде суммы всевозможных слов, состоящих из k букв a и $(p - k)$ букв b, и приведение всех этих подобных слагаемых означает представление этой суммы в виде

$$a^k b^{p-k} \cdot (\underbrace{1 + 1 + \ \cdots \ + 1}_{\frac{p!}{k!(p-k)!} \text{ раз}})\,.$$

Поскольку $\frac{p!}{k!(p-k)!}$ делится на p при простом p и $1 \leqslant k \leqslant (p - 1)$ (ибо числитель делится на p, а знаменатель — нет), сумма в скобках обращается в нуль при всех $k \neq 0, p$. Это даёт ещё одно доказательство *малой теоремы Ферма* (см. n° 7.3.2):

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

7.9.1. Пример: конечные геометрии. Многие понятия и конструкции из геометрии вещественной координатной плоскости $\mathbb{R}^2$ или вещественного координатного пространства $\mathbb{R}^3$ сохраняют свой смысл после замены поля вещественных чисел $\mathbb{R}$ *произвольным* полем $\Bbbk$. А именно, будем называть *координатной плоскостью* над полем $\Bbbk$ множество упорядоченных пар элементов поля $\Bbbk$:

$$\Bbbk^2 \stackrel{\text{def}}{=} \Bbbk \times \Bbbk = \{(x, y) \mid x, y \in \Bbbk\}\,.$$

Элементы (x, y) этой плоскости мы будем называть *точками*. Наряду с точками в геометрии рассматриваются *векторы*, также представляющие собою упорядоченные пары чисел $(a_1, a_2) \in \Bbbk \times \Bbbk$. Пространство векторов удобно рассматривать отдельно от пространства точек. Векторы можно складывать и умножать на числа из поля $\Bbbk$: если $a = (a_1, a_2)$, $b = (b_1, b_2)$ и $\lambda \in \Bbbk$, то по определению $a + b = (a_1 + a_2, b_1 + b_2)$ и $\lambda \cdot a = (\lambda a_1, \lambda a_2)$. В частности, векторы образуют абелеву группу относительно операции сложения. Эта абелева группа действует на точечном пространстве $\Bbbk^2$ преобразованиями сдвига: каждому вектору $v = (v_1, v_2)$ отвечает *сдвиг на вектор v*

$$\tau_v : \Bbbk^2 \xrightarrow{(x,y) \mapsto (x+v_1, y+v_2)} \Bbbk_2$$

(проверьте, что композиции сдвигов отвечает сложение векторов, т. е. $\tau_v \tau_w = \tau_{v+w}$). Прямую на плоскости $\Bbbk^2$ можно определить либо как множество точек (x, y), удовлетворяющих какому-нибудь линейному уравнению $ax + by = c$, в котором хотя бы один из коэффициентов a, b отличен от нуля, либо как траекторию движения какой-нибудь точки $z_0 = (x_0, y_0)$ с ненулевой постоянной скоростью $v = (v_1, v_2)$, т.е. как множество точек вида $z_t = z_0 + tv = (x_0 + tv_1, y_0 + tv_2)$, где «время» t пробегает поле $\Bbbk$.

Упражнение 7.9. Убедитесь, что эти два определения эквивалентны в том смысле, что прямая, заданная уравнением $ax + by = c$ представляет собой траекторию любой своей точки, выпущенной со скоростью $(-b, a)$, и наоборот, траектория точки (x_0, y_0), выпущенной со скоростью $v = (v_1, v_2)$, задаётся уравнением $v_2x - v_1y = v_2x_0 - v_1y_0$.

Упражнение 7.10. Проверьте, что на плоскости $\Bbbk^2$ над любым полем $\Bbbk$ выполняются евклидовы аксиомы инцидентности:

а) имеются три точки, не лежащие на одной прямой;

б) через любые две точки проходит ровно одна прямая;

в) через точку, не лежащую на данной прямой, проходит ровно одна прямая, не пересекающаяся с данной.

Таким образом, любые конфигурационные задачи[1] школьной планиметрии можно рассматривать над любым полем. Например, над конечным полем $\mathbb{F}_p$ из p элементов.

Плоскость $\mathbb{F}_p^2$ над полем $\mathbb{F}_p$ состоит из p^2 точек. Каждая лежащая на ней прямая содержит в точности p из них, поскольку точки $z + t_1v$ и $z + t_2v$ различны при $t_1 \neq t_2$. Так как через любую пару различных точек проходит единственная прямая, через каждую точку плоскости проходит ровно $(p^2 - 1)/(p - 1) = p + 1$ прямых[2], а всего на плоскости $\mathbb{F}_p^2$ будет $\binom{p^2}{2}/\binom{p}{2} = p(p+1)$ прямых[3].

На рис. 7◇1 изображены все 25 точек плоскости $\mathbb{F}_5^2$. Начало координат помечено символом $+$, горизонтальная и вертикальная координатные оси состоят из точек, помеченных символами «0» и «∞» соответственно, точки каждой из проходящих через начало координат прямых $y = kx$, где $k \equiv 0, 1, \dots, 5$, также помечены соответствующей цифрой k (вертикальная координатная ось $x = 0$ отвечает значению $k = \infty$).

4	3	∞	2	1
2	4	∞	1	3
0	0	+	0	0
3	1	∞	4	2
1	2	∞	3	4

Рис. 7◇1. Шесть проходящих через начало координат прямых на плоскости $\mathbb{F}_5^2$.

Обратите внимание, что четыре точки «3», также как и четыре точки «2», тоже составляют одну прямую вместе с точкой «+».

Упражнение 7.11. Нарисуйте на плоскости $\mathbb{F}_5^2$ коники $y = x^2$, $x^2 + y^2 = 1$ и $x^2 + y^2 = -1$.

Упражнение 7.12. Сколько прямых и плоскостей имеется в трёхмерном пространстве $\mathbb{F}_p^3$ над полем из p элементов, и сколько из них проходит через начало координат?

7.10. Поля частных. Способ, которым поле $\mathbb{Q}$ получается из кольца $\mathbb{Z}$, дословно обобщается на произвольное целостное кольцо K. А именно, с K можно связать поле Q_K и гомоморфизм

$$K \overset{\iota}{\hookrightarrow} Q_K \tag{7-10}$$

обладающий следующим *свойством универсальности*: для любого вложения $K \overset{\varphi}{\hookrightarrow} \mathbb{F}$ в произвольное поле $\mathbb{F}$ существует единственное вложение полей $\mathbb{Q}_F \xrightarrow{\widetilde{\varphi}} \mathbb{F}$, такое что $\varphi = \widetilde{\varphi} \circ \iota$:

$$\begin{tikzcd} K \arrow[rr, "\iota"] \arrow[dr, "\varphi"'] & & Q_K \arrow[dl, "\widetilde{\varphi}"] \\ & \mathbb{F} & \end{tikzcd}$$

Таким образом, поле Q_K будет наименьшим по включению полем, в которое можно вложить кольцо K.

[1] т.е. относящиеся к взаимному расположению точек и прямых и не использующие понятий из метрической геометрии, таких как расстояния или величины углов

[2] при фиксированном $z \in \mathbb{F}_p^2$ имеется $p^2 - 1$ записей (z, w) с $w \neq z$, $w \in \mathbb{F}_p^2$, и для каждой проходящей через z прямой ℓ имеется ровно $p - 1$ способ записать её в виде (z, w) с $w \neq z$, $w \in \ell$

[3] всего имеется $\binom{p^2}{2}$ записей (z, w) с $z, w \in \mathbb{F}_p^2$ и $w \neq z$, и каждая прямая ℓ ровно $\binom{p}{2}$ способами записывается в виде (z, w) с $z, w \in \ell$ и $w \neq z$

Отметим, что этим свойством поле Q_K определяется однозначно с точностью до единственного изоморфизма перестановочного с ι, в том смысле, что для любого другого универсального гомоморфизма $K \xrightarrow{\iota'} Q'_K$ имеется единственный изоморфизм $\psi : Q_K \xrightarrow{\sim} Q'_K$, такой что $\iota' = \psi \circ \iota$. В самом деле, в силу универсальности гомоморфизма ι, гомоморфизм ι' единственным образом представляется в виде $\iota' = \psi \circ \iota$, а в силу универсальности гомоморфизма ι', гомоморфизм ι точно так же единственным образом представляется в виде $\iota = \psi' \circ \iota'$, причём композиция $\psi' \circ \psi$ доставляет разложение самого гомоморфизма ι в виде $\iota = \psi' \circ \psi \circ \iota$. Поскольку одновременно $\iota = \mathrm{Id}_{Q_K} \circ \iota$, из единственности такого представления вытекает, что $\psi' \circ \psi = \mathrm{Id}_{Q_K}$. Аналогично проверяется, что $\psi \circ \psi' = \mathrm{Id}_{Q'_K}$. Таким образом, ψ' и ψ являются взаимно обратными изоморфизмами, что и утверждалось.

Универсальное поле Q_K называется *полем частных* целостного кольца K. Для его построения рассмотрим множество всех формальных дробей a/b, в которых $a, b \in K$ и $b \neq 0$. Зададим на этом множестве отношение эквивалентности (см. (n° 1.4.3)), полагая

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \quad \iff \quad a_1 b_2 - a_2 b_1 = 0 \,. \tag{7-11}$$

Это отношение очевидно рефлексивно и симметрично. Если $a_1/b_1 \sim a_2/b_2$ и $a_2/b_2 \sim a_3/b_3$, то умножая равенство $a_1 b_2 - a_2 b_1 = 0$ на b_3 и равенство $a_2 b_3 - a_3 b_2 = 0$ на b_1 и вычитая второе из первого, мы получим равенство $a_1 b_3 - a_3 b_1 = 0$, означающее, что $a_1/b_1 \sim a_3/b_3$. Тем самым, отношение (7-11) транзитивно, и стало быть, множество всех дробей разбивается в объединение непересекающихся классов эквивалентности. Обозначим множество классов эквивалентности через Q_K и определим сложение и умножение классов стандартными правилами

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \,.$$

Упражнение 7.13. Проверьте, что эти определения корректны (не зависят от выбора представителей в классах: если $a'b'' - a''b' = 0$, то $(a'/b') \cdot (c/d) \sim (a''/b'') \cdot (c/d)$ и $(a'/b') + (c/d) \sim (a''/b'') + (c/d)$ для любой дроби (c/d)) и задают на Q_K структуру коммутативного кольца с единицей.

Поскольку любой элемент $a/b \in Q_K$ с $a \neq 0$ обладает обратным элементом b/a, кольцо Q_K является полем. Зададим гомоморфизм (7-10) правилом

$$\iota : K \xhookrightarrow{a \mapsto a/1} Q_K \tag{7-12}$$

($a \in K$ переходит в класс дроби $a/1$). Он, очевидно, инъективен. Если мы хотим продолжить ненулевой гомоморфизм $K \xrightarrow{\varphi} \mathbb{F}$ до гомоморфизма $Q_K \xrightarrow{\widetilde{\varphi}} \mathbb{F}$, то такое продолжение единственно, ибо обязано задаваться правилом

$$\widetilde{\varphi}(a/b) = \widetilde{\varphi}\left(ab^{-1}\right) = \widetilde{\varphi}(a) \cdot \widetilde{\varphi}\left(b^{-1}\right) = \varphi(a)\varphi(b)^{-1} \in \mathbb{F} \,.$$

Упражнение 7.14. Проверьте, что это правило и в самом деле корректно определяет гомоморфизм.

Применительно к кольцу $K = \mathbb{Z}$ эта конструкция приводит к полю $Q_{\mathbb{Z}} = \mathbb{Q}$, и его универсальность означает в этом случае, что поле рациональных чисел $\mathbb{Q}$ единственным образом вкладывается в любое поле $\mathbb{F}$, содержащее $\mathbb{Z}$ в качестве подкольца. В частности, оно остаётся на месте при любом автоморфизме $\mathbb{F} \longrightarrow \mathbb{F}$ такого поля. Тем самым, любой автоморфизм полей $\mathbb{R}$ и $\mathbb{C}$ оставляет поле $\mathbb{Q}$ на месте.

Упражнение 7.15. Покажите, что не существует ненулевого гомоморфизма $\mathbb{Q} \longrightarrow \mathbb{F}_p$.

§8. Ряды и многочлены.

8.1. Кольцо формальных степенных рядов. Пусть K — произвольное коммутативное кольцо с единицей. Бесконечное выражение вида

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots , \quad \text{где } a_i \in K ,$$

называется *формальным степенным рядом* от переменной x с коэффициентами из K. Первый ненулевой коэффициент a_i называется *младшим коэффициентом* ряда, а коэффициент a_0 — *свободным членом*. Два формальных степенных ряда

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \cdots \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \cdots \end{aligned} \tag{8-1}$$

равны, если $a_i = b_i$ для всех i. Ряды, у которых все коэффициенты кроме a_0 нулевые, называются *константами*.

Ряд, в котором только конечное число коэффициентов a_i отлично от нуля, называется *многочленом*. Последний ненулевой коэффициент многочлена называется его *старшим* коэффициентом. Номер старшего коэффициента называется *степенью* многочлена f и обозначается $\deg(f)$. Многочлен степени n обычно записывают как $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$.

Сумма и произведение рядов (8-1) вычисляется по обычным правилам раскрытия скобок и приведения подобных слагаемых. А именно, сумма $f(x) + g(x) = s_0 + s_1 x + s_2 x^2 + \cdots$ и произведение $f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \cdots$, по определению, имеют при x^m коэффициенты

$$s_m = a_m + b_m \quad \text{и} \quad p_m = a_0 b_m + a_1 b_{m-1} + \cdots + a_{m-1} b_1 + a_m b_0 = \sum_{i=0}^{m} a_i b_{m-i} . \tag{8-2}$$

Упражнение 8.1. Убедитесь, что формальные степенные ряды образуют коммутативное кольцо, нулём и единицей которого являются нулевая и единичная константы.

Кольцо формальных степенных рядов от переменной x с коэффициентами из K обозначается $K[[x]]$. Кольцо K вкладывается в $K[[x]]$ в качестве подкольца констант. Многочлены также образуют в $K[[x]]$ подкольцо. Оно называется *кольцом многочленов* и обозначается через $K[x]$.

Отметим, что младший коэффициент произведения рядов равен произведению младших коэффициентов сомножителей. Поэтому, если в кольце K нет делителей нуля, то их не будет и в $K[[x]]$. Для многочленов старший коэффициент произведения также будет равен произведению старших коэффициентов сомножителей, поэтому в кольце многочленов над целостным кольцом K справедливо равенство

$$\forall\, f, k \in K[x] \quad \deg(fg) = \deg(f) + \deg(g) . \tag{8-3}$$

Кольцо формальных степенных рядов $K[[x_1, x_2, \dots , x_n]]$ от нескольких переменных определяется по индукции как как кольцо формальных степенных рядов от переменной x_n с коэффициентами в кольце $K[[x_1, x_2, \dots , x_{n-1}]]$:

$$K[[x_1, x_2, \dots , x_n]] \overset{\text{def}}{=} K[[x_1, x_2, \dots , x_{n-1}]][[x_n]] .$$

Ряды от нескольких переменных представляют собою формальные бесконечные суммы вида

$$f(x_1, x_2, \dots , x_n) = \sum_{\nu_1, \dots, \nu_n \geqslant 0} a_{\nu_1 \dots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n} .$$

Отдельные слагаемые $a_{\nu_1 \dots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}$ такой суммы называются *одночленами*, а произведения $x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}$ — *мономами*. Сумма степеней $\nu_1 + \nu_2 + \cdots + \nu_n$ называется *полной степенью монома*.

8.2. Обратимые элементы колец $K[x]$ и $K[[x]]$. В этом разделе мы предполагаем, что в кольце K нет делителей нуля. В этом случае согласно формуле (8-3) никакой многочлен положительной степени не может быть обратим в $K[x]$, а обратным элементом к константе может быть только константа. Поэтому в кольце многочленов над целостным кольцом обратимыми элементами являются обратимые константы и только они. Если K — поле, то таковыми являются все ненулевые константы.

В кольце формальных степенных рядов $K[[x]]$ дело обстоит совершенно иначе.

8.2.1. ПРЕДЛОЖЕНИЕ. *Ряд $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[[x]]$ обратим в кольце $K[[x]]$ тогда и только тогда, когда его свободный член a_0 обратим в K. В частности, любой многочлен с обратимым свободным членом можно обратить в $K[[x]]$.*

Доказательство. Если существует ряд $f^{-1}(x) = b_0 + b_1x + b_2x^2 + \cdots \in K[[x]]$, такой что $f(x) \cdot f^{-1}(x) = 1$, то $a_0b_0 = 1$, т. е. $a_0 \in K$ обратим. Наоборот, допустим, что $a_0 \in K$ обратим. Приравнивая коэффициенты при одинаковых степенях x в правой и левой части равенства $f(x) \cdot f^{-1}(x) = 1$, мы получаем на коэффициенты b_i бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \cdots\cdots\cdots&\cdots\cdots \\ a_0b_\nu + a_1b_{\nu-1} + \cdots + a_\nu b_0 &= 0 \\ \cdots\cdots\cdots\cdots&\cdots\cdots\cdots \end{aligned} ,$$

из которой они все однозначно определяются по рекуррентным формулам $b_0 = 1/a_0$ и далее, для всех $k \geqslant 1$, $b_k = -(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0)/a_0$. □

8.2.2. Пример: геометрическая прогрессия. Непосредственная проверка показывает, что обратным элементом к линейному двучлену $1 - x$ является формальный ряд

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ \cdots \ = \sum_{k \geqslant 0} x^k \ , \tag{8-4}$$

который называется *геометрической прогрессией*.

Упражнение 8.2. Явно выпишите все коэффициенты рядов а) $1/(1+x)$ б) $1/(1 \pm x^m)$ в) $1/(1+x+x^2)$

8.3. Алгебраические операции над формальными рядами. Будем называть *n-арной*[1] *алгебраической операцией* над формальными рядами любое правило, сопоставляющее набору рядов $f_1, f_2, \dots, f_n$ новый ряд g, зависящий от $f_1, f_2, \dots, f_n$ так, что для вычисления каждого его коэффициента достаточно проделать конечное число операций сложения, вычитания, умножения и деления над конечным числом коэффициентов этих рядов.

Например, сложение и умножение рядов являются бинарными (двухместными) алгебраическими операциями, заданными на всём кольце $K[[x]]$, а отыскание обратного ряда — унарной (одноместной) алгебраической операцией, заданной на множестве рядов с обратимым свободным членом. Напротив, вычисление значение ряда $f(x) \in K[[x]]$ в какой-либо точке $x = \alpha \in K$ не является алгебраической операцией, если только ряд f не многочлен.

А вот подстановка в произвольный ряд $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[[x]]$ вместо x любого ряда $g(x) = b_1x + b_2x^2 + \ \cdots$ *с нулевым свободным членом* является алгебраической операцией, поскольку в результате такой подстановки получится ряд

$$f(g(x)) = \sum_{k \geqslant 0} a_\nu (b_1x + b_2x^2 + \ \cdots)^k \ \in \ K[[x]] \ ,$$

в котором на коэффициент при x^m оказывают влияние не более m начальных членов каждого из первых m слагаемых написанной суммы, и потому этот коэффициент вычисляется за конечное число сложений и умножений.

[1] или *n-местной*

8.3.1. Пример: обращение многочленов и рекуррентные уравнения. Пусть $K = \mathbb{C}$. Подставляя в формулу для геометрической прогрессии (8-4) вместо x одночлен αx с $\alpha \in \mathbb{C}$, мы получаем

$$\frac{1}{1-\alpha x} = 1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots = \sum_{k \geqslant 0} \alpha^k x^k . \tag{8-5}$$

При помощи этой формулы можно находить ряды, обратные к многочленам вида

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \prod_{i=1}^{n} (1 - \alpha_i x) , \tag{8-6}$$

где все константы $\alpha_i \in \mathbb{C}$ попарно различны. Для этого надо разложить $1/f(x)$ в сумму геометрических прогрессий:

$$\frac{1}{(1-\alpha_1 x)(1-\alpha_2 x)\cdots(1-\alpha_n x)} = \frac{\beta_1}{1-\alpha_1 x} + \frac{\beta_2}{1-\alpha_2 x} + \cdots + \frac{\beta_n}{1-\alpha_n x} . \tag{8-7}$$

Чтобы найти константы $\beta_i \in \mathbb{C}$, умножим левую и правую части (8-7) на общий знаменатель

$$1 = \sum_{i=1}^{n} \prod_{\nu \neq i} (1 - \alpha_\nu x) \cdot \beta_i$$

и подставим в это равенство $x = \alpha_i^{-1}$. Тогда все слагаемые, кроме i-того, обратятся в нуль, и мы получим

$$\beta_i = \prod_{\nu \neq i} \frac{1}{(1 - (\alpha_\nu / \alpha_i))} = \frac{\alpha_i^{n-1}}{\prod\limits_{\nu \neq i} (\alpha_i - \alpha_\nu)} .$$

Остаётся разложить каждую геометрическую прогрессию в правой части (8-7) по формуле (8-5) и сложить полученные результаты: $1/f(x) = \sum \left(\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \cdots + \beta_n \alpha_n^k\right) \cdot x^k$.

Эту технику можно применять для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \cdots + a_n z_{k-n} = 0 , \tag{8-8}$$

где коэффициенты $a_1, a_2, \dots, a_n \in \mathbb{C}$ — некоторые фиксированные заданные числа. Найдём, к примеру, явное выражение через k для *чисел Фиббоначчи* z_k, которые определяются условиями

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

и тем самым, решают линейное рекуррентное уравнение второго порядка

$$z_k - z_{k-1} - z_{k-2} = 0 .$$

Заметим, что этому же уравнению удовлетворяют при всех $k \geqslant 2$ и любом выборе чисел $b_0, b_1 \in \mathbb{C}$ коэффициенты формального степенного ряда

$$\frac{b_0 + b_1 x}{1 - x - x^2} = z_0 + z_1 x + z_2 x^2 + \cdots \tag{8-9}$$

(умножим обе части на $1 - x - x^2$ и сравним коэффициенты при x^k для $k \geqslant 2$).

Упражнение 8.3. Покажите, что для любых $b_0, b_1, \dots, b_{n-1} \in \mathbb{C}$ коэффициенты степенного ряда

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

удовлетворяют при $k \geqslant n$ общему рекуррентному уравнению (8-8).

Сравнение в (8-9) коэффициентов при x^0 и x^1 приводит к соотношениям $b_0 = z_0$ и $b_1 = z_1 - z_0$, которые показывают, что числа Фиббоначчи $z_0 = 0$, $z_1 = 1$ являются начальными коэффициентами ряда

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

получающегося из (8-9) при $b_0 = 0$, $b_1 = 1$. Чтобы явно найти все остальные коэффициенты этого ряда, представим его в виде суммы геометрических прогрессий:

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\alpha_+x)(1-\alpha_-x)} = \frac{\beta_+}{1-\alpha_+x} + \frac{\beta_-}{1-\alpha_-x}\,, \tag{8-10}$$

где числа $\alpha_\pm$, будучи корнями квадратного уравнения[1] $t^2 - t - 1 = 0$, удовлетворяют соотношениям

$$\alpha_\pm = \frac{1\pm\sqrt{5}}{2}\,, \quad \alpha_+\alpha_- = -1\,, \quad \alpha_+ + \alpha_- = 1\,,$$

при помощи которых, умножая дроби в (8-10) на общий знаменатель и подставляя $x = \alpha_\pm$, находим $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$. Таким образом,

$$z_0 + z_1x + z_2x^2 + \cdots = \frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha_+x} - \frac{1}{1-\alpha_-x}\right) = \sum_{k\geqslant 0}\frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}}\cdot x^k\,,$$

т. е. k-тое число Фиббоначчи $z_k = \dfrac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k\sqrt{5}}$.

8.4. Дифференциальное исчисление. Есть два подхода к определению производной от функции $\mathbb{R} \xrightarrow{f} \mathbb{R}$, почти дословно применимые для определения унарной *алгебраической* операции дифференцирования $f \mapsto f'$ формальных степенных рядов с коэффициентами *в произвольном* коммутативном кольце K.

Согласно аналитическому определению, производная $f'(x)$ функции $\mathbb{R} \xrightarrow{f} \mathbb{R}$ есть линейная часть приращения функции f в точке x, определяемая из формулы

$$f(x+\delta) = f(x) + f'(x)\cdot\delta + o(x,\delta)$$

в которой функция $o(x,\delta) = f(x+\delta) - f(x) - f'(x)\cdot\delta$ при $\delta \to 0$ должна стремиться к нулю быстрее, чем δ (и только при наличии такого разложения производная определена). Рассмотрим теперь произвольный степенной ряд

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[[x]] \tag{8-11}$$

и, считая символ δ второй формальной переменной, запишем $f(x+\delta) \in K[[x,\delta]]$ в виде формального степенного ряда от δ с коэффициентами из $K[[x]]$:

$$\begin{gathered} f(x+\delta) = \sum_{k\geqslant 0} a_k(x+\delta)^k = \sum_{k\geqslant 0}\sum_{\nu=1}^{k} a_k\binom{k}{\nu}x^\nu\delta^{k-\nu} = \sum_{m\geqslant 0} f_m(x)\cdot\delta^m\,, \\ \text{где}\quad f_m(x) = \sum_{k\geqslant m}\binom{k}{m}a_kx^{k-m}\quad \text{для всех } m\geqslant 0 \end{gathered} \tag{8-12}$$

Ряд $f_1(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots \in k[[x]]$, стоящий в разложении (8-12) в качестве коэффициента при δ^1, называется *производным рядом* или *производной* от ряда (8-11) и обозначается

$$f'(x) \overset{\text{def}}{=} f_1(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots = \sum_{k\geqslant 1} k\cdot a_kx^{k-1}\,. \tag{8-13}$$

[1] отметим, что при $a_0a_n \neq 0$ равенства

$$t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n = \prod_{i=1}^{n}(t-\alpha_i)$$

$$1 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n = \prod_{i=1}^{n}(1-\alpha_ix)$$

равносильны одно другому, т. к. получаются друг из друга заменой $x = 1/t$ и домнажением на общий знаменатель

Подчеркнём, что производная от многочлена является многочленом *строго меньшей степени*[1], чем исходный.

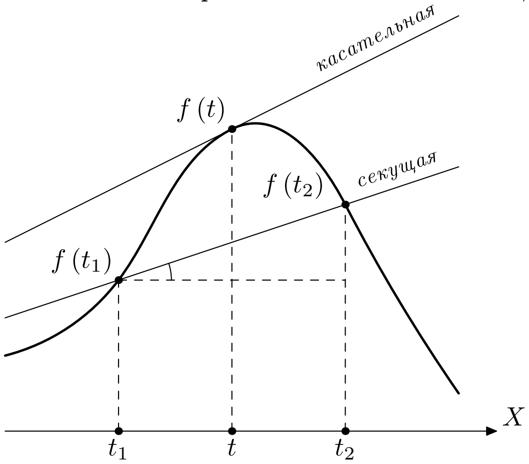


Рис. 8◇1. Касательная и секущая.

Согласно геометрическому определению, производная функции $\mathbb{R} \xrightarrow{f} \mathbb{R}$ в точке x есть наклон касательной к графику функции f в точке с абсциссой x. Касательная, в свою очередь, определяется как предел секущих, пересекающих график в точках с абсциссами t_1 и t_2, когда обе они сливаются в точку x (см. рис. 8◇1). Т. к. наклон секущей равен $\big(f(t_2) - f(t_1)\big)/(t_2 - t_1)$, производная есть предел этого выражения при $t_1, t_2 \to x$ (и определена только когда этот предел существует).

Для произвольного степенного ряда (8-11) стоящая в числителе формулы для наклона разность $f(t_2) - f(t_1)$ является элементом кольца $K[[t_1, t_2]]$ и *нацело делится* в этом кольце на $t_2 - t_1$, поскольку

$$\frac{t_2^n - t_1^n}{t_2 - t_1} = t_1^{n-1} + t_1^{n-2}t_2 + t_1^{n-3}t_2^2 + \cdots + t_1t_2^{n-2} + t_1^{n-1} ,$$

и стало быть

$$\frac{f(t_2) - f(t_1)}{t_2 - t_1} = \sum_{k\geqslant 1} a_k \big(\underbrace{t_1^{k-1} + t_1^{k-2}t_2 + t_1^{k-3}t_2^2 + \cdots + t_1t_2^{k-2} + t_2^{k-1}}_{k \text{ слагаемых}}\big) . \tag{8-14}$$

В этот ряд можно *подставить* $t_1 = t_2 = x$, в результате чего получится в точности ряд (8-13). Тем самым, «геометрическое» определение производной согласуется с «аналитическим». Отображение, сопоставляющее степенному ряду его производную, называется *дифференцированием по переменной* x и обозначается

$$\frac{\partial}{\partial x} : K[[x]] \xrightarrow{f \mapsto f'} K[[x]] . \tag{8-15}$$

8.4.1. ЛЕММА. *Для любого $a \in K$ и любых $f, g \in K[[x]]$ справедливы равенства*

$$(a)' = 0 , \quad (af)' = a \cdot f' , \quad (f+g)' = f' + g' , \quad (fg)' = f' \cdot g + f \cdot g' . \tag{8-16}$$

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

$$(f(g(x))' = g'(x) \cdot f'(g(x)) , \tag{8-17}$$

а если ряд f обратим, то $(1/f)' = -f'/f^2$.

Доказательство. Первые три равенства в (8-16) вытекают прямо из определений и формулы (8-13). Четвёртое равенство[2] в (8-16) и правило дифференцирования композиции (8-17) следуют из «аналитического» определения производной: записывая в $K[[x, \delta]]$

$$f(x+\delta) = f(x) + \delta \cdot f'(x) + (\text{члены, делящиеся на } \delta^2)$$
$$g(x+\delta) = g(x) + \delta \cdot g'(x) + (\text{члены, делящиеся на } \delta^2) ,$$

мы видим, что с точностью до мономов, делящихся на δ^2,

$$f(x+\delta)g(x+\delta) = f(x)g(x) + \delta \cdot (f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } \delta^2) ,$$

откуда $(fg)' = f' \cdot g + f \cdot g'$. Аналогично для сложной функции имеем

$$f(g(x+\delta)) = f\big(g(x) + \delta \cdot g'(x) + (\text{члены, делящиеся на } \delta^2)\big) .$$

[1] см. предупреждение (n° 8.4.2) ниже

[2] его обычно называют *правилом Лейбница*

Обозначая ряд, который прибавляется к $g(x)$ в аргументе f, через

$$\varepsilon(x,\delta) = \delta \cdot g'(x) + (\text{члены, делящиеся на } \delta^2)\ ,$$

получаем

$$\begin{aligned} f(g(x+\delta)) = f\big(g(x) + \varepsilon(x,\delta)\big) = \\ = f(g(x)) + \varepsilon(x,\delta)\cdot f'(g(x)) + (\text{члены, делящиеся на } \varepsilon(x,\delta)^2) = \\ = f(g(x)) + \delta\cdot g'(x)\cdot f'(g(x)) + (\text{члены, делящиеся на } \delta^2)\ , \end{aligned}$$

что и утверждается. Наконец, формула для $(1/f)'$ получается взятием производной от обеих частей равенства $f \cdot f^{-1} = 1$. $\square$

Упражнение 8.4. Найдите все коэффициенты степенных рядов $\dfrac{1}{(1-x)^2}, \dfrac{1}{(1-x)^3}, \ \dots\ , \dfrac{1}{(1-x)^m}$ и напишите явную формулу для k-того члена последовательности a_k, заданной рекуррентным соотношением: $a_0 = 1$, $a_1 = -1$ и $a_k = 2a_{k-1} - a_{k-2}$ при $k \geqslant 2$.

8.4.2. Предостережение: $f' = 0 \not\Rightarrow f = \mathrm{const}$! Дифференцирование является алгебраической операцией, определённой для любого кольца коэффициентов K. При работе в такой общности необходимо иметь в виду, что коэффициент k, появляющийся в равенстве (8-13) при дифференцировании каждого монома

$$(a_k x^k)' = k \cdot a_k x^{k-1}\ ,$$

и возникающий при подстановке $t_1 = t_2 = x$ в правую часть формулы (8-14), представляет собою *сумму n единиц кольца K*. Поэтому, если в кольце K сумма n единиц равна нулю (как это происходит, например, в кольце вычетов $K = \mathbb{Z}/(n)$), то производная любого одночлена, степень которого делится на n, будет нулевой:

$$\underbrace{1+1+\dots+1}_{n \text{ единиц}} = 0 \quad \Rightarrow \quad (x^{mn})' = 0 \ \ \forall\, m \in \mathbb{N}\ .$$

Например, ненулевой многочлен $x^p - 1 \in \mathbb{F}_p[x]$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$ имеет по этой причине тождественно нулевую производную.

Упражнение 8.5. Покажите, что для многочлена $f \in \mathbb{F}_p[x]$ равенство $f'(x) = 0$ равносильно тому, что $f(x) = g(x^p)$ для некоторого $g \in \mathbb{F}_p[x]$.

В дальнейшем мы ещё вернёмся к этому явлению, однако пока, до конца этого параграфа, если специально не оговаривается противное, мы будем предполагать, что кольцо коэффициентов K удовлетворяет следующему условию:

$$K \text{ *содержит в качестве подкольца поле рациональных чисел* } \mathbb{Q} \tag{8-18}$$

В этом случае сумма любого числа единиц обратима, и дифференциальное исчисление формальных рядов и многочленов с коэффициентами из K становится похоже на дифференциальное исчисление гладких функций в анализе. В частности условие $f' = 0$ равносильно тому, что $f = \mathrm{const}$. Кроме того, имеет место

8.4.3. ПРЕДЛОЖЕНИЕ (ФОРМУЛА ТЭЙЛОРА). *При выполнении условия* (8-18) *для любого ряда $f(x) \in K[[x]]$ в кольце $K[[x,\delta]]$ справедливо равенство*

$$f(x+\delta) = \sum_{m \geqslant 0} \frac{1}{m!}\, f^{(m)}(x)\cdot \delta^m$$

где $f^{(m)}(x) = \left(\frac{\partial}{\partial x}\right)^m f(x)$ есть m-тая производная от f .

Доказательство. При условии (8-18) коэффициенты $f_m(x)$ в правой части формулы (8-12), дающей разложение ряда $f(x+\delta)$ по степеням δ, переписываются согласно (8-12) в виде

$$f_m(x) = \sum_{k \geqslant m} \binom{k}{m} a_k x^{k-m} = \frac{1}{m!} \sum_{k \geqslant m} \underbrace{k(k-1)\,\cdots\,(k-m+1)}_{m \text{ сомножителей}} a_k x^{k-m} = \frac{1}{m!} f^{(m)}(x)\ ,$$

что и требуется. □

8.4.4. Первообразный ряд. Из формулы для производной (8-13) вытекает, что при выполнении условия (8-18) для любого ряда $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[[x]]$ существует единственный ряд без свободного члена

$$F(x) = \int f(x)\,dx \overset{\text{def}}{=} \sum_{k\geqslant 1} \frac{a_{k-1}}{k}\, x^k \tag{8-19}$$

такой что $F'(x) = f(x)$. Он называется *первообразным рядом* или *первообразной* от f.

8.5. Экспонента и логарифм. Для произвольного кольца K, удовлетворяющего (8-18), обозначим через

$$\mathscr{N}(K) \overset{\text{def}}{=} x\cdot K[[x]] \quad \text{и} \quad \mathscr{U}(K) \overset{\text{def}}{=} 1 + x\cdot K[[x]] \tag{8-20}$$

множества рядов с нулевым и с единичным свободным членом соответственно. Отметим, что $\mathscr{N}(K)$ является абелевой группой относительно операции сложения рядов, а $\mathscr{U}(K)$ — абелевой группой относительно умножения. Формальный степенной ряд

$$e^x \overset{\text{def}}{=} \sum_{k\geqslant 0} \frac{x^k}{k!} = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \;\cdots\; \in \mathscr{U}(\mathbb{Q}) \tag{8-21}$$

называется *экспонентой*. Он замечателен тем, что совпадает со своей производной: $(e^x)' = e^x$.

Упражнение 8.6. Убедитесь в том, что e^x — это *единственный* ряд из $\mathscr{U}(\mathbb{Q})$, обладающий таким свойством.

Подставляя в e^x вместо x любой ряд $\tau(x)$ без свободного члена, мы получаем ряд $e^{\tau(x)}$ со свободным членом 1, который называется *экспонентой* ряда $\tau(x)$. Первообразный ряд от геометрической прогрессии

$$\ln(1+x) \overset{\text{def}}{=} \int \frac{dx}{1+x} = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \;\cdots \in \mathscr{N}(\mathbb{Q}) \tag{8-22}$$

называется *логарифмом*. Для любого ряда $u(x) \in \mathscr{U}(K)$, ряд $u(X)-1$, у которого нет свободного члена, можно подставить вместо x в ряд $\ln(1+x)$. Получится ряд без свободного члена $\ln u(x)$, называемый *логарифмом* ряда $u(x)$. Таким образом, экспоненцирование и логарифмирование являются алгебраическими операциями, переводящими абелевы группы (8-20) друг в друга:

$$\begin{aligned} \exp\,:\mathscr{N}(K) &\xrightarrow{\tau\mapsto e^\tau} \mathscr{U}(K) \\ \mathscr{N}(K) &\xleftarrow[u\mapsto \ln u]{} \mathscr{U}(K)\,:\,\log \end{aligned} \tag{8-23}$$

Упражнение 8.7. Выведите из формулы (8-17) для производной от композиции, что $\forall\, u \in \mathscr{U}(K)$ выполняется тождество $(\ln u)' = u'/u$ (этот ряд называется *логарифмической производной* от u).

8.5.1. ТЕОРЕМА. *Отображения (8-23) являются взаимно обратными изоморфизмами групп, т. е. для любых рядов $u, u_1, u_2 \in \mathscr{U}(K)$, $\tau, \tau_1, \tau_2 \in \mathscr{N}(K)$ выполняются тождества:*

$$\ln e^\tau = \tau\,, \quad e^{\ln u} = u\,, \quad \ln(u_1u_2) = \ln(u_1) + \ln(u_2)\,, \quad e^{\tau_1+\tau_2} = e^{\tau_1}e^{\tau_2}\,.$$

Доказательство. Для рядов $\tau_1, \tau_2 \in \mathscr{N}(K)$ равенства $\tau_1 = \tau_2$ и $\tau_1' = \tau_2'$ равносильны друг другу. Поэтому ряды $\ln(e^x)$ и x, лежащие в $\mathscr{N}(\mathbb{Q})$ и имеющие тождественно равные единице производные, совпадают. Подставляя в равенство $\ln(e^x) = x$ вместо x произвольные ряды без свободного члена, получаем $\forall\,\tau \in \mathscr{N}(K)$ равенство $\ln e^\tau = \tau$. Для рядов $u_1, u_2 \in \mathscr{U}(K)$ соотношения $u_1 = u_2$ и $u_1' = u_2'$ также равносильны друг другу. Поэтому ряды без свободного члена $\ln(u_1u_2)$ и $\ln u_1 + \ln u_2$, также имеющие одинаковые производные:

$$(\ln(u_1u_2))' = \frac{(u_1u_2)'}{u_1u_2} = \frac{u_1'u_2 + u_1u_2'}{u_1u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = (\ln u_1)' + (\ln u_2)' = (\ln u_1 + \ln u_2)'\,,$$

тоже совпадают. Тем самым, логарифмирование $\mathscr{U}(K) \xrightarrow{\log} \mathscr{N}(K)$ является гомоморфизмом мультипликативной группы в аддитивную и обратно слева к экспоненцированию, из чего следует, что оно сюрьективно. Покажем, что оно инъективно. Для этого проверим, что следующие три равенства на ряды $u_1, u_2 \in \mathscr{U}(K)$ попарно эквивалентны:

$$u_1 = u_2 \quad\Longleftrightarrow\quad \ln(u_1) = \ln(u_2) \quad\Longleftrightarrow\quad (\ln u_1)' = (\ln u_2)' \tag{8-24}$$

Обе импликации «$\Rightarrow$» тривиальны, и достаточно вывести первое равенство из третьего, которое согласно упр. 8.7 можно переписать в виде $u_1(x)' \cdot u_2(x) = u_2'(x) \cdot u_1(x)$. Подставляя $u_1 = a_0 + a_1x + a_2x^2 + \cdots$ и $u_2 = b_0 + b_1x + b_2x^2 + \cdots$ и сравнивая коэффициенты при одинаковых степенях x получаем соотношения

$$\begin{gathered}
a_1 \cdot 1 = 1 \cdot b_1\\
2a_2 + a_1b_1 = a_1b_1 + 2b_2\\
\cdots\cdots\cdots\\
k \cdot a_k \;+\; \sum_{m=1}^{k-1} m \cdot a_m b_{k-m-1} = \sum_{m=1}^{k-1} (k-m) \cdot a_{m-1} b_{k-m} \;+\; k \cdot b_k\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{gathered}$$

из которых последовательно вытекают нужные равенства $a_k = b_k$. Таким образом, логарифмирование является изоморфизмом групп, а экспоненцирование — обратным к нему изоморфизмом. $\square$

Упражнение 8.8. Покажите, что $\forall\, u \in \mathscr{U}(K)$ $\ln(1/u) = -u$, а также проверьте равенства $e^{\tau_1+\tau_2} = e^{\tau_1}e^{\tau_2}$ и $e^{\ln u} = u$, сравнив логарифмические производные от обеих частей.

8.6. Степень с произвольным показателем. В предположении, что кольцо K обладает свойством (8-18) со стр. 59 рассмотрим для любого $\alpha \in K$ ряд

$$(1+x)^{\alpha} \overset{\text{def}}{=} e^{\alpha \ln(1+x)} \in \mathscr{U}(K)\,.$$

Он называется *биномом с показателем* α. Подставляя в бином вместо x произвольные ряды $\tau(x) = u(x) - 1$ без свободного члена, мы получаем на группе рядов с единичным свободным членом алгебраическую операцию *возведения в α-тую степень*

$$\mathscr{U}(K) \xrightarrow{u \mapsto u^{\alpha} = e^{\alpha \ln u}} \mathscr{U}(K)\,,$$

обладающую интуитивно ожидаемыми свойствами возведения в степень: для любых рядов $u, v \in \mathscr{U}(K)$ и чисел $\alpha, \beta \in K$ будут выполнены равенства

$$u^{\alpha} \cdot u^{\beta} = u^{\alpha+\beta}\,, \quad (u^{\alpha})^{\beta} = u^{\alpha\beta}\,, \quad (uv)^{\alpha} = u^{\alpha}v^{\alpha}\,. \tag{8-25}$$

Упражнение 8.9. Докажите это.

Чтобы отыскать явные значения коэффициентов бинома $(1+x)^{\alpha} = a_0 + a_1x + a_2x^2 + \cdots$, возьмём от него логарифмическую производную:

$$\frac{((1+x)^{\alpha})'}{(1+x)^{\alpha}} = \left(\ln e^{\alpha \ln(1+x)}\right)' = \big(\alpha \ln(1+x)\big)' = \frac{\alpha}{1+x}\,.$$

Получаем соотношение $((1+x)^{\alpha})' \cdot (1+x) = \alpha \cdot (1+x)^{\alpha}$. Сравнение коэффициентов при x^{k-1} в правой и левой части даёт равенства $ka_k + (k-1)a_{k-1} = \alpha a_{k-1}$, из которых

$$a_k = \frac{a_{k-1}}{k}(\alpha - k + 1) = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

(напомним, что $a_0 = 1$, поскольку $(1+x)^{\alpha} \in \mathscr{U}(\mathbb{Q})$). Как и в формуле (1-7) на стр. 6 эти числа называются *биномиальными коэффициентами* и обозначаются

$$\binom{\alpha}{k} \overset{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \in K$$

(в числителе и в знаменателе стоит по k последовательно уменьшающихся на единицу множителей, однако при $\alpha \notin \mathbb{N}$ числитель будет отличен от нуля при всех k).

8.6.1. СЛЕДСТВИЕ (ФОРМУЛА НЬЮТОНА). *Для любого коммутативного кольца K, удовлетворяющего условию (8-18) со стр. 59 в кольце $K[[x]]$, при всех $\alpha \in K$ справедливо тождество*

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

□

8.6.2. Пример: метод производящих функций. Степенной ряд $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in K[[x]]$ иногда называют *производящей функцией* для последовательности элементов $a_0, a_1, a_2, \cdots \in K$. В ситуации, когда свойства последовательности (a_ν) выражаются алгебраическими или дифференциальными уравнениями на $f(t)$, исчисление формальных степенных рядов оказывается одним из наиболее эффективных методов изучения последовательности. Проиллюстрируем это, найдя явную формулу для *чисел Каталана*, которые определяются следующим образом.

Пусть при вычислении суммы $(n+1)$ чисел $a_0 + a_1 + a_2 + \cdots + a_n$ в каждый момент времени разрешается делать не более одного сложения. Тогда такое вычисление разобьётся на n последовательных шагов, на каждом которых будет вычисляться значение некоторого конкретного сложения, в результате чего все знаки «+» окажутся занумерованными в соответствии с тем, в каком порядке они выполняются. Количество всех возникающих таким способом нумераций (или иначе, количество допустимых расстановок $n+1$ пар скобок в нашей сумме) называется n-ым *числом Каталана* c_n. Например, $c_1 = 1$, $c_2 = 2$, $c_3 = 5$, $c_4 = 14$, ...

Чтобы явно выразить c_n через n положим $c_0 = 1$ и рассмотрим производящую функцию $c(x) = \sum_{k \geqslant 0} c_k x^k$. Поскольку число таких расстановок скобок, при которых последним выполняется i-тый слева знак «+» равно $c_{i-1}c_{n-i-1}$, n-тое число Каталана c_n удовлетворяет рекуррентному соотношению

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \cdots + c_{n-2}c_1 + c_{n-1}c_0 .$$

Это соотношение означает, что $c(x) - 1 = xc(x)^2$ (написанная выше формула сравнивает коэффициенты при x^n в левой и правой части). В целостном кольце $\mathbb{Q}[[x]]$ квадратное уравнение $xt^2 - t - 1 = 0$ имеет два решения $\dfrac{1 \pm \sqrt{1-4x}}{2x}$, где $\sqrt{1-4x} = (1-4x)^{1/2} = \sum_{k \geqslant 0} \dfrac{(-1)^{k-1}}{k!} \cdot 4^k \cdot \dfrac{1}{2} \cdot \left(\dfrac{1}{2} - 1\right) \cdots \left(\dfrac{1}{2} - k + 1\right) \cdot x^k$. Поскольку $c_0 = 1$, искомая нами функция $c(x)$ получится при выборе перед радикалом знака «+». Получаем[1]

$$c(x) = \frac{1}{2x} \sum_{k \geqslant 0} \frac{(-1)^{k-1}}{k!} \cdot 4^k \cdot \underbrace{\frac{1}{2}\left(\frac{1}{2} - 1\right) \cdots \left(\frac{1}{2} - k + 1\right)}_{k} x^k =$$

$$= \sum_{k \geqslant 1} 2^{k-1} \cdot \frac{1 \cdot (2 \cdot 1 - 1) \cdot (4 \cdot 1 - 1) \cdot \cdots \cdot (2(k-1) - 1)}{k!} x^{k-1} =$$

$$= \sum_{k \geqslant 1} \frac{(2k-2)!}{k!(k-1)!} \cdot x^{k-1} = \sum_{k \geqslant 0} \binom{2k}{k} \frac{x^k}{k+1}$$

Итак, $c_n = \dfrac{1}{n+1}\dbinom{2n}{n}$. Отметим, что с первого взгляда даже не вполне понятно, почему это число является целым.

[1] при переходе от первой строки ко второй мы умножили каждый из k множителей в числителе дроби на 2, отщепив эти k двоек из 4^k, и сменили знак последних $(k-1)$ множителях; при переходе от второй строчки к третьей — домножили и числитель и знаменатель на $(k-1)!$, что вместе с 2^{k-1} дополняет числитель до полного факториала

§9. Многочлены и алгебраические числа.

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

9.1. Вычисление значения многочлена в точке. Любой многочлен $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ можно *вычислить* в любой точке $\alpha \in K$, подставив в f вместо x значение $x = \alpha$. В результате возникает *гомоморфизм вычисления*

$$\mathrm{ev}_\alpha \,:\, K[x] \xrightarrow{\mathrm{ev}_\alpha} K \,, \quad f \longmapsto f(\alpha) \overset{\text{def}}{=} a_0 + a_1\alpha + \cdots + a_n\alpha^n \in K\,. \tag{9-1}$$

Отметим, что пользуясь дистрибутивностью, $f(\alpha)$ можно вычислить за $2n$ операций сложения и умножения, не подсчитывая все степени α^k по-отдельности:

$$f(\alpha) = a_0 + \alpha \cdot \Big(a_1 + \alpha \cdot \Big(a_2 + \;\cdots\; + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n)\big) \cdots \Big)\Big)\,. \tag{9-2}$$

9.2. Деление с остатком. Многочлены $f \in K[x]$ со старшим коэффициентом единица называются *приведёнными* или *унитарными*.

9.2.1. ПРЕДЛОЖЕНИЕ. *Для любого многочлена f и любого унитарного многочлена u над произвольным кольцом K с единицей существуют* неполное частное *$q \in K[x]$ и* остаток *$r \in K[x]$, такие что:*

$$f(x) = u(x) \cdot q(x) + r(x) \quad \textit{и} \quad \deg(r) < \deg(u) \quad \textit{или} \quad r = 0\,. \tag{9-3}$$

Если кольцо K целостное, то такие q и r единственны (для данного f).

Доказательство. Существование устанавливается при помощи стандартного «деления уголком»: полагаем $r_0 = f$, $q_0 = 0$ и далее для каждого $k = 1,\,2,\,\dots$ до тех пор, пока $\deg(r_{k-1}) \geqslant \deg(u)$ строим многочлены

$$q_k(x) = (\text{старший коэффициент } r_{k-1}) \cdot x^{\deg(r_{k-1}) - \deg(u)} \quad \text{и} \quad r_k = r_{k-1} - q_k u\,,$$

степень которых с каждым шагом строго уменьшается. Когда на каком-то ℓ-том шаге мы получим $\deg(r_\ell) < \deg(u)$, равенство (9-3) будет выполняться для $r = r_\ell$ и $q = q_1 + q_2 + \cdots + q_\ell$. Если p и s — другая пара многочленов, таких что $\deg(s) < \deg(u)$ и $f = up + s$, то из $uq + r = up + s$ вытекает, что $u(q-p) = r - s$. Если в K нет делителей нуля, при $p \neq q$ будем иметь $\deg(u(q-p)) = \deg(u) + \deg(q-p) \geqslant \deg(u) > \deg(r-s)$, что противоречит равенству $u(q-p) = r - s$. Следовательно, $p - q = 0$, а значит, и $r - s = 0$. $\square$

9.2.2. СЛЕДСТВИЕ. *Для любых многочленов f, g с коэффициентами в произвольном поле $\Bbbk$ существует единственная пара многочленов $q, r \in \Bbbk[x]$, таких что в кольце $\Bbbk[x]$ выполняется равенство $f = g \cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$.*

Доказательство. Записывая g в виде $g = a \cdot u$, где $a \in \Bbbk$ — старший коэффициент многочлена g, а $u \in \Bbbk[x]$ унитарен, мы видим, что требуемое представление $f = g \cdot q + r$ равносильно представлению $f = u \cdot (aq) + r$ вида (9-3). $\square$

9.2.3. Пример: значение в точке как остаток. Остаток от деления многочлена

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \;\cdots\; + a_1x + a_0$$

на линейный двучлен $u(x) = x - \alpha$ — это константа, равная значению $f(\alpha)$ многочлена f в точке α, в чём легко убедиться, вычислив обе части равенства $f(x) = (x - \alpha) \cdot q(x) + r$ при $x = \alpha$. Поучительно, однако, увидеть это непосредственно, честно вычисляя остаток при помощи описанного выше алгоритма деления и сравнивая это вычисление с вычислением значения по формуле (9-2) со страницы 63:

$$\begin{aligned}
r_1(x) &= (a_{n-1} + \alpha a_n)x^{n-1} + a_{n-2}x^{n-2} + \;\cdots\; + a_1x + a_0 \\
r_2(x) &= \big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)x^{n-2} + a_{n-3}x^{n-3} + \;\cdots\; + a_1x + a_0 \\
r_3(x) &= \Big(a_{n-3} + \alpha\big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)\Big)x^{n-2} + a_{n-4}x^{n-4} + \;\cdots\; + a_1x + a_0 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
r_n(x) &= a_0 + \alpha \cdot \Big(a_1 + \alpha \cdot \Big(a_2 + \;\cdots\; + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n)\big) \cdots \Big)\Big) = f(\alpha)
\end{aligned} \tag{9-4}$$

Читателю настоятельно рекомендуется самостоятельно проделать это вычисление в конкретном следующем конкретном случае: разделить в $\mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ многочлен $y^n - x^n$ на линейный двучлен $(y-x)$.

Упражнение 9.1. Найдите остатки от деления многочлена $x^{179} + x^{57} + x^2 + 1$ в $\mathbb{Z}[x]$ на многочлены а) $x^2 - 1$ б) $x^2 + 1$ в) $x^2 + x + 1$.

9.2.4. Пример: нод и алгоритм Евклида. В кольце $\Bbbk[x]$ многочленов с коэффициентами в произвольном поле $\Bbbk$ у любого набора элементов $f_1, f_2, \dots, f_n$ имеется наибольший общий делитель[1], причём его можно представить в виде

$$\text{нод}(f_1, f_2, \dots, f_n) = f_1 h_1 + f_2 h_2 + \dots + f_n h_n \tag{9-5}$$

с подходящими $h_i \in \Bbbk[x]$. Доказывается это точно также, как и для целых чисел. А именно, обозначим через

$$(f_1, f_2, \dots, f_n) \overset{\text{def}}{=} \{f_1 h_1 + f_2 h_2 + \dots + f_n h_n \mid h_i \in \Bbbk[x]\} \tag{9-6}$$

множество всех многочленов, представимых в виде (9-5) с фиксированными $f_1, f_2, \dots, f_n$ и произвольными $h_1, h_2, \dots, h_n \in \Bbbk[x]$, и обозначим через $d(x) \in (f_1, f_2, \dots, f_n)$ любой ненулевой многочлен минимальной встречающейся в $(f_1, f_2, \dots, f_n)$ степени.

Упражнение 9.2. Покажите, что подмножество $(f_1, f_2, \dots, f_n) \subset \Bbbk[x]$ обладает следующими свойствами:
а) любой многочлен из $(f_1, f_2, \dots, f_n)$ делится на каждый общий делитель многочленов $f_1, f_2, \dots, f_n$
б) $f_1, f_2, \dots, f_n \in (f_1, f_2, \dots, f_n)$
в) $g_1, g_2 \in (f_1, f_2, \dots, f_n) \Rightarrow g_1 \pm g_2 \in (f_1, f_2, \dots, f_n)$
г) $g \in (f_1, f_2, \dots, f_n) \Rightarrow gh \in (f_1, f_2, \dots, f_n)\ \forall\, h \in \Bbbk[x]$
д) любой многочлен из $(f_1, f_2, \dots, f_n)$ делится на $d(x)$

Из последнего утверждения задачи вытекает, что, $(f_1, f_2, \dots, f_n) = (d)$ совпадает с множеством всех многочленов, кратных d. В частности $d = \text{нод}(f_1, f_2, \dots, f_n)$ и представляется в виде (9-5).

Отметим, что из этого вытекает, что отсутствие у пары многочленов $f, g \in \Bbbk[x]$ нетривиальных[2] общих делителей равносильна их *взаимной простоте*, т. е. возможности представления единицы кольца в виде $1 = fh_1 + gh_2$ с подходящими $h_1, h_2 \in \Bbbk[x]$.

Для практического отыскания наибольшего общего делителя и наименьшего общего кратного пары многочленов с коэффициентами в произвольном поле $\Bbbk$ применяется дословно тот же самый алгоритм Евклида, что и для целых чисел (ср. с n° 7.4). А именно, для пары многочленов $f_1(x)$ и $f_2(x)$ с $\deg(f_1) \geqslant \deg(f_2)$ положим $E_0 = f_1$, $E_1 = f_2$, и $E_k =$ остатку от деления E_{k-2} на E_{k-1} при $k \geqslant 1$. Степени многочленов E_k будут строго убывать до тех пор, пока какой-то E_r не разделит нацело предыдущий E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой многочлен E_r будет равен $\text{нод}(f_1, f_2)$, причём если при вычислении каждого E_k мы будем представлять его в виде $E_k = h_1^{(k)} f_1 + h_2^{(k)} f_2$, то $E_r = \text{нод}(f_1, f_2)$ и $E_{r+1} = 0$ тоже получатся представленными в таком виде. Отметим, что в выражении $E_{r+1} = 0 = h_1^{(r+1)} f_1 + h_2^{(r+1)} f_2$ многочлены $h_1^{(r+1)}$ и $h_2^{(r+1)}$ будут взаимно простыми множителями, дополняющими f_1 и f_2 до их наименьшего общего кратного $\text{нок}(f_1, f_2) = h_1^{(r+1)} f_1 = -h_2^{(r+1)} f_2$.

Упражнение 9.3. Докажите все эти утверждения.

Например, для $f_1 = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4$, $f_2 = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4$ первый шаг алгоритма Евклида приводит к

$$\begin{aligned}
E_0 &= x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4\\
E_1 &= x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4\\
E_2 &= -4x^4 - 13x^3 - 21x^2 - 10x - 8 = E_0 - \left(x^2 - 2x + 3\right) E_1
\end{aligned}$$

дальше удобнее делить на E_2 не E_1, а $16E_1$, а затем умножить результат на $1/16$:

$$E_3 = \frac{1}{16}\left(x^3 + 5x^2 + 10x + 8\right) = \frac{1}{16}\left(16E_1 + (4x+7)\ E_2\right) = \frac{4x+7}{16} E_0 - \frac{4x^3 - x^2 - 2x + 5}{16} E_1$$

следующий шаг уже даёт наибольший общий делитель

$$E_4 = -16\left(x^2 + 3x + 4\right) = E_2 + 16\ (4x - 7)\ E_3 = 16\left(x^2 - 3\right) E_0 - 16\left(x^4 - 2x^3 + 2x - 2\right) E_1$$

[1] напомним, что общий делитель называется *наибольшим*, если он делится на любой другой общий делитель
[2] т. е. отличных от констант и не кратных самим этим многочленам

поскольку

$$E_5 = E_3 + \frac{x+2}{256}\,E_4 = 0 = \frac{x^3+2\,x^2+x+1}{16}\,E_0 - \frac{x^5+x^2+1}{16}\,E_1 \ .$$

Таким образом,

$$\text{нод}(f_1,f_2) = x^2+3\,x+4 = -\left(x^2-3\right)\,f_1(x) + \left(x^4-2\,x^3+2\,x-2\right)\,f_2(x)$$
$$\text{нок}(f_1,f_2) = \left(x^3+2\,x^2+x+1\right)\,f_1(x) = \left(x^5+x^2+1\right)\,f_2(x)\ .$$

9.3. Разложение на множители. Напомним (см. (n° 8.2)), что обратимыми элементами кольца $K[x]$ являются в точности обратимые константы $\alpha\in K$. Отличный от обратимой константы многочлен $p\in K[x]$ называется *неприводимым*[1], если из равенства $p=fg$ вытекает, что один из сомножителей f, g является обратимой константой. В противном случае p называется *приводимым*. Если $K=\Bbbk$ является полем, то приводимость многочлена $f\in\Bbbk[x]$ означает его представимость в виде произведения $f=gh$ двух многочленов строго меньшей степени $\deg(g),\deg(h)<\deg(f)$.

9.3.1. ПРЕДЛОЖЕНИЕ. *Всякий многочлен f с коэффициентами в произвольном поле $\Bbbk$ является произведением конечного числа неприводимых многочленов, причём любые два таких представления $p_1p_2\cdots p_k=f=q_1q_2\cdots q_m$ имеют одинаковое число сомножителей $k=m$, и эти сомножители можно перенумеровать так, чтобы $\forall\ i\ p_i=s_iq_i$, где $s_i\in\Bbbk$ — некоторые константы.*

Доказательство. Годятся дословно те же аргументы, что и для целых чисел (ср. с n° 7.8.1). Первое утверждение очевидно: если f неприводим, то он сам и будет своим разложением, если f приводим, то он является произведением 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, мы в конце концов получим требуемое разложение. Для доказательства его единственности рассмотрим равенство

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m\ , \tag{9-7}$$

в котором все сомножители неприводимы. Поскольку p_1 неприводим, он делится только на константы и на многочлены вида $s\cdot p_1$ с $s\in\Bbbk$. Если таких многочленов среди q_i нет, то $\forall\ i$ $\text{нод}(p_1,q_i)=1$, а значит p_1 взаимно прост с каждым из q_i, а следовательно, и с их произведением. Но равенство $h_1p_1+h_2q_1\cdots q_m=1$ невозможно, поскольку его левая часть в силу (9-7) делится на p_1. Итак, один из q_i — назовём его q_1 — имеет вид $q_1=s_1p_1$ с $s_1\in\Bbbk$. Тогда (9-7) можно переписать в виде $p_1(p_2\cdots p_k+s_1\cdot q_2\cdots q_m)=0$, откуда следует более короткое равенство $p_2p_3\cdots p_k=(s_1q_2)q_3\cdots q_m$ (в котором s_1q_2 тоже неприводим), к которому применимо то же рассуждение. □

9.4. Корни многочленов. Элемент $\alpha\in K$, называется *корнем* многочлена $f\in K[x]$, если $f(\alpha)=0$. Как мы видели в примере (n° 9.2.3), это условие равносильно тому, что $f(x)$ делится в $K[x]$ на $(x-\alpha)$.

9.4.1. ПРЕДЛОЖЕНИЕ. *Если в K нет делителей нуля, то всякий многочлен $f\in K[x]$, имеющий несколько попарно различных корней $\alpha_1,\alpha_2,\dots,\alpha_s\in K$, делится в $K[x]$ на произведение*

$$\prod_{i=1}^{s}(x-\alpha_i)\ .$$

В частности, если $f\neq 0$, то $\deg(f)\geqslant s$.

Доказательство. Запишем f в виде $f(x)=(x-\alpha_1)\cdot f_1(x)$. Поскольку в K нет делителей нуля и $(\alpha_i-\alpha_1)\neq 0$ при $i\neq 1$, вычисляя обе части при $x=\alpha_2,\alpha_3,\dots,\alpha_s$, мы заключаем, что $\alpha_2,\alpha_3,\dots,\alpha_s$ являются корнями многочлена $f_1(x)$, и можем применить к ним то же самое рассуждение. □

9.4.2. СЛЕДСТВИЕ. *Ненулевой многочлен f с коэффициентами из целостного кольца не может иметь в этом кольце более $\deg(f)$ различных корней.* □

[1] ср. с общим определением неприводимости из (n° 7.8)

9.4.3. СЛЕДСТВИЕ. *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. Многочлен $f - g$ нулевой, поскольку имеет степень $\leqslant n$ и больше, чем n корней. □

9.4.4. Пример: общие корни нескольких многочленов. Пусть $\Bbbk$ — поле. Число α тогда и только тогда является общим корнем нескольких многочленов $f_1, f_2, \dots, f_m \in \Bbbk[x]$, когда α является корнем их наибольшего общего делителя. В самом деле, если $(x-\alpha)$ делит каждый из f_i, то $(x-\alpha)$ делит $\text{нод}(f_1, f_2, \dots, f_m)$, и наоборот. Таким образом, отыскание общих корней набора многочленов — это отыскание корней их наибольшего общего делителя, что часто бывает проще, чем отыскание корней любого из f_i в отдельности, т.к. $\deg \text{нод}(f_1, f_2, \dots, f_m)$ обычно бывает меньше $\min\bigl(\deg(f_i)\bigr)$.

В частности, если $\text{нод}(f_1, f_2, \dots, f_m) = 1$, то у многочленов f_i нет общих корней, причём не только в поле $\Bbbk$, над которым заданы эти многочлены, но и ни в каком большем кольце $K \supset \Bbbk$. Действительно, $f_i(\alpha)$ никак не могут одновременно обратиться в нуль, поскольку $\exists\, h_1, h_2, \dots, h_m \in \Bbbk[x]$, такие что

$$f_1 h_1 + f_2 h_2 + \dots + f_m h_m = \text{нод}(f_1, f_2, \dots, f_m) = 1$$

никогда не обращается в нуль.

9.4.5. Пример: кратные корни. Корень $\alpha \in K$ многочлена $f \in K[x]$ называется *кратным*, если $f(x)$ делится в $K[x]$ на $(x-\alpha)^2$. В этом случае $f(x) = (x-\alpha)^2 g(x)$ для некоторого $g \in K[x]$, и стало быть, $f'(x) = (x-a)\,(2g(x) - (x-\alpha)g'(x))$ делится на $(x-\alpha)$. Таким образом, все кратные корни многочлена f являются общими корнями f и f', а значит, являются корнями $\text{нод}(f, f')$.

Пусть $K = \mathbb{Q}$. В этом случае производная f' любого многочлена $f \in \mathbb{C}[x]$ положительной степени является ненулевым многочленом степени $\deg(f') = \deg(f) - 1$, а условие взаимной простоты f и f' можно поверять при помощи алгоритма Евклида в пределах кольца $\mathbb{Q}[x]$. В частности, если f неприводим в $\mathbb{Q}[x]$, то он будет взаимно прост с f'. Согласно предыдущему примеру, f и f' в этом случае не будут иметь общих корней не только в $\mathbb{Q}$, но и ни в каком большем поле $K \supset \mathbb{Q}$, к примеру, в поле комплексных чисел. Таким образом, неприводимый многочлен $f \in \mathbb{Q}[x]$ не может иметь кратных комплексных корней.

Назовём *кратностью* корня $\alpha \in \mathbb{C}$ многочлена $f \in \mathbb{C}[x]$ такое число $m \in \mathbb{N}$, что $f(x) = (x-\alpha)^m \cdot g(x)$, где $g(\alpha) \neq 0$. Всякий m-кратный корень α многочлена f является $(m-1)$-кратным корнем его производной, поскольку

$$f'(x) = (x-\alpha)^{m-1} \cdot (m + (x-\alpha) \cdot g(x)) \ ,$$

и значение второго сомножителя в точке α отлично от нуля. Таким образом, $\alpha \in \mathbb{C}$ тогда и только тогда является m-кратным корнем многочлена $f \in \mathbb{C}[x]$, когда $f(\alpha) = f'(\alpha) = \dots = f^{(m-1)}(\alpha) = 0$, но $f^{(m)}(\alpha) \neq 0$ (ср. с (n° 8.4.3)).

Упражнение 9.4. Пусть $\Bbbk$ — поле. Проверьте, что многочлен второй степени неприводим в $\Bbbk[x]$ тогда и только тогда, когда у него нет корней в поле $\Bbbk$

9.5. Кольца вычетов $\Bbbk[x]/(f)$, где $\Bbbk$ — поле, определяются аналогично кольцам $\mathbb{Z}/(n)$. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$, обозначим через

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

множество всех многочленов, делящихся на f и рассмотрим смежные классы

$$[g]_f = g \pmod f = g + (f) \stackrel{\text{def}}{=} \{g + fh \mid h \in \Bbbk[x]\} \ . \tag{9-8}$$

Два многочлена g_1 и g_2 лежат в одном и том же смежном классе $[g_1]_f = [g_2]_f$, если и только если разность $g_1 - g_2$ делится на f.

Упражнение 9.5. Убедитесь, что любые два смежных класса $[g_1]_f$, $[g_2]_f$ либо не пересекаются, либо совпадают.

Сложение и умножение смежных классов задаётся теми же самыми формулами (7-1), что и сложение целочисленных вычетов:

$$[g] + [h] \stackrel{\text{def}}{=} [g+h] \ , \quad [g] \cdot [h] \stackrel{\text{def}}{=} [gh] \ . \tag{9-9}$$

Упражнение 9.6. Проверьте корректность этого определения (т. е. независимость классов $[g+h]$ и $[gh]$ от выбора представителей $g \in [g]$ и $h \in [h]$), а также выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулевым элементом кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей является класс $[1]_f = 1 + (f)$. Поскольку никакая константа не может делиться на многочлен положительной степени, классы всех констант $c \in \Bbbk$ будут различны. Иначе говоря, поле $\Bbbk$ *вкладывается* в кольцо $\Bbbk[x]/(f)$ в качестве классов констант, и далее мы будем писать c вместо $[c]_f$ для $c \in \Bbbk$.

Упражнение 9.7. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Поскольку любой многочлен $g \in \Bbbk[x]$ единственным образом записывается в виде $g = fh + r$, где $\deg(r) < \deg(f)$, в каждом классе $[g]_f$ имеется единственный представитель $r \in [g]_f$ степени $\deg(r) < \deg(f)$. Таким образом, каждый класс *единственным образом* записывается в виде

$$[a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}\,, \quad \text{где } \vartheta = [x]_f\,, \text{ а } a_i \in \Bbbk\,.$$

Заметим, что класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, т. к. $f(\vartheta) = f([x]_f) = [f(x)]_f = [0]_f$. Таким образом, сложение и умножение классов по правилам (9-9) можно интерпретировать как формальное сложение и умножение записей

$$a_0 + a_1\vartheta + \ \cdots \ + a_{n-1}\vartheta^{n-1}\,, \tag{9-10}$$

по стандартным правилам раскрытия скобок и приведения подобных, но с учётом того, что символ ϑ удовлетворяет соотношению $f(\vartheta) = 0$. Поэтому кольцо $\Bbbk[x]/(f)$ иначе обозначают через $\Bbbk[\vartheta] : f(\vartheta) = 0$ и называют *расширением* поля $\Bbbk$ при помощи *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$. Выражения (9-10) в таком контексте называются (обобщёнными[1]) *алгебраическими числами*.

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

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a+c) + (b+d)\sqrt{2}\\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2\,bd) + (cb + ad)\sqrt{2}\end{aligned}$$

Упражнение 9.8. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых ϑ удовлетворяет соотношению: а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$?

9.5.1. Пример: «алгебраическое» определение комплексных чисел. Поле комплексных чисел можно *определить* как расширение поля $\mathbb{R}$ при помощи корня квадратного уравнения $x^2 + 1 = 0$, т. е. как кольцо

$$\mathbb{R}[x]/(x^2+1) = \mathbb{R}\left[\sqrt{-1}\right] : \left(\sqrt{-1}\right)^2 = -1\,,$$

состоящее из чисел вида $a + b\sqrt{-1}$, где $a, b \in \mathbb{R}$, а символ $\sqrt{-1}$ обозначает класс одночлена x по модулю (x^2+1). Сложение и умножение таких чисел происходит по правилам

$$\begin{aligned}(a + b\sqrt{-1}) + (c + d\sqrt{-1}) &= (a+c) + (b+d)\sqrt{-1}\\ (a + b\sqrt{-1})(c + d\sqrt{-1}) &= (ac - bd) + (cb + ad)\sqrt{-1}\,.\end{aligned}$$

Кольцо $\mathbb{R}\left[\sqrt{-1}\right]$ является полем, поскольку каждый ненулевой класс $a + b\sqrt{-1}$ обладает обратным

$$\frac{1}{a + b\sqrt{-1}} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\sqrt{-1}\,.$$

[1] *алгебраическим числом* в классическом смысле называется элемент поля $\mathbb{Q}[x]/(f)$, где $f \in \mathbb{Q}[x]$ — неприводимый многочлен (см. предложение (n° 9.5.2) ниже); наша обобщённая трактовка отличается от классической тем, что во-первых, вместо $\mathbb{Q}$ разрешается произвольное поле $\Bbbk$, а во-вторых, не требуется, чтобы соотношение на ϑ было неприводимо

Отображение $\mathbb{R}\left[\sqrt{-1}\right] \xrightarrow{\gamma} \mathbb{C}$ из этого поля в поле комплексных чисел $\mathbb{C}$, определённое в §6, сопоставляющее числу $a+b\sqrt{-1} \in \mathbb{R}\left[\sqrt{-1}\right]$ вектор $\gamma\left(a+b\sqrt{-1}\right) = a+bi \in \mathbb{C}$, является изоморфизмом полей.

9.5.2. ПРЕДЛОЖЕНИЕ. *Кольцо $\Bbbk[x]/(f)$ является полем тогда и только тогда, когда многочлен f неприводим в $\Bbbk[x]$.*

Доказательство. Если $f = gh$, где оба многочлена f, g имеют строго меньшую, чем f, степень, то ненулевые классы $[g],[h]$ будут делителями нуля в $\Bbbk[x]/(f)$, что невозможно в поле. Если же f неприводим, то он будет взаимно прост с любым многочленом $g \notin (f)$, т.е. для некоторых $h, q \in \Bbbk[x]$ будет выполняться равенство $fh + gq = 1$, и стало быть $[q]\cdot[g] = [1]$ в $\Bbbk[x]/(f)$, т.е. любой ненулевой класс $[g]_f \in \Bbbk[x]/(f)$ будет обратим. □

Упражнение 9.9. Напишите явную формулу для вычисления обратного элемента
а) к числу $a_0 + a_1\vartheta$ в поле $\mathbb{Q}[\vartheta] : \vartheta^2 + \vartheta + 1 = 0$;
б) к числу $a_0 + a_1\vartheta + a_2\vartheta^2$ в поле $\mathbb{Q}[\vartheta] : \vartheta^3 + \vartheta^2 + \vartheta + 1 = 0$.

9.5.3. ПРЕДЛОЖЕНИЕ (КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ). *Пусть $\Bbbk$ — произвольное поле, и многочлен $f \in \Bbbk[x]$ является произведением m попарно взаимно простых сомножителей: $f = f_1 f_2 \cdots f_m$. Отображение*

$$\Bbbk[x]/(f) \xrightarrow{\varphi} (\Bbbk[x]/(f_1)) \times (\Bbbk[x]/(f_2)) \times \cdots \times (\Bbbk[x]/(f_m)) ,$$

переводящее класс $[g]_f \in \Bbbk[x]/(f)$ в набор классов $\varphi([g]_f) \stackrel{\text{def}}{=} ([g]_{f_1}, [g]_{f_2}, \ldots, [g]_{f_m})$, является корректно определённым изоморфизмом колец.

Доказательство. Корректность определения φ (независимость $\varphi([g]_f)$ от выбора представителя $g \in \Bbbk[x]$ в классе $[g]_f \subset \Bbbk[x]$) и то, что φ переводит суммы и произведения, соответственно, в суммы и произведения, проверяется дословно так же, как в примере (n° 7.6.1).

Упражнение 9.10. Обязательно выполните все эти проверки.

Также, как в (n° 7.6.1), проверим, что φ, рассматриваемый как гомоморфизм аддитивных групп, имеет нулевое ядро: если $\forall\ i\ [g]_{f_i} = 0$, то g делится на каждое f_i, а в силу их попарной взаимно просты — и на произведение $f_1 f_2 \cdots f_m = f$, откуда $[g]_f = 0$. Следовательно, по теореме о строении гомоморфизма групп, φ является вложением. Сюрьективность φ устанавливается явным построением для заданного набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f)$ такого многочлена $g \in \Bbbk[x]$, что $g \equiv r_i \pmod{f_i}$ сразу для всех i. Как и в (n° 7.6.1), для каждого i обозначим через

$$F_i = \prod_{\nu \neq i} f_\nu$$

произведение всех сомножителей f_ν кроме f_i и построим многочлен

$$g_i = F_i \cdot h_i \equiv 1 \pmod{f_i} .$$

В качестве h_i в этой формуле можно взять любой многочлен[1], класс которого по модулю f_i обратен классу $F_i \pmod{f_i}$ (который взаимно прост с f_i и потому обратим). Тогда

$$\varphi(g_i) = \left([0]_{f_1}, \ldots, [0]_{f_{i-1}}, [1]_{f_i}, [0]_{f_{i+1}}, \ldots, [0]_{f_m}\right) ,$$

и в качестве многочлена g, отображающегося в заданные классы $[r_i]_{f_i}$ при всех i, можно взять $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m$. □

9.5.4. Пример: разложение рациональных функций на простейшие дроби. Пусть $\Bbbk$ — произвольное поле. Поле частных (см. n° 7.10) целостного кольца $\Bbbk[x]$ обозначается $\Bbbk(x)$ и называется *полем рациональных функций*. Рассуждение, использованное нами в доказательстве китайской теоремы об остатках, показывает, что любая несократимую дробь $f(x)/g(x) \in \Bbbk(x)$, знаменатель которой является произведением взаимно простых многочленов $g(x) = g_1(x)g_2(x)\ldots g_m(x)$, *единственным образом* записывается в виде суммы

$$\frac{f(x)}{g(x)} = h(x) + \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} + \cdots + \frac{f_m(x)}{g_m(x)} , \tag{9-11}$$

[1] чтобы найти его явно, можно, например, взять остаток R_i от деления F_i на f_i и применить к паре $E_0 = f_i$, $E_1 = R_i$ алгоритм Евклида, что даст на выходе представление $1 = \text{нод}(F_i, f_i) = \text{нод}(R_i, f_i)$ в виде $1 = R_i h_i + f_i \tilde{h}_i$, из которого вытекает, что класс $[h_i]_{f_i} = [R_i]_{f_i}^{-1} = [F_i]_{f_i}^{-1}$ обладает нужным свойством

в которой $\deg h = \deg f - \deg g$ и $\deg f_i < \deg g_i$. В самом деле, домножая обе части (9-11) на g, получаем в $\Bbbk[x]$ равенство

$$f = hg + f_1Q_1 + f_2Q_2 + \cdots + f_mQ_m \ , \quad \text{где } Q_i = \prod_{\nu\neq i} g_\nu \quad \text{и} \quad \deg(\textstyle\sum f_\nu Q_\nu) < \deg Q \ , \tag{9-12}$$

из которого многочлены h и $r = \sum f_\nu Q_\nu$ однозначно определяются как неполное частное и остаток от деления f на g, а каждый из f_i — как единственный многочлен степени $< \deg g_i$, представляющий в $\Bbbk[x]/(g_i)$ класс $r^{-1} \pmod{g_i} \equiv f\,Q_i^{-1} \pmod{g_i}$.

Если разложить знаменатель в произведение: $g = q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s}$, где все q_i неприводимы и попарно различны, и взять $g_i = q_i^{m_i}$, то сумму (9-11) разложить и дальше, записав числитель f_i каждой из дробей $f_i/q_i^{m_i}$ в q_i-ической позиционной системе счисления, т. е. представить его в виде[1]

$$p = \sum_{\nu=1}^{d} p_\nu q^\nu \ , \quad \text{где } \deg(p_\nu) < \deg(q) \ .$$

Упражнение 9.11. Убедитесь, что такое представление существует и единственно (решение можно подглядеть в сноске ([2])).

В результате мы получим представление рациональной функции f/g в виде суммы многочлена степени $\deg f - \deg g$ и *простейших дробей* вида p/q^m, где q пробегает множество неприводимых делителей знаменателя, m меняется от 1 до кратности вхождения q в разложение знаменателя, и $\deg p < \deg q$, причём такое представление будет *единственным*. Это представление часто бывает полезно при дифференцировании и интегрировании и рациальных функций, а также при их разложении в степенные ряды (мы уже пользовались им в примере (n° 8.3.1)).

Упражнение 9.12. Найдите первообразную и 2005-ю производную от $x^4/(1+x^2)$.

Указание. Согласно предыдущему, $x^4/(x^2+1) = x^2 + \alpha/(x+i) + \beta/(x-i)$; для отыскания $\alpha, \beta \in \mathbb{C}$ умножьте обе части на общий знаменатель и подставьте $x = \pm i$.

9.6. Конечные поля $\mathbb{F}_p[\vartheta]$. Если в конструкции из n° 9.5 взять в качестве $\Bbbk$ конечное поле $\mathbb{F}_p = \mathbb{Z}/(p)$ из p элементов, а в качестве $f \in \mathbb{F}_p[x]$ неприводимый многочлен степени n, то кольцо алгебраических чисел $\mathbb{F}_p[x]/(f)$ будет конечным полем, состоящим из p^n элементов вида $a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}$ со всевозможными $a_i \in \mathbb{F}_p$. Например, $x^2 + x + 1 \in \mathbb{F}_2[x]$ неприводим согласно упр. 9.4, т. к. у него нет корней в $\mathbb{F}_2$. Поле $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \mathbb{F}_2[\omega]$, где $\omega^2+\omega+1 = 0$ состоит из четырёх элементов: $0\,,\ 1\,,\ \omega = x \pmod{(x^2+x+1)}$ и $1 + \omega = \omega^2 = \omega^{-1}$ (обратите внимание, что в следствие равенства $-1 = 1$ в поле $\mathbb{F}_2$ можно обходиться без «минусов»).

Упражнение 9.13. Решите в поле $\mathbb{F}_4$ уравнение $x^2 + x + 1 = 0$.

Отметим, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

Точно также, $x^2 + 1 \in \mathbb{F}_3[x]$ не имеет корней в $\mathbb{F}_3$, и значит, неприводим. Соответствующее поле $\mathbb{F}_9 = \mathbb{F}_3\left[\sqrt{-1}\right]$ состоит из девяти элементов $a + b\sqrt{-1}$ где $a, b \in \{-1, 0, 1\} = \mathbb{F}_3$.

Упражнение 9.14. Составьте для поля $\mathbb{F}_9$ таблицу умножения, таблицу обратных элементов, таблицу квадратов и таблицу кубов. Изоморфна ли мультипликативная группа $\mathbb{F}_9^*$ циклической группе $\mathbb{Z}/(8)$?

На самом деле, для каждого $n \in \mathbb{N}$ и любого простого $p \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$, состоящее из $q = p^n$ элементов, и всякое конечное поле изоморфно одному из этих полей $\mathbb{F}_q$. Этот факт (а также неприводимые многочлены над полями $\mathbb{F}_p$) обсуждается в задачах из (необязательного) листка $6\frac{1}{2}$. Здесь же мы ограничимся всего одним результатом в этом направлении — покажем, что мультипликативная группа конечного поля, состоящего из q элементов является циклической группой порядка $q - 1$ (и тем самым, зависит только от q). Это следует из следующего более общего предложения.

9.6.1. ПРЕДЛОЖЕНИЕ. *Любая конечная подгруппа в мультипликативной группе произвольного поля $\Bbbk$ является циклической.*

---

[1] то же самое верно и для натуральных чисел: всякое $p < q^k$ единственным образом представляется в виде $\sum\limits_{\nu=1}^{d} p_\nu / q^\nu$ с $p_\nu < q$; мы постоянно пользуемся этим в повседневной жизни, полагая $q = 10$

[2] РЕШЕНИЕ: p_0 есть остаток от деления p на q, разность $p - a_0$ делится на q, и p_1 есть остаток от деления $(p - a_0)/q$ на q, и т. д.

Доказательство. Пусть подгруппа $G \subset \Bbbk^*$ состоит из n элементов. Обозначим через m максимальный из порядков элементов группы G. Мы должны показать, что $m \geqslant n$. Для этого достаточно убедиться, что порядок любого элемента группы G является делителем числа m. В самом деле, если это верно, то все n элементов группы G будут корнями многочлена $x^m - 1 = 0$, откуда и следует нужное неравенство.

Чтобы доказать, что порядки всех элементов группы являются делителями максимального порядка, достаточно для любых двух элементов $b_1, b_2 \in G$, имеющих порядки m_1, m_2, построить элемент $b \in G$, порядок которого равен $\text{нок}(m_1, m_2)$.

Упражнение 9.15. Покажите, что при $\text{нод}(m_1, m_2) = 1$ в качестве такого элемента подойдёт $b = b_1 b_2$.

Если m_1 и m_2 не взаимно просты, то, раскладывая их в произведение простых чисел, мы можем представить $\text{нок}(m_1, m_2)$ в виде произведения $\ell_1 \ell_2$ так, что[1] $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ и $\text{нод}(\ell_1, \ell_2) = 1$. Тогда элементы $b_1' = b_1^{k_1}$ и $b_2' = b_2^{k_2}$ будут иметь взаимно простые порядки ℓ_1 и ℓ_2, а их произведение $b_1' b_2'$ по упр. 9.15 будет иметь порядок $\ell_1 \ell_2 = \text{нок}(n_1, n_2)$. □

9.6.2. Пример: квадратичные вычеты. Зафиксируем целое простое $p > 2$. Ненулевые элементы поля $\mathbb{F}_p$, которые являются квадратами, называются *квадратичными вычетами* по модулю p. Иными словами, квадратичные вычеты составляют образ отображения возведения в квадрат $\mathbb{F}_p^* \xrightarrow{x \mapsto x^2} \mathbb{F}_p^*$. Поскольку это отображение является гомоморфизмом мультипликативных групп, и его ядро состоит из двух элементов[2] ± 1, квадратичных вычетов имеется ровно $(p-1)/2$ и они образуют в $\mathbb{F}_p^*$ мультипликативную подгруппу индекса 2.

Судить о том, является ли данный элемент $a \in \mathbb{F}_p^*$ квадратом или нет, можно при помощи малой теоремы Ферма. А именно, если $a = b^2$, то $a^{\frac{p-1}{2}} = b^{p-1} = 1$. Возведение в $\frac{p-1}{2}$-тую степень

$$\mathbb{F}_p^* \xrightarrow{x \mapsto x^{\frac{p-1}{2}}} \mathbb{F}_p^* \tag{9-13}$$

также является гомоморфизмом мультипликативных групп, причём его образ содержится среди корней всё того же уравнения $x^2 = 1$. Отметим, что -1 лежит в этом образе, поскольку $\mathbb{F}_p^*$ — это циклическая группа, и при $p > 2$ в ней есть элемент порядка $(p-1) > (p-1)/2$. Следовательно, ядро гомоморфизма (9-13) совпадает с подгруппой квадратичных вычетов, и $a \in \mathbb{F}_p^*$ является квадратом тогда и только тогда, когда $a^{\frac{p-1}{2}} = 1$ (для $p = 2$ это, формально, тоже так).

Например, -1 является квадратом в $\mathbb{F}_p$ в точности тогда, когда $(p-1)/2$ чётно.

Вместо того, чтобы вычислять $a^{\frac{p-1}{2}}$, можно воспользоваться следующим соображением, восходящим к Гауссу. Запишем элементы поля $\mathbb{F}_p$ в виде

$$-(p-1)/2\,,\ \dots\,,\ -1\,,\ 0\,,\ 1\,,\ \dots\,,\ (p-1)/2 \tag{9-14}$$

и умножим все «положительные» числа на a. Произведение всех полученных чисел будет отличаться от произведения всех «положительных» чисел в точности на множитель $a^{\frac{p-1}{2}}$. С другой стороны, каждое из произведений ac будет числом вида $\pm b$, где b «положительно», причём для каждого b ровно одно из чисел $\pm b$ будет представлено среди этих произведений, поскольку равенство $ab = \pm ac$ возможно только при $b = \pm c$. Таким образом, произведение всех чисел ac, где c «положительно», будет отличаться от произведения всех c знаком, равным $(-1)^s$, где s — количество «положительных» чисел, ставших после умножения на a «отрицательными». Таким образом, a является квадратичным вычетом тогда и только тогда, когда при умножении на a меняет знак чётное число «положительных» элементов записи (9-14).

Например, 2 является квадратичным вычетом по модулю p, если и только если $p \equiv \pm 1 \pmod 8$.

Упражнение 9.16. Покажите, что $a^{\frac{p-1}{2}}$ равно знаку перестановки элементов поля $\mathbb{F}_p$, происходящей при их умножении на a.

В задачах упражнений (дополнительный листок $5\frac{1}{2}$) доказывается *квадратичный закон взаимности* Гаусса, который позволяет выяснить, является ли заданное a квадратичным вычетом по модулю p, примерно за столько же действий, за сколько отыскивается $\text{нод}(a, p)$.

[1] в ℓ_1 надо отправить все простые делители m_1, которые входят в m_1 в бóльшей степени, чем в m_2, причём взять их нужно ровно с теми степенями, которые они имеют в m_1

[2] ибо уравнение $x^2 = 1$ имеет в любом целостном кольце с единицей ровно два корня

§10. Фактор кольца и идеалы.

10.1. Идеалы. Подмножество I коммутативного кольца K называется *идеалом*, если оно удовлетворяет следующим двум условиям:

$$a_1, a_2 \in I \quad \Rightarrow \quad a_1 \pm a_2 \in I \tag{10-1}$$

$$a \in I \quad \Rightarrow \quad \forall\, b \in K \;\; ab \in I \tag{10-2}$$

Первое условие означает, что идеал является аддитивной подгруппой в кольце, второе — что вместе с каждым элементом идеал содержит и все кратные ему элементы. В (n° 6.5) мы видели, что этими свойствами обладает ядро любого гомоморфизма $K \xrightarrow{\varphi} K'$, так что ядра гомоморфизмов являются идеалами. Примерами идеалов являются подмножества вида

$$(a) = \{ka \mid k \in K\}\,, \tag{10-3}$$

состоящие из всех элементов, кратных фиксированному элементу $a \in K$. Идеалы вида (10-3) называются *главными*. Мы встречались с ними при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов

$$\mathbb{Z} \xrightarrow{m \mapsto [m]_n} \mathbb{Z}/(n)\;, \quad \Bbbk[x] \xrightarrow{g \mapsto [g]_f} \Bbbk[x]/(f)$$

сопоставляющих целому числу (соотв. многочлену) класс его вычета.

Более общим образом, для любого набора элементов $a_1, a_2, \dots, a_m \in K$ множество всех элементов, представимых в виде $k_1a_1 + k_2a_2 + \dots + k_ma_m$ с произвольными $k_1, k_2, \dots, k_m \in K$

$$(a_1, a_2, \dots, a_m) \stackrel{\text{def}}{=} \{k_1a_1 + k_2a_2 + \dots + k_ma_m \mid k_1, k_2, \dots, k_m \in K\} \tag{10-4}$$

тоже является идеалом. Он называется *идеалом, порождённым* $a_1, a_2, \dots, a_m$. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Отметим, что в любом кольце K имеются *тривиальные* идеалы $(0) = \{0\}$ и $(1) = K$.

Упражнение 10.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей попарно равносильны: а) $I = K$ б) $1 \in I$ в) I содержит какой-нибудь обратимый элемент.

10.1.1. ПРЕДЛОЖЕНИЕ. *Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.*

Доказательство. Если K поле, $I \subset K$ — идеал, и $b \in I$ отличен от нуля, то $1 = b^{-1}b \in I$, и значит $I = K$, поскольку $\forall\, b \in K \;\; b = 1 \cdot b \in I$ по свойству (10-2). Наоборот, тривиальность главного идеала $(b) = \{bc \mid c \in K\}$ означает, что либо $b = 0$, либо $(b) \ni 1$. В последнем случае $bc = 1$ для некоторого c, т. е. b обратим. Тем самым, если все главные идеалы тривиальны, то все ненулевые элементы обратимы. □

10.2. Факторизация. Пусть произвольное коммутативное кольцо K разбито в объединение непустых непересекающихся подмножеств:

$$K = \bigsqcup_{x \in X} K_x\,, \tag{10-5}$$

занумерованных элементами некоторого множества X. Иначе можно сказать, что имеется сюрьективное отображение множеств

$$K \xrightarrow{x} X\,, \tag{10-6}$$

сопоставляющее каждому элементу $a \in K$ номер $x(a)$ того подмножества разбиения (10-5), где лежит a. Для каждого $a \in K$ обозначим через $[a] = X_{x(a)} \subset K$ множество всех элементов, имеющих тот же номер, что и a, и будем называть его *классом элемента* a. Мы хотим задать на множестве X сложение и умножение, согласованные со сложением и умножением в кольце K, т. е. определить их формулами

$$x(a) + x(b) = x(a+b)\ , \quad x(a)\cdot x(b) = x(ab)\ .$$

Это то же самое, что задать сложение и умножение классов разбиения (10-5) формулами

$$[a] + [b] = [a+b]\ , \quad [a]\cdot[b] = [ab]\ . \tag{10-7}$$

Покажем, что эти формулы тогда и только тогда корректно наделяют множество X структурой коммутативного кольца, когда класс $[0] \subset K$ является идеалом в K, а все остальные классы представляют собой смежные классы по модулю этого идеала, т. е.

$$\forall\, a\in K \ \ [a] = a + I = \{a + i \mid i \in I\} = \{b \in A \mid b - a \in I\}\ .$$

В самом деле, пусть $[0]$ — идеал в K и равенство классов $[a_1] = [a_2]$ означает, что $a_2 - a_1 \in [0]$. Тогда формулы (10-7) корректно задают операции над классами, т. е. при $[a_1] = [a_2]$ и $[b_1] = [b_2]$ мы получим $[a_1 + b_1] = [a_2 + b_2]$ и $[a_1 b_1] = [a_2 b_2]$. Действительно, если $a_2 = a_1 + \alpha$ и $b_2 = b_1 + \beta$, где $\alpha, \beta \in [0]$, то $a_2 + b_2 = a_1 + b_1 + (\alpha + \beta)$ и $a_2 + b_2 = a_1 b_1 + (\alpha b_1 + \beta a_1 + \alpha\beta)$, где заключённые в скобки члены лежат в $[0]$, поскольку $[0]$ идеал. Выполнение аксиом коммутативного кольца в K автоматически влечёт их выполнение в X. Например, дистрибутивность проверяется выкладкой

$$[a]\cdot([b] + [c]) = [a]\cdot[b+c] = [a(b+c)] = [ab + bc] = [ab] + [bc] = [a]\cdot[b] + [a]\cdot[c]\,.$$

Упражнение 10.2. Проверьте аналогичным образом выполнение всех остальных аксиом.

Наоборот, если формулы (10-7) корректно задают на X структуру кольца, то отображение (10-6) является гомоморфизмом колец с ядром $\ker(x) = [0]$. Следовательно $[0] = \ker(x)$ — идеал в K, и любой класс $[a] = x^{-1}(x(a))$ является смежным классом ядра.

10.2.1. Определение фактор кольца. Множество аддитивных смежных классов идеала $I \subset K$ со структурой кольца, заданной формулами (10-7), обозначается K/I и называется *фактор кольцом* кольца K по идеалу I.

10.2.2. Строение гомоморфизма. Из предыдущего следует, что образ любого гомоморфизма коммутативных колец $K_1 \xrightarrow{\varphi} K_2$ изоморфен фактор кольцу $K_1/\ker(\varphi)$, а сам гомоморфизм раскладывается в композицию вложения $K_1/\ker(\varphi) \simeq \mathrm{im}\,(\varphi) \xhookrightarrow{\varphi'} K_2$ и эпиморфизма факторизации $K_1 \overset{\varphi''}{\twoheadrightarrow} K_1/\ker(\varphi) \simeq \mathrm{im}\,(\varphi)$, т. е. мы имеем коммутативную диаграмму

$$\begin{tikzcd} K_1 \arrow[rr, "\varphi"] \arrow[dr, "\varphi''"'] & & K_2 \\ & K_1/\ker(\varphi) \simeq \mathrm{im}\,(f) \arrow[ur, hook, "\varphi'"'] & \end{tikzcd} \tag{10-8}$$

аналогичную (5-9).

10.2.3. Пример: редукция целочисленных многочленов по модулю n. Рассмотрим в кольце $\mathbb{Z}[x]$ главный идеал (n), где $n \neq 1$ — целая константа. Этот идеал состоит из многочленов, все коэффициенты которых делятся на n. Фактор кольцо $\mathbb{Z}[x]/(n)$ изоморфно кольцу $\big(\mathbb{Z}/(n)\big)[x]$ многочленов с коэффициентами в кольце вычетов $\mathbb{Z}/(n)$. В самом деле, отображение

$$\begin{gathered} \varrho_n : \mathbb{Z}[x] \xrightarrow{f \mapsto [f]_n} \big(\mathbb{Z}/(n)\big)[x]\ , \quad \text{где} \\ \left[a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0\right]_n \overset{\text{def}}{=} [a_m]_n\, x^m + [a_{m-1}]_n\, x^{m-1} + \cdots + [a_1]_n\, x + [a_0]_n\ , \end{gathered} \tag{10-9}$$

является сюрьективным гомоморфизмом колец с $\ker(\varrho_n) = (n)$.

Гомоморфизм (10-9) называется *редукцией по модулю* n. Он часто бывает полезен для доказательства неприводимости того или иного многочлена $f \in \mathbb{Z}[x]$. Ход мысли при этом таков: если $f = gh$ в

$\mathbb{Z}[x]$, то во всех кольцах $\big(\mathbb{Z}/(n)\big)[x]$ выполняется равенство $[f]_n = [g]_n \cdot [h]_n$. Если $n = p$ — простое, то кольцо $\mathbb{Z}/(n) = \mathbb{F}_p$ является полем, в частности, в $\mathbb{F}_p[x]$ имеется однозначное разложение на неприводимые множители. Более того, все потенциальные неприводимые делители любого многочлена $[f]_p$, в принципе, можно перебрать, ибо над $\mathbb{F}_p$ есть лишь конечное число многочленов заданной степени.

Упражнение 10.3. Перечислите все неприводимые многочлены степени $\leqslant 3$ в $\mathbb{F}_2[x]$ и в $\mathbb{F}_3[x]$.

Например, чтобы убедиться в неприводимости многочлена $f(x) = x^5 + x^2 + 1$ в кольце $\mathbb{Z}[x]$, достаточно рассмотреть его редукцию по модулю 2. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$, а т. к. у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Тогда $x^5 + x^2 + 1$, согласно упр. 10.3, должен делиться в $\mathbb{F}_2[x]$ на $x^2 + x + 1$, что не так.

Ещё один пример: покажем, что многочлен деления круга на простое число частей

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}\,, \quad \text{где } p \text{ простое}\,,$$

неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от новой переменной $t = x - 1$:

$$f(t) = \frac{(t+1)^p - 1}{t} = t^p + \binom{p}{1} t^{p-1} + \cdots + \binom{p}{p-1} t\,.$$

При редукции по модулю p от многочлена $f(t)$ остаётся только старший моном $[f(t)]_p = t^n$. Если $f(t) = g(t)h(t)$ в $\mathbb{Z}[t]$, то $[g(t)]_p[h(t)]_p = t^n$ в $\mathbb{F}_p[t]$, откуда вытекает[1], что g и h тоже редуцируются по модулю p в свои старшие мономы: $[g(x)]_p = x^m$, $[h(x)]_p = x^k$, где $m = \deg(g)$, $k = \deg(h)$. Тем самым, все коэффициенты g, h, кроме старшего, делятся на p. Но тогда младший коэффициент f, будучи произведением младших коэффициентов g, h, должен делиться на p^2, что не так. Следовательно, f неприводим.

Упражнение 10.4 (критерий Эйзенштейна). Пусть все 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. Покажите, что f неприводим в $\mathbb{Z}[x]$.

10.3. Кольца главных идеалов. Целостное кольцо K с единицей называется *кольцом главных идеалов*, если каждый идеал $I \subset K$ является *главным*, т. е. имеет вид $I = (d) = \{ad \mid a \in K\}$.

Параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, который мы наблюдали в предыдущих двух параграфах, объясняется тем, что оба этих кольца являются кольцами главных идеалов. Доказательство этого факта основано на возможности деления с остатком, и фактически было дано нами в (n° 7.7) и (n° 9.2.4), когда мы обсуждали свойства наибольших общих делителей. Сейчас мы воспроизведём его ещё раз таким образом, чтобы оно годилось для любого кольца, допускающего «деление с остатком» в следующем точном смысле.

10.3.1. Евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если существует функция

$$K \setminus \{0\} \xrightarrow{\ \nu\ } \mathbb{N} \cup \{0\}\,,$$

сопоставляющая каждому ненулевому элементу $a \in K$ целое неотрицательное число $\nu(a)$, которое называется *евклидовой нормой* (или *высотой*) элемента a так, что $\forall\, a, b \in K \setminus \{0\}$ выполняются следующие два свойства:

$$\nu(ab) \geqslant \nu(a) \tag{10-10}$$

$$\exists\, q, r \in K\ :\ a = bq + r \ \text{ и либо } \nu(r) < \nu(b)\,, \text{ либо } r = 0\,. \tag{10-11}$$

Так, в кольце целых чисел $\mathbb{Z}$ функцией высоты является абсолютная величина, а в кольце многочленов $\Bbbk[x]$ с коэффициентами в поле $\Bbbk$ высотой служит степень многочлена.

Упражнение 10.5. Покажите, что кольца

а) $\mathbb{Z}[i] \overset{\text{def}}{=} \{\, a + bi \in \mid a, b \in \mathbb{Z}\,,\ i^2 = -1\}$

б) $\mathbb{Z}[\omega] \overset{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}\,,\ \omega^2 + \omega + 1 = 0\,\}$

являются евклидовыми относительно высоты $\nu(z) = |z|^2$.

[1]здесь мы используем единственность разложения на неприводимые множители в кольце $\mathbb{F}_p[x]$

Элементы q и r, о которых идёт речь во втором свойстве (10-10), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Упражнение 10.6. Покажите, что в любом евклидовом кольце равенство $\nu(ab) = \nu(a)$ в свойстве (10-10) равносильно тому, что элемент b обратим (решение можно подглядеть в сноске ([1])).

Покажем, что в любом евклидовом кольце K всякий идеал $I \subset K$ является главным. Выберем в I какой-нибудь ненулевой элемент $d \in I$ наименьшей высоты. Тогда всякий элемент $a \in I$ делится на d. Действительно, деля a на d с остатком, получаем $a = dq + r$, где $r = a - dq \in I$, поскольку $a, d \in I$. При этом либо $\nu(r) < \nu(d)$, что невозможно по выбору d, либо $r = 0$, что и утверждается. Таким образом, $I \subset (d)$. Так как $d \in I$, мы имеем равенство $I = (d)$.

Итак, все евклидовы кольца являются кольцами главных идеалов[2]. В частности, кольцами главных идеалов являются $\mathbb{Z}$, $\Bbbk[x]$, где $\Bbbk$ — поле, а также кольца $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ из упр. 10.5.

10.3.2. НОД и взаимная простота. Любой набор элементов $a_1, a_2, \dots, a_n$ произвольного кольца главных идеалов K имеет наибольший общий делитель $d = \text{нод}(a_1, a_2, \dots, a_n)$, который можно представить в виде $d = x_1a_1 + x_2a_2 + \dots + x_na_n$. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным:

$$(a_1, a_2, \dots, a_n) = \{x_1a_1 + x_2a_2 + \dots + x_na_n \mid x_i \in K\} = (d) \ .$$

В самом деле, образующая d, как и все элементы $(a_1, a_2, \dots, a_n)$, имеет вид $d = \sum x_\nu a_\nu$, и значит, делится на любой общий делитель чисел a_i. С другой стороны, все элементы $(a_1, a_2, \dots, a_n) = (d)$, включая сами a_i, делятся на d.

Из наличия представления $\text{нод}(a_1, a_2, \dots, a_n) = x_1a_1 + x_2a_2 + \dots + x_na_n$ вытекает, что в любом кольце главных идеалов отсутствие у элементов $a_1, a_2, \dots, a_n$ необратимых общих делителей влечёт за собой их взаимную простоту[3], т. е. возможность представить единицу кольца в виде

$$1 = x_1a_1 + x_2a_2 + \dots + x_na_n \quad \text{с некоторыми } x_i \in K \ .$$

Упражнение 10.7. Покажите, что если элементы $a_1, a_2, \dots, a_m$ кольца главных идеалов K таковы, что $\forall\, i \neq j$ $\text{нод}(a_i, a_j) = 1$, то $K/(a_1 \cdot a_2 \cdot \dots \cdot a_m) \simeq (K/(a_1)) \times (K/(a_2)) \times \cdots (K/(a_m))$.

10.3.3. ПРЕДЛОЖЕНИЕ. *В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:*

(1) *$K/(p)$ является полем;*

(2) *в $K/(p)$ нет делителей нуля;*

(3) *p неприводим, т. е. $p = ab \Rightarrow a$ или b обратим в K .*

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была доказана нами для любого поля в (n° 7.2). Покажем, что в любом целостном кольце K (не обязательно являющемся кольцом главных идеалов) имеет место импликация (2) $\Rightarrow$ (3). Из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и если в $K/(p)$ нет делителей нуля, то один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, и значит, $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим. Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Если p неприводим, то $\forall\, b \notin (p)$ $\text{нод}(p, b) = 1$, а значит, $\exists\, x, y \in K : px + by = 1$, откуда $[b][y] = 1$ в $K/(p)$. Тем самым, любой класс $[b] \neq [0]$ обратим в $K/(p)$, т. е. $K/(p)$ — поле. □

10.3.4. Однозначность разложения на неприводимые множители. Целостное кольцо называется *факториальным*, если каждый его необратимый элемент a является произведением конечного числа неприводимых элементов $a = p_1p_2 \cdots p_m$, причём любое другое такое разложение

[1] решение: 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

[2] отметим, что обратное неверно, но контрпримеры приходят из достаточно глубокой теории чисел и алгебраической геометрии, так что для их полноценного понимания требуется техника, которой мы пока ещё не владеем; впрочем, заинтересовавшийся читатель может обратиться к замечанию 3 на стр. 365 книги Э. Б. Винберга «*Курс алгебры*» (цит. по изданию М. «Факториал» (1999))

[3] иначе взаимную простоту $a_1, a_2, \dots, a_n$ можно охарактеризовать как равенство $(a_1, a_2, \dots, a_n) = K$

$a = q_1 q_2 \cdots q_k$ состоит из того числа сомножителей $k = m$, и после надлежащей перенумерации каждый q_ν будет ассоциирован[1] с p_ν.

Упражнение 10.8. Покажите, что в произвольном кольце главных идеалов K любые два неприводимых элемента p, q либо взаимно просты (т. е. $px + qy = 1$ для некоторых $x, y \in K$), либо ассоциированы (т. е. $p = qs$ для некоторого обратимого $s \in K$).

10.3.5. ПРЕДЛОЖЕНИЕ. *Всякое кольцо главных идеалов факториально.*

Доказательство. Докажем сначала существование разложения произвольного элемента a в произведение конечного числа неприводимых множителей. Если a неприводим, то доказывать нечего. Если нет, запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Этот процесс не кончится через конечное число шагов построением требуемого разложения, только если в K существует бесконечная последовательность элементов $\{a_i\}$, в которой a_{i+1} делит a_i, но a_i не делит a_{i+1}, т. е. $(a_i) \subsetneq (a_{i+1})$.

Упражнение 10.9. Убедитесь, что для любой цепочки вложенных идеалов $\cdots \subset I_\nu \subset I_{\nu+1} \subset \cdots$ произвольного коммутативного кольца объединение $I = \bigcup\limits_\nu I_\nu$ также является идеалом.

Поскольку все идеалы в K главные, $\bigcup\limits_\nu (a_\nu) = (d)$ для некоторого $d \in \bigcup\limits_\nu (a_\nu)$. Коль скоро d лежит в объединении, $\exists\, i : d \in (a_i)$. А тогда $(d) = \bigcup\limits_\nu (a_\nu) = (a_i)$. В частности, $\forall\, k > 0\ (a_{i+k}) = (a_i)$ вопреки предположению о том, что $(a_i) \subsetneq (a_{i+1})$. Тем самым, процесс разложения не может продолжаться бесконечно.

Докажем теперь единственность разложения. Пусть мы имеем равенство $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, в котором все множители неприводимы. Заметим, что p_i не может быть взаимно прост с каждым из q_i, поскольку в этом случае он будет взаимно прост и с их произведением (см. n° 7.6), т. е. найдутся $x, y \in K : 1 = xp_1 + yq_1 q_2 \cdots q_m = xp_1 + yp_1 p_2 \cdots p_k = p_1(x + yp_2 \cdots p_k)$, что невозможно, поскольку p_1 необратим. Тем самым, в правой части существует множитель, скажем q_1, который не взаимно прост с p_1, а значит (см. упр. 10.8) $q_1 = sp_1$ для некоторого обратимого $s \in K$. Тогда $p_1(p_2 \cdots p_k - sq_2 \cdots q_m) = 0$, откуда следует более короткое равенство $p_2 p_3 \cdots p_k = (sq_2) q_3 \cdots q_m$, к которому применимо предыдущее рассуждение. □

10.3.6. Некоторые предостережения. Разумеется, не все кольца являются кольцами главных идеалов. Например, идеалы $(2, x) \subset \mathbb{Z}[x]$ и $(x, y) \subset \mathbb{Q}[x, y]$ не являются главными.

Упражнение 10.10. Докажите это.

Через некоторое время мы покажем, что кольца $\mathbb{Z}[x]$ и $\mathbb{Q}[x, y]$ факториальны. Таким образом, факториальность является существенно более слабым ограничением на кольцо, чем свойство быть кольцом главных идеалов.

Пример нефакториального целостного кольца доставляет кольцо алгебраических чисел

$$\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)\ ,$$

в котором есть такие два различных разложения на неприводимые множители:

$$2 \cdot 2 = \left(\sqrt{5} + 1\right) \cdot \left(\sqrt{5} - 1\right)\ .$$

Упражнение 10.11. Докажите, что 2, $\sqrt{5} + 1$, $\sqrt{5} - 1$ неприводимы и попарно неассоциированы.

10.3.7. Пример: простые и неприводимые элементы. Ключевым местом в доказательстве единственности разложения из предложения (n° 10.3.5) была такая импликация: если произведение $q_1 q_2 \cdots q_m$ делится на p_1, то хотя бы один из сомножителей делится на p_1.

Необратимый элемент p произвольного целостного кольца K называется *простым*, если для любых $a, b \in K$ из того, что произведение ab делится на p, вытекает, что a или b делится на p. Иначе можно сказать, что простота элемента p означает, что в кольце $K/(p)$ нет делителей нуля.

В доказательстве предложения (n° 10.3.3) мы видели, что в любом целостном кольце все простые элементы автоматически неприводимы. Мы видели также, что в кольце главных идеалов справедливо и обратное: всякий неприводимый элемент прост. Именно в этом и заключается причина факториальности колец главных идеалов.

[1] т. е. $q_\nu = s_\nu \cdot p_\nu$ для некоторых обратимых $s_\nu \in K$, см. (n° 7.7)

Упражнение 10.12. Пусть в целостном кольце K всякий элемент является произведением конечного числа неприводимых. Покажите, что K факториально тогда и только тогда, когда все неприводимые элементы в K просты.

Для общего целостного кольца K простота является строго более сильным свойством, чем неприводимость. Так, в уже упоминавшемся выше кольце алгебраических чисел $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ число 2 неприводимо, но не просто, поскольку в фактор кольце

$$\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2,x^2-5) \simeq \mathbb{Z}[x]/(2,x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$$

имеется очевидный делитель нуля $(x+1) \pmod{(2,x^2+1)}$. На языке алгебраических чисел это означает, что $\sqrt{5}+1$ не делится на 2 в $\mathbb{Z}[\sqrt{5}]$, а $(\sqrt{5}+1)^2 = 6+2\sqrt{5}$ — делится, хотя двойка при этом неприводима.

10.3.8. Пример: гауссовы целые числа (продолжение примера n° 6.4.1). Согласно упр. 10.5, кольцо гауссовых чисел $\mathbb{Z}[i] \subset \mathbb{C}$ является кольцом главных идеалов, а потому в нём справедлива теорема об однозначности разложения на неприводимые множители. Выясним, какие целые простые числа $p \in \mathbb{Z}$ остаются неприводимыми в кольце гауссовых чисел. Для этого заметим, что разложение любого целого вещественного $n \in \mathbb{Z}$, будучи инвариантным относительно комплексного сопряжения, должно вместе с каждым неприводимым множителем $a+ib \in \mathbb{C} \smallsetminus \mathbb{R}$ содержать и сопряжённый ему множитель $a-ib$. В частности, если простое $p \in \mathbb{Z}$ перестаёт быть неприводимым в $\mathbb{Z}[i]$, то оно представляется в виде $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a,b \in \mathbb{Z}$. Таким образом, простое $p \in \mathbb{Z}$ тогда и только тогда приводимо в $\mathbb{Z}[i]$, когда p является суммой двух квадратов. Чтобы явно описать все такие p, вспомним, что неприводимость $p \in \mathbb{Z}[i]$ равносильна тому, что фактор кольцо $\mathbb{Z}[i]/(p)$ является полем[1], и посмотрим на это фактор кольцо как на фактор кольца многочленов $\mathbb{Z}[x]$ по идеалу $(p,x^2+1) \subset \mathbb{Z}[x]$, порождённому элементами p и (x^2+1):

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p,x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)\ .$$

Самое правое кольцо является полем тогда и только тогда, когда многочлен x^2+1 неприводим над $\mathbb{F}_p$, что равносильно отсутствию у него корней в $\mathbb{F}_p$. Таким образом, простое $p \in \mathbb{Z}$ является суммой двух квадратов, если и только если -1 квадратичный вычет по модулю p. Как мы видели в примере (n° 9.6.2), это происходит в точности тогда, когда $(p-1)/2$ чётно, т. е. для простых $p = 4k+1$ и $p = 2$.

10.3.9. Пример: взаимно простые идеалы. Два идеала I, J произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если существуют $x \in I$ и $y \in J$, такие что $x+y = 1$. Это условие равносильно тому, что идеал $I+J \overset{\text{def}}{=} (I,J) = \{x+y \mid x \in I\ ,\ y \in J\}$, порождённый их объединением и состоящий из всевозможных сумм, совпадает со всем кольцом. Свойства взаимно простых идеалов обобщают свойства взаимно простых чисел.

10.3.10. ЛЕММА. *Если идеал I взаимно прост с каждым из идеалов $J_1, J_2, \dots, J_n$, то он взаимно прост и с их пересечением*[2].

Доказательство. Для каждого $\nu = 1,\,2,\,\dots\,,n$ мы имеем элементы $x_\nu \in I$ и $y_\nu \in J_\nu$, такие что $x_\nu + y_\nu = 1$. Перемножая все эти эти равенства и раскрывая скобки, мы получим равенство вида

$$(\text{члены, содержащие множитель вида } x_\nu) + y_1 y_2\ \cdots\ y_n = 1\ ,$$

в котором первое слагаемое лежит в I, а второе — в $\bigcap\limits_\nu J_\nu$. □

10.3.11. ПРЕДЛОЖЕНИЕ (КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ). *Пусть идеалы $I_1, I_2, \dots, I_n$ произвольного коммутативного кольца K с единицей попарно взаимно просты. Тогда для любого набора из n классов $[a_\nu] \in K/I_\nu$ (где $\nu = 1,\,2,\,\dots\,,n$) существует $a \in K$, такое что $[a_\nu] = a \pmod{I_\nu}$ одновременно для всех ν, причём для любого другого $a' \in K$, обладающего этим свойством, мы будем иметь $a'-a \in \bigcap\limits_\nu I_\nu$. Иными словами, имеется канонический изоморфизм колец*

$$K/\bigcap_\nu I_\nu \xrightarrow[\sim]{a \mapsto (a \,(\mathrm{mod}\, I_1),\, a\,(\mathrm{mod}\, I_2),\,\dots\,,\, a\,(\mathrm{mod}\, I_n))} (K/I_1) \times (K/I_2) \times\ \cdots\ \times (K/I_n)\ . \qquad (10\text{-}12)$$

Доказательство. Отображение $K \xrightarrow[\sim]{a \mapsto (a \,(\mathrm{mod}\, I_1),\, a\,(\mathrm{mod}\, I_2),\,\dots\,,\, a\,(\mathrm{mod}\, I_n))} (K/I_1) \times (K/I_2) \times\ \cdots\ \times (K/I_n)$ является гомоморфизмом колец с ядром $\bigcap\limits_\nu I_\nu$. Поэтому нам достаточно доказать его сюрьективность. По

[1] см. предложение (n° 10.3.3)

[2] убедитесь, что пересечение идеалов тоже является идеалом

предыдущей лемме I_k взаимно прост с $\bigcap\limits_{\nu\neq k} I_\nu$ для каждого k. Поэтому найдутся $x_k \in I_k$ и $y_k \in \bigcap\limits_{\nu\neq k} I_\nu$, такие что $x_k + y_k = 1$. Это означает, что

$$y_k \,(\operatorname{mod} I_\nu) = \begin{cases} 0\,, & \text{при } \nu \neq k \\ 1\,, & \text{при } \nu = k \end{cases}$$

и в качестве элемента $a \in K$, отображающегося в произвольно заданный набор классов $[a_k] \in K/I_k$, мы можем взять $a = \sum\limits_{k=1}^{n} y_k a_k$. □

Упражнение 10.13. Выведите из предложения (n° 10.3.11) предыдущие версии китайской теоремы об остатках, доказанные в (n° 7.6.1) и (n° 9.5.3).

10.4. Характеристика. Для любого кольца с единицей K имеется канонический гомоморфизм

$$\mathbb{Z} \xrightarrow{\varkappa} K\,,$$

переводящий единицу в единицу и действующий на произвольное целое число по правилу

$$\varkappa(\pm n) = \pm(\underbrace{1 + 1 + \cdots + 1}_{n}) \quad \text{для } \; n \in \mathbb{N}\,.$$

Если $\varkappa$ инъективен, то говорят, что K имеет *характеристику нуль*, в противном случае *характеристикой* называют наименьшее натуральное число p, для которого

$$\underbrace{1 + 1 + \cdots + 1}_{p} = 0\,.$$

Иначе это можно сказать так: поскольку в $\mathbb{Z}$ все идеалы главные, $\ker(\varkappa) = (p)$ для некоторого целого неотрицательного p, которое и называется *характеристикой* кольца K. Характеристика обозначается $\operatorname{char}(K)$. Если кольцо K целостное, то его подкольцо $\mathbb{Z}/(p) \simeq \operatorname{im}(\varkappa) \subset K$ также не будет иметь делителей нуля. Таким образом, характеристика целостного кольца или равна нулю или является простым числом.

Упражнение 10.14. Докажите это непосредственно, пользуясь равенством

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

10.4.1. Простое подполе. Пусть $\Bbbk$ — поле. Наименьшее по включению подполе в $\Bbbk$, содержащее 1 и 0, называется *простым подполем* в $\Bbbk$. Простое подполе, таким образом, содержит $\operatorname{im}(\varkappa)$.

Если $\operatorname{char}(\Bbbk) = p > 0$, то $\operatorname{im}(\varkappa) \simeq \mathbb{F}_p$ и будет простым подполем поля $\Bbbk$.

Если $\operatorname{char}(\Bbbk) = 0$, т. е. $\varkappa(q) \neq 0$ при $q \neq 0$, то гомоморфизм $\varkappa$ можно продолжить до (автоматически инъективного по n° 6.5.1) гомоморфизма полей

$$\varkappa : \mathbb{Q} \xhookrightarrow{\frac{p}{q} \mapsto \frac{\varkappa(p)}{\varkappa(q)}} \Bbbk\,.$$

Следовательно, в этом случае простое подполе в $\Bbbk$ изоморфно полю рациональных чисел $\mathbb{Q}$.

Таким образом, всякое поле является либо расширением поля $\mathbb{Q}$, либо расширением одного из полей $\mathbb{F}_p$ с простым $p \in \mathbb{N}$, причём никаких ненулевых гомоморфизмов между полями разных характеристик нет.

10.4.2. Гомоморфизм Фробениуса. Если $\operatorname{char}(\Bbbk) = p > 0$, тоже самое вычисление, что и в (n° 7.9), показывает, что

$$\forall\, a, b \in \Bbbk \quad (a+b)^p = a^p + \sum_{k=1}^{p-1} (\underbrace{1 + 1 + \cdots + 1}_{\binom{p}{k}}) a^k b^{p-k} + b^p = a^p + b^p\,.$$

Тем самым, отображение возведения в p-тую степень $F_p : \Bbbk \xrightarrow{x \mapsto x^p} \Bbbk$ является гомоморфизмом из поля $\Bbbk$ в себя. Он называется *гомоморфизмом Фробениуса*. Согласно малой теореме Ферма[1] гомоморфизм Фробениуса тождественно действует на простом подполе $\mathbb{F}_p \subset \Bbbk$. Например, для $\Bbbk = \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$ гомоморфизм Фробениуса $\mathbb{F}_4 \xrightarrow{F_2} \mathbb{F}_4$ является автоморфизмом, аналогичным комплексному сопряжению: он тождественно действует на подполе $\mathbb{F}_2 = \{0, 1\}$ и переводит друг в друга элементы $\omega = [x]$ и ω^2, являющиеся корнями многочлена $x^2 + x + 1$.

Упражнение 10.15. Опишите действие Фробениуса F_3 на поле $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$.

10.5. Кольца функций. Пусть K — коммутативное кольцо, а X — произвольное множество. Множество всех функций $X \longrightarrow K$ обозначается K^X и образует кольцо относительно операций поточечного сложения и умножения значений функций:

$$f + g : x \mapsto f(x) + g(x) \qquad fg : x \mapsto f(x)g(x) \ .$$

Тождественно нулевая функция является в K^X нулём, а тождественно единичная (если в K есть единица) — единицей.

Иначе K^X можно воспринимать как *прямое произведение*[2] одинаковых копий кольца K, занумерованных элементами $x \in X$. Если множество X состоит из n элементов, то вместо K^X обычно пишут K^n и изображают элементы такого кольца строчками[3] $(a_1, a_2, \dots, a_n)$.

Поскольку произведение любых двух функций с непересекающимися носителями[4] равно нулю, в кольце K^X много делителей нуля, даже если K — поле. Обратимыми элементами K^X являются функции, принимающие обратимое значение в каждой точке.

10.5.1. Гомоморфизмы подъёма. С каждым отображением множеств $X \xrightarrow{\varphi} Y$ связан гомоморфизм *подъёма*[5] вдоль φ

$$\varphi^* \ : \ K^Y \xrightarrow{f \mapsto f \circ \varphi} K^X \ ,$$

который переводит функции на Y в их композиции с φ, являющиеся функциями на X, и тем самым, действует в противоположном к φ направлении. На языке некоммутативной алгебры подъём есть не что иное, как правое умножение всех отображений из $\operatorname{Hom}(Y, K)$ на отображение $\varphi \in \operatorname{Hom}(X, Y)$:

$$\operatorname{Hom}(Y, K) \xrightarrow{f \mapsto f\varphi} \operatorname{Hom}(X, K)$$

Отметим, что хотя кольца функций и не целостные, гомоморфизм подъёма всегда переводит единицу кольца K^Y в единицу кольца K^X.

Упражнение 10.16. Из каких функций состоит ядро гомоморфизма подъёма?

В геометрии и анализе множества X и Y обычно наделяются той или иной дополнительной структурой: мерой, топологией, локальными координатами и т. п. Соответственно и функции рассматриваются не любые, а согласованные с этой структурой: интегрируемые, непрерывные, гладкие и т. п. Такие специальные функции образуют в кольце всех функций подкольцо, которое в алгебре принято обозначать $K[X] \subset K^X$ и называть *структурным кольцом* (или *кольцом регулярных функций*) соответствующей теории.

Отображения между множествами с дополнительной структурой тоже рассматриваются не произвольные, а согласованные с этой структурой: скажем, непрерывные или дифференцируемые. В алгебре такие отображения тоже называются *регулярными*. Как только зафиксирована теория, т. е. в кольце функций каждого рассматриваемого в этой теории множества X выделено подкольцо регулярных функций $K[X]$, так регулярные отображения между множествами

[1] см. (n° 7.9) и (n° 7.3.2)

[2] см. (n° 7.5)

[3] напомним (см. n° 7.5), что сложение и умножение таких строк производится покомпонентно

[4] напомним, что *носителем* функции $X \xrightarrow{f} K$ называется множество $\operatorname{Supp}(f) = \{x \in X \mid f(x) \neq 0\}$.

[5] по-английски он называется *pull back homomorphism*; по-русски подъёмы тоже иногда называют *обратными образами*, и их ни в коем случае не следует путать с *прообразами*

теории обычно становится возможным определить чисто алгебраически, а именно, как такие отображения $X \xrightarrow{\varphi} Y$, подъём вдоль переводит регулярные функции на Y в регулярные функции на X, т. е. корректно определяет гомоморфизмом подколец $K[Y] \xrightarrow{\varphi^*} K[X]$.

Упражнение 10.17* (для тех, кто знаком с непрерывностью). Обозначим кольцо непрерывных функций $[0,1] \longrightarrow \mathbb{R}$ через $C \subset \mathbb{R}^{[0,1]}$. Покажите, что

а) отображение $[0,1] \xrightarrow{\varphi} [0,1]$ непрерывно тогда и только тогда, когда $\varphi^*(C) \subset C$;

б) для непрерывного φ инъективность гомоморфизма $C \xrightarrow{\varphi^*} C$ равносильна сюръективности φ.

10.5.2. Гомоморфизмы вычисления. В случае, когда $X = \{*\}$ состоит из одной точки, гомоморфизм поднятия, отвечающий её вложению $\{*\} \overset{y}{\hookrightarrow} Y$ в какое-нибудь множество Y в качестве некой точки $y \in Y$, переводит функцию $f \in Y^K$ в число $f(y) \in K^{\{*\}} = K$, и тем самым, представляет собою *гомоморфизм вычисления*[1] значений функций на Y в точке $y \in Y$:

$$\mathrm{ev}_y \;:\; K^Y \xrightarrow{f \mapsto f(y)} K$$

Этот гомоморфизм эпиморфен, а его ядро состоит из всех функций, которые обращающихся в нуль в точке y.

Используя гомоморфизмы вычисления, можно для любого абстрактно заданного кольца с единицей R, содержащего основное кольцо K в качестве подкольца, построить множество $X[R]$, для которого R можно будет естественным образом отождествить с некоторым подкольцом в $K^{X[R]}$ и, тем самым, рассматривать как «кольцо регулярных функций» некоторой «геометрической теории». А именно, назовём *K-точкой* кольца R произвольный гомоморфизм $R \xrightarrow{p} K$, тождественно действующий на подкольце $K \subset R$, и возьмём в качестве $X[R]$ множество всех K-точек кольца R. Каждый элемент $f \in R$ может восприниматься как функция на $X[R] \xrightarrow{f} K$, значение которой на K-точке $R \xrightarrow{p} K$, по определению, равно $p(f) \in K$. Подкольцо $K \subset R$ при этом превращается в множество постоянных функций.

Упражнение 10.18*. Имеется ли биекция между точками отрезка $[0,1]$ и $\mathbb{R}$-точками кольца непрерывных функций $[0,1] \longrightarrow \mathbb{R}$? Изменится ли ответ, если заменить отрезок на полуинтервал? Изменятся ли ответы, если заменить непрерывные функции на а) дифференцируемые б) полиномиальные?

Тем самым, как только зафиксировано кольцо констант K, например $K = \mathbb{R}$, и выбран некоторый класс колец R, содержащих K в качестве подкольца, так сразу же возникает геометрическая теория, пространствами в которой будут множества $X[R]$, описанные выше, а кольцами регулярных функций на этих пространствах будут подкольца $R \subset K^{X[R]}$, вложенные в $K^{X[R]}$ так, как это объяснялось выше. Замечательно, что всякий гомоморфизм колец

$$R_1 \xrightarrow{\varphi} R_2\,,$$

тождественно действующий на кольце констант K, может восприниматься при этом как гомоморфизм подъёма для некоторого отображения пространств, ассоциированных с этими кольцами, а именно, для отображения подъёма

$$\varphi^* : X[R_2] \xrightarrow{p \mapsto p \circ \varphi} X[R_1]\,,$$

переводящего K-точку $R_2 \xrightarrow{p} K$ в её подъём $R_1 \xrightarrow{\varphi} R_2 \xrightarrow{p} K$ вдоль гомоморфизма φ.

Упражнение 10.19. Убедитесь, что $(\varphi^*)^* = \varphi$.

В результате между точками и функциями возникает замечательная симметрия, играющая фундаментальную роль во всей математике. Причина её кроется в том, что выражение $f(x)$ в действительности абсолютно симметрично по x и f — можно считать, что f вычисляется на x, а можно считать, что x вычисляется на f — и нет никакого естественного способа сделать этот выбор *a priori*. Точки точно также являются же функциями на пространстве функций, как функции — на пространстве точек.

[1] по-английски: *evaluation map*

Если в качестве кольца констант взять некоторое поле $\Bbbk$, а в качестве колец регулярных функций — конечные прямые произведения $\Bbbk^n$ (с произвольными $n \in \mathbb{N}$), то описанный выше механизм сопоставления кольцам пространств выдаст в качестве результата геометрическую теорию, известную как *конечномерная линейная алгебра*, с которой начнём знакомиться в следующем модуле. Если взять более сложный класс колец — кольца многочленов $\Bbbk[x_1, x_2, \dots, x_n]$ и их фактор кольца, то мы получим теорию, известную как *аффинная алгебраическая геометрия*, которую мы тоже обсудим через некоторое время. Описания классов колец, отвечающих за более сложные геометрические теории, возникающие в анализе, топологии и математической физике, можно отнести к наиболее ярким достижениям математики XX века.