А. Л. Городенцев[1]

АЛГЕБРА

(первый семестр)

Это начальный курс алгебры, который я читаю в НМУ в 2013/14 учебном году. Упражнения, встречающиеся в тексте существенны для его понимания и часто используются в дальнейшем.

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

Оглавление

§1. Справочник по множествам и отображениям

1.1. Множества. Мы не будем заниматься основаниями теории множеств, полагаясь на школьное интуитивное представление о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множества мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

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

Множество X называется *подмножеством* множества Y, если каждый элемент $x \in X$ лежит также и в Y. В этом случае пишут $X \subset Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Непустые подмножества, отличные от всего множества, называются *собственными подмножествами*.

Упражнение 1.1. Сколько всего подмножеств (включая несобственные) 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 $X \setminus Y$, 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 $X \cap Y = X \setminus (X \setminus Y)$. Можно ли выразить разность через пересечение и объединение?

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

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

1.2. Отображения. Отображение $f : X \to Y$ из множества X в множество Y — это правило, которое сопоставляет каждой точке $x \in X$ некоторую однозначно определяемую по x точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f.

Множество всех точек $x \in X$, образ которых равен данной точке $y \in Y$, называется *полным прообразом* точки y (или *слоем* отображения f над y) и обозначается

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

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

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

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

Отображение $f : X \to Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\mathrm{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюръективные отображения стрелками $X \twoheadrightarrow Y$.

Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$, т. е. когда прообраз каждой точки $y \in Y$ содержит не более одного элемента. Инъективные отображения мы обозначает стрелками $X \hookrightarrow Y$.

Упражнение 1.3. Перечислите все отображения $\{0, 1, 2\} \to \{0, 1\}$ и все отображения $\{0, 1\} \to \{0, 1, 2\}$. Сколько среди них вложений и сколько наложений?

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

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

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

Упражнение 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.

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

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

Пример 1.1 (запись отображений словами)
Рассмотрим множества $X = \{1, 2, \ldots, n\}$ и $Y = \{1, 2, \ldots, m\}$, сопоставим каждому отображению $f : X \to Y$ последовательность его значений:

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

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

Запись отображения словом задаёт биекцию

$$w : \mathrm{Hom}(X, Y) \xrightarrow{\sim} \{\text{слова из } |X| \text{ букв в алфавите } Y\}, \quad f \mapsto w(f). \tag{1-2}$$

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюръективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых задействованы все буквы алфавита Y, причём каждая — ровно по одному разу.

1.3. Разбиения. Задать отображение $f : X \to Y$ это то же самое, что представить X в виде дизъюнктного объединения непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \operatorname{im}(f)$:

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

Такой взгляд на отображения часто оказывается полезным при подсчёте числа элементов в том или ином множестве.

Скажем, когда все непустые слои отображения $f : X \to Y$ состоят из одного и того же числа точек $m = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X формулой

$$|X| = m \cdot |\operatorname{im} f|\,, \tag{1-4}$$

которая при всей своей банальности имеет множество применений.

Предложение 1.1
Если $|X| = n$ и $|Y| = m$, то $|\operatorname{Hom}(X, Y)| = m^n$.

Доказательство. Зафиксируем какую-нибудь точку $x \in X$ и рассмотрим *отображение вычисления*[1], сопоставляющее отображению $f : X \to Y$ его значение в точке x:

$$\operatorname{ev}_x : \operatorname{Hom}(X, Y) \to Y\,, \quad f \mapsto f(x)\,. \tag{1-5}$$

Прообраз $\operatorname{ev}_x^{-1}(y)$ любой точки $y \in Y$ находится в очевидной биекции с множеством всех отображений из $(n-1)$-элементного множества $X \smallsetminus \{x\}$ в Y:

$$\operatorname{ev}_x^{-1}(y) = \{f : X \to Y \mid f(x) = y\} \simeq \operatorname{Hom}\left(X \smallsetminus \{x\}\,,\, Y\right)\,.$$

Так как $\operatorname{im} \operatorname{ev}_x = Y$, по формуле (1-4) получаем $|\operatorname{Hom}(X, Y)| = |\operatorname{Hom}\left(X \smallsetminus \{x\}\,,\, Y\right)| \cdot |Y|$, т. е. при добавлению к множеству X одной точки, количество отображений из X в Y увеличивается в $|Y|$ раз. Отсюда $\operatorname{Hom}(X, Y) = |Y|^{|X|}$. □

Замечание 1.1. Множество отображений $\operatorname{Hom}(X, Y)$ часто обозначают через Y^X, и предыдущее рассуждение объясняет это обозначение.

Замечание 1.2. В предл. 1.1 мы молчаливо предполагали, что $m, n > 0$, т. е. что оба множества X, Y непусты. Если $X = \varnothing$, то удобно считать, что $\operatorname{Hom}(\varnothing, Y)$ для любого множества Y состоит ровно из одного элемента, «вкладывающего» $\varnothing$ в качестве подмножества в Y, ибо формально $\varnothing \subset Y$. И хотя отображения вычисления (1-5) в этом случае не определены, утверждение предл. 1.1 формально верно: $1 = m^0$. Если $Y = \varnothing$, то $\operatorname{Hom}(X, \varnothing) = \varnothing$ для любого $X \neq \varnothing$, а $\operatorname{Hom}(\varnothing, \varnothing)$ — это одноэлементное множество $\{\mathrm{Id}_\varnothing\}$. Первое также формально согласуется с предл. 1.1: $0^n = 0$. Последнее указывает на то, что 0^0 имеет смысл считать равным 1.

[1] обозначение «ev» является сокращением слова *evaluation*

Предложение 1.2
Если $|X| = n$, то $|\operatorname{Aut}(X)| = n!$.

Доказательство. Положим $Y = X$ в доказательстве предл. 1.1 и ограничим отображение вычисления (1-5) на подмножество биекций $\operatorname{Aut}(X) \subset \operatorname{Hom}(X, X)$. Получим отображение

$$\mathrm{ev}_x : \operatorname{Aut}(X) \to X, \quad f \mapsto f(x).$$

Его слой $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X$ состоит из всех биекций $X \xrightarrow{\sim} X$, переводящих x в x'. Беря композицию такой биекции с автоморфизмом $X \xrightarrow{\sim} X$, который переставляет между собой x и x', оставляя все остальные точки на месте, мы получаем взаимно однозначное отображение из $\mathrm{ev}_x^{-1}(x')$ в множество автоморфизмов $(n-1)$-элементного множества $X \smallsetminus \{x\}$. Поэтому все слои $\mathrm{ev}_x^{-1}(x')$ непусты и состоят из одного и того же числа элементов. По формуле (1-4) $|\operatorname{Aut}(X)| = |\operatorname{Aut}(X \smallsetminus \{x\})| \cdot |X|$, т. е. при добавлении n-той точки к $(n-1)$-элементному множеству количество его автоморфизмов увеличивается в n раз. Поэтому $|\operatorname{Aut}(X)| = n \cdot (n-1) \cdot (n-2) \cdot \ \cdots \ \cdot 1 = n!$. □

Замечание 1.3. Так как $|\operatorname{Aut}(\varnothing)| = |\{Id_\varnothing\}| = 1$, мы по определению полагаем $0! \stackrel{\text{def}}{=} 1$.

Пример 1.2 (мультиномиальные коэффициенты)
При раскрытии скобок в выражении $(a_1 + a_2 + \ \cdots \ + a_m)^n$ получится сумма одночленов вида $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$, где каждый показатель k_i заключен в пределах $0 \leqslant k_i \leqslant n$, а общая степень $k_1 + k_2 + \ \cdots \ + k_m = n$. Коэффициент, возникающий при таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{k_1 \dots k_m}$. Таким образом,

$$(a_1 + a_2 + \ \cdots \ + a_m)^n = \sum_{\substack{k_1+k_2+\ \cdots \ +k_m=n \\ \forall i \ 0 \leqslant k_i \leqslant n}} \binom{n}{k_1 \dots k_m} \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}, \tag{1-6}$$

Чтобы явно выразить $\binom{n}{k_1 \dots k_m}$ через $k_1, k_2, \dots, k_m$, заметим, что раскрытие n скобок

$$(a_1 + a_2 + \ \cdots \ + a_m)(a_1 + a_2 + \ \cdots \ + a_m) \ \cdots \ (a_1 + a_2 + \ \cdots \ + a_m)$$

заключается в последовательном выборе внутри каждой из скобок какой-нибудь одной буквы и выписывании их слева направо друг за другом в одно n-буквенное слово. Это надо сделать всеми возможными способами и сложить все полученные слова. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$ суть слова, состоящие ровно из k_1 букв a_1, k_2 букв a_2, … , k_m букв a_m. Количество таких слов легко подсчитать по формуле (1-4).

А именно, сделаем на время k_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с k_2 буквами a_2, k_3 буквами a_3 и т. д. В результате получится набор из $n = k_1 + k_2 + \ \cdots \ + k_m$ попарно различных букв:

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

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n различными буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, $|X| = n!$. В качестве Y возьмём интересующее нас множество слов из k_1 одинаковых букв a_1, k_2 одинаковых букв a_2, и т. д. и рассмотрим отображение $f : X \to Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1! \cdot k_2! \cdot \ \cdots \ \cdot k_m!$ слов, которые получаются из y всевозможными расстановками k_1 верхних индексов у букв a_1, k_2 верхних индексов у букв a_2, и т. д. По формуле (1-4)

$$\binom{n}{k_1 \dots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ \cdots \ \cdot k_m!}\,. \tag{1-7}$$

Тем самым, разложение (1-6) имеет вид

$$(a_1 + a_2 + \ \cdots \ + a_m)^n = \sum_{\substack{k_1 + \ \cdots \ + k_m = n \\ \forall i \ 0 \leqslant k_i \leqslant n}} \frac{n! \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}}{k_1! \cdot k_2! \cdot \ \cdots \ \cdot k_m!}\,. \tag{1-8}$$

Упражнение 1.7. Сколько всего слагаемых в правой части формулы (1-8)?

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

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

При $m = 2$ мультиномиальный коэффициент

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

(и в числителе и в знаменателе стоят по k последовательно убывающих сомножителей) обозначается через $\binom{n}{k}$ или C_n^k и называется k-тым *биномиальным коэффициентом* степени n или *числом сочетаний* из n по k.

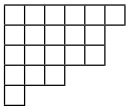
Пример 1.3 (диаграммы Юнга)
Разбиение конечного множества $X = \{1, 2, \dots, n\}$ в объединение непересекающихся подмножеств

$$X = X_1 \sqcup X_1 \sqcup X_2 \sqcup \ \dots \ \sqcup X_k\,. \tag{1-10}$$

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

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

которая называется *формой* разбиения (1-10). Форму разбиения удобно представлять себе в виде *диаграммы Юнга* — картинки вида

 , (1-11)

[1] это частный случай *формулы Ньютона*, которую в полной общности мы обсудим в n° 4.5, когда будем заниматься степенными рядами

составленной из выровненных по левому краю горизонтальных клетчатых полос, в i-той полосе λ_i клеток. Общее число клеток в диаграмме λ называется *весом* диаграммы и обозначается $|\lambda|$, а число строк называется *длиной* и обозначается $\ell(\lambda)$.

Так, диаграмма Юнга (1-11) отвечает разбиению формы $\lambda = (6,5,5,3,1)$ и имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 1.8. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток (включая пустую диаграмму и сам прямоугольник).

Будем называть *заполнением* диаграммы λ множеством X из $|X| = |\lambda|$ элементов произвольную расстановку этих элементов в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всего имеется $n!$ различных заполнений диаграммы λ множеством X.

Объединяя элементы, стоящие в i-той строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств $X_1, X_2, \dots, X_k$. Ясно, что любое разбиение (1-10) можно получить таким образом, так что мы получаем сюръективное отображение из множества заполнений диаграммы λ в множество разбиений множества X формы λ. Покажем, что все слои этого отображения состоят из одного и того же числа элементов.

Два заполнения приводят к одинаковым разбиениям тогда и только тогда, когда они получаются друг из друга перестановками элементов внутри строк и перестановками строк одинаковой длины между собою как единого целого. Если обозначить через m_i число строк длины[1] i в диаграмме λ, то перестановок первого типа будет $\prod \lambda_i! = \prod\limits_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod\limits_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod\limits_{i=1}^{n} (i!)^{m_i} m_i!$ элементов. Из формулы (1-4) вытекает

Предложение 1.3
Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, … , m_n n-элементных подмножеств равно

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

□

1.4. Классы эквивалентности. Альтернативный способ разбить заданное множество X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так. Назовём *бинарным отношением* на множестве X произвольное подмножество $R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}$. Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$.

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

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

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{1-13}$$

$$\text{неравенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{1-14}$$

$$\text{делимость} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 | x_2 \tag{1-15}$$

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \,(\mathrm{mod}\ n) \tag{1-16}$$

(последнее условие $x_1 \equiv x_2 \,(\mathrm{mod}\ n)$ читается как «x_1 сравнимо с x_2 по модулю n» и по определению означает, что x_1 и x_2 имеют одинаковые остатки от деления на n).

Определение 1.1
Бинарное отношение $\underset{R}{\sim}$ называется *эквивалентностью*, если оно обладает следующими тремя свойствами:

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

Среди перечисленных выше бинарных отношений на множестве $\mathbb{Z}$ отношения (1-13) и (1-16) являются эквивалентностями, а (1-14) и (1-15) не являются (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, пусть на множестве X задано какое-нибудь отношение эквивалентности R. Рассмотрим для каждого $x \in X$ подмножество в X, состоящее из всех элементов, эквивалентных x. Оно называется *классом эквивалентности* элемента x и обозначается

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

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

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

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]\,, \tag{1-17}$$

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

Пример 1.4 (классы вычетов)
Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (1-16) обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и опускать индекс n, когда понятно чему он равен. Класс эквивалентности

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z-x) \vdots n\} \tag{1-18}$$

называется *классом вычетов по модулю* n. Отображение факторизации

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

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

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

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

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

Упражнение 1.9. Докажите правомочность этого вычисления: проверьте, что классы вычетов $[x+y]_n$ и $[xy]_n$ не зависят от выбора чисел $x \in [x]_n$ и $y \in [y]_n$, т. е. правила

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{1-20}$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \tag{1-21}$$

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

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

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

переходит в себя при симметрии $(x,y) \leftrightarrows (y,x)$ и вместе с каждой парой точек вида (x,y), (y,z) содержит также и точку (x,z), то этими свойствами обладает и пересечение $\bigcap\limits_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества $R \subset X \times X$ существует *наименьшее по включению* отношение эквивалентности $\overline{R}$, содержащее R — пересечение всех содержащих R отношений эквивалентности. Отношение $\overline{R}$ называется эквивалентностью, *порождённой* отношением R. К сожалению, по данному множеству R не всегда легко судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу[2], часто бывает не просто.

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

[2] т. е. существует ли хоть одна собственная (отличная от всего произведения $X \times X$) эквивалентность, содержащая R

Пример 1.5 (дроби)
Множество рациональных чисел $\mathbb{Q}$ обычно определяют как множество дробей a/b с $a, b \in \mathbb{Z}$ и $b \neq 0$. При этом под *дробью* понимается класс эквивалентности упорядоченных пар $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus 0)$ по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \qquad \forall\, c \neq 0\,. \tag{1-22}$$

Отношения (1-22) выражают собою равенства дробей $a\,/\,b = ac\,/\,bc$, но сами по себе не образуют эквивалентности. Например, при $a_1 b_2 = a_2 b_1$ в двухшаговой цепочке отождествлений (1-22)

$$(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$$

самый левый и самый правый элементы может оказаться нельзя отождествить напрямую по правилу (1-22). Но эквивалентность, порождённая отождествлениями (1-22), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{1-23}$$

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

Упражнение 1.10. Проверьте, что набор отношений (1-23) рефлексивен, симметричен и транзитивен (и, тем самым, полностью описывает минимальное отношение эквивалентности, содержащее все отождествления (1-22)).

1.5. Композиции отображений. Отображение $X \to Z$, получающееся в результате последовательного выполнения двух отображений $X \xrightarrow{f} Y \xrightarrow{g} Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf. Таким образом,

$$\forall\, x \in X \;\; gf(x) \stackrel{\text{def}}{=} g(f(x))\,.$$

Композиция gf определена только тогда, когда образ f содержится в множестве, на котором определено отображение g.

Композицию трёх отображений $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ можно вычислять двумя способами: как $(hg)f$ или как $h(gf)$. В обоих случаях получится отображение, переводящее точку $x \in X$ в точку $h(g(f(x))) \in T$. Это означает, что композиция отображений *ассоциативна*[1]: $(hg)f = h(gf)$ всякий раз, когда написанные композиции определены.

Предостережение 1.1. Хотя мы и обозначаем композицию отображений точно так же, как произведение, обращаться с формулами, включающими в себя композиции, надо с осторожностью: некоторые привычные по опыту работы с числами преобразования недопустимы при работе с композициями отображений. Так, умножение чисел *коммутативно*[2]: $fg = gf$, а композиция отображений, как правило, нет[3].

[1] т. е. подчиняется *сочетательному закону* — не зависит от расстановки скобок

[2] т. е. удовлетворяет *переместительному закону* — перестановка сомножителей в произведении не влияет на результат

[3] хотя бы потому, что одна из частей этого равенства может быть определена, а другая — нет

Упражнение 1.11. Рассмотрим на плоскости пару различных прямых ℓ_1, ℓ_2, пересекающихся в точке O, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. При каком условии на прямые выполняется равенство $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Чтобы почувствовать отличие алгебраических свойств композиции от свойств умножения чисел, поучительно взглянуть на «таблицу умножения» отображений из двухэлементного множества $X = \{1, 2\}$ в себя.

Есть ровно четыре таких отображения, причём все композиции между ними определены. Если обозначать отображение $f \in \mathrm{End}(X)$ двухбуквенным словом $(f(1),\ f(2))$, как в прим. 1.1, то эти четыре эндоморфизма запишутся словами

$$(1,1),\ (1,2) = \mathrm{Id}_X,\ (2,1),\ (2,2).$$

Значения композиций gf представлены в таблице:

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

(1-24)

Обратите внимание на то, 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, т. е. 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 1.12 (левые обратные отображения). Покажите, что следующие три условия на отображение $f : X \to Y$ эквивалентны:

а) f инъективно

б) $\exists\ g : Y \to X$ такое что $gf = \mathrm{Id}_X$ (такое g называется *левым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \to X$ из $fg_1 = fg_2$ вытекает $g_1 = g_2$

и выясните, сколько левых обратных отображений имеется у заданного вложения n-элементного множества в m-элементное.

Упражнение 1.13 (правые обратные отображения). Покажите, что следующие три условия на отображение $f : X \to Y$ эквивалентны:

а) f сюръективно

б) $\exists\ g : Y \to X$ такое что $fg = \mathrm{Id}_Y$ (такое g называется *правым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \to X$ из $g_1 f = g_2 f$ вытекает $g_1 = g_2$

и выясните, сколько правых обратных отображений имеется у заданного наложения m-элементного множества на n-элементное.

1.5.1. Обратимые отображения. Если отображение $g : X \xrightarrow{\sim} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки. В этом случае правило $y \mapsto g^{-1}(y)$ определяет отображение $g^{-1} : Y \to X$, которое одновременно является и левым и правым обратным к g в смысле упр. 1.12 и упр. 1.13:

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

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

Предложение 1.4
Следующие условия на отображение $g : X \to Y$ попарно эквивалентны:

(1) g взаимно однозначно

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

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

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 отображением g^{-1} описанным выше.

Доказательство. Импликация (1) ⇒ (2) уже была установлена. Импликация (2) ⇒ (3) очевидна. Докажем, что (3) ⇒ (2). Если у отображения $g : X \to Y$ есть левое обратное $f : Y \to X$ и правое обратное $h : Y \to X$, то $f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h$ и условие (2) выполняется для $g' = f = h$.

Остаётся показать, что (2) ⇒ (1) и доказать равенство $g' = g^{-1}$. Поскольку $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, для любого $x \in g^{-1}(y)$ выполнено 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, и $g' = g^{-1}$. □

1.6. Группы преобразований. Непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$.

Если группа преобразований G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G.

Если подмножество $H \subset G$ тоже является группой, то H называются *подгруппой* группы G.

Пример 1.6 (группы перестановок)
Множество $\mathrm{Aut}(X)$ всех взаимно однозначных отображений $X \to X$ является группой. Эта группа называется *симметрической группой* (или *группой перестановок*) множества X. Все прочие группы преобразований множества X являются подгруппами этой группы.

Группа перестановок n-элементного множества $\{1, 2, \ldots, n\}$ обозначается S_n и называется n-той *симметрической группой*. Согласно предл. 1.2 $|S_n| = n!$.

Перестановку $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ мы будем записывать строчкой

$$(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

её значений $\sigma_i = \sigma(i)$, как в прим. 1.1. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ это отображения

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

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

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

Упражнение 1.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (1-24) на стр. 13.

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

§2. Коммутативные кольца и поля

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

Определение 2.1
Множество $\mathbb{F}$ с двумя операциями $\mathbb{F}\times\mathbb{F}\to\mathbb{F}$: *сложением* $(a,b)\mapsto a+b$ и *умножением* $(a,b)\mapsto ab$ называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

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

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

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

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

свойства умножения

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

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

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

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

свойства, связывающие сложение с умножением

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

нетривиальность: $0\neq 1$ (2-10)

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

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

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, а операции сложения и умножения — как операции сложения и умножения классов вычетов, определённые формулами (1-20) и (1-21) из упр. 1.9 на стр. 11. С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как «ложь» $=0$ и «истина» $=1$, сложение — как логическое «исключающее или[1]», а умножение — как логическое «и[2]». При такой интерпретации алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

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

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

Упражнение 2.2. Напишите над полем $\mathbb{F}_2$ многочлен от x, равный «не x», а также многочлен от x и y, равный «x или[1] y».

Пример 2.2 (рациональные числа)
Напомним, что поле рациональных чисел $\mathbb{Q}$ можно определить как множество дробей a/b, где под «дробью» понимается класс эквивалентности упорядоченной пары (a, b) с $a, b \in \mathbb{Z}$ и $b \neq 0$ по отношению $(a_1, b_1) \sim (a_2, b_2)$ при $a_1 b_2 = a_2 b_1$, которое является минимальным отношением эквивалентности, содержащим все отождествления

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

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

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

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

Пример 2.3 (вещественные числа)
Множество вещественных чисел $\mathbb{R}$ определяется в курсе анализа несколькими различными способами: как множество классов эквивалентности десятичных[2] дробей, как множество дедекиндовых сечений упорядоченного множества $\mathbb{Q}$, или как множество классов эквивалентности рациональных последовательностей Коши. Мы полагаем, что читатель знаком с этими определениями и понимает, как они связаны друг с другом. Какое бы описание множества $\mathbb{R}$ ни использовалось, задание на нём сложения и умножения и проверка аксиом из опр. 2.1 требуют некоторой работы, традиционно проделываемой в курсе анализа.

2.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти эти операции обладают всеми свойствами из опр. 2.1 на стр. 16 за исключением свойства (2-8) существования мультипликативно обратного элемента.

Если, кроме существования обратного, из списка аксиом поля исключаются требование существования единицы (2-7) и условие $0 \neq 1$, то множество K с двумя операциями, удовлетворяющими оставшимся аксиомам, называется просто *коммутативным кольцом*.

Примерами отличных от полей колец с единицами являются кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные целые числа, многочлены с чётными целыми коэффициентами, многочлены без свободного члена с коэффициентами в любом коммутативном кольце и т. п.

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

[2] или привязанных к какой-либо другой позиционной системе счисления, например, двоичных

2.1.2. Абелевы группы. Множество A *с одной* операцией $A \times A \to A$, удовлетворяющей первым четырём аксиомам сложения из опр. 2.1, называется *абелевой группой*. Таким образом, всякое коммутативное кольцо K является абелевой группой относительно операции сложения. Эта группа называется *аддитивной группой кольца*. Пример абелевой группы, не являющейся кольцом, доставляют *векторы*.

Пример 2.4 (геометрические векторы)
Будем называть *геометрическим вектором* класс направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему отрезки, получающиеся друг из друга параллельным переносом. Нулевым вектором назовём класс эквивалентности точки — это единственный вектор, имеющий нулевую длину и не имеющий направления. Сложение векторов определяется стандартным образом: надо выбрать представителей векторов a и b так, чтобы конец a совпал с началом b, и объявить $a+b$ равным вектору с началом в начале a и концом в конце b. Коммутативность и ассоциативность этой операции демонстрируются на рис. 2⋄1 и рис. 2⋄2.

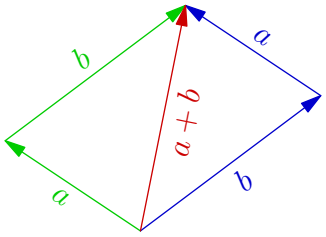


Рис. 2⋄1. Правило параллелограмма.

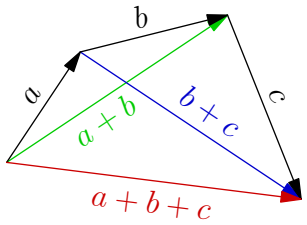


Рис. 2⋄2. Правило четырёхугольника.

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

Пример 2.5 (мультипликативная группа поля)
Четыре аксиомы умножения из опр. 2.1 на стр. 16 утверждают, то множество

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

всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно умножения. Эту группу называют *мультипликативной группой поля*. Роль нуля из аддитивной группы $\mathbb{F}$ в мультипликативной группе $\mathbb{F}^*$ исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Лемма 2.1
В любой абелевой группе A нейтральный элемент единственен, и для любого $a \in A$ элемент, противоположный к a, однозначно определяется по a (в частности, $-(-a) = a$).

Доказательство. Будем записывать операцию в A аддитивно. Если есть два нулевых элемента 0_1 и 0_2, то $0_1 = 0_1 + 0_2 = 0_2$ (первое равенство выплнено, поскольку 0_2 является нулевым элементом, второе — в силу того, то нулевым элементом является 0_1). Если есть два элемента $-a$ и $-a'$, противоположных к a, то $-a = (-a) + 0 = (-a) + \big(a + (-a')\big) =$ $= \big((-a) + a\big) + (-a') = 0 + (-a') = -a'$. □

Лемма 2.2
В любом коммутативном кольце K для любого $a \in K$ выполняется равенство $0 \cdot a = 0$, и если в K имеется единица, то $(-1) \cdot a$ противоположен к a для любого $a \in A$.

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

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

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

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

В частности, операция вычитания имеется в абелевой группе любого коммутативного кольца. В поле ненулевые элементы образуют абелеву группу по умножению. Поэтому в любом поле имеется ровно один единичный элемент, и для любого ненулевого элемента a обратный к нему элемент a^{-1} однозначно определяются по a. Тем самым, в любом поле помимо сложения, умножения и вычитания (2-12) имеется операциия *деления* на любые ненулевые элементы

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

2.2. Делимость в кольце целых чисел. Основным отличием коммутативных колец с единицей от полей является отсутствие обратных элементов к некоторым ненулевым элементам кольца. Элемент a коммутативного кольца K с единицей называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*.

Например, в кольце $\mathbb{Z}$ обратимыми элементами являются только 1 и -1. В кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами обратимыми элементами являются только ненулевые константы (многочлены степени нуль).

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

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

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

множество всех целых чисел, представимых в виде $ax + by$ с целыми x, y. Это множество образует в $\mathbb{Z}$ подкольцо, и вместе с каждым своим элементом содержит и все его кратные. Кроме того, все числа из (a, b) нацело делятся на каждый общий делитель чисел a и b, и сами a и b тоже входят в (a, b).

Обозначим через d наименьшее положительное число в (a, b). Остаток от деления любого числа $z \in (a, b)$ на d лежит в кольце (a, b), поскольку он представляется в виде

$z - kd$, а z и kd лежат в кольце (a, b). Так как этот остаток строго меньше d, он равен нулю. Следовательно, (a, b) совпадает с множеством всех чисел, кратных d.

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

Упражнение 2.4. Обобщите предыдущее рассуждение: для любого конечного набора чисел $a_1, a_2, \dots, a_m$ постройте число d, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + a_2x_2 + \cdots + a_mx_m$ с целыми x_i. Покажите, что уравнение $n = a_1x_1 + a_2x_2 + \cdots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ тогда и только тогда, когда n делится на d.

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

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

Числа E_k строго убывают до тех пор, пока очередное число E_r не разделит нацело предыдущее число E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой элемент E_r последовательности E_k и будет наибольшим общим общим делителем чисел (a, b), причём он автоматически получится представленным в виде $E_r = x \cdot E_0 + y \cdot E_1$, если при вычислении каждого E_k мы будем представлять его в виде $E_k = x \cdot E_0 + y \cdot E_1$.

Упражнение 2.5. Докажите это.

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

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

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

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

Упражнение 2.6. Докажите, что в возникающем на последнем шаге работы алгоритма Евклида представлении нуля в виде $0 = E_{r+1} = q_0E_0 + q_1E_1$ число $|q_0E_0| = |q_1E_1|$ рано *наименьшему общему кратному* нок(a, b).

Замечание 2.2. С вычислительной точки зрения алгоритм Евклида *несопоставимо* быстрее разложения на простые множители. Читателю предлагается убедиться в этом, попытавшись «вручную» разложить на простые множители числа $n = 10\,203$ и $m = 4\,687$ из абсолютно ручного вычисления (2-16). Найти два очень больших простых числа по заданному их произведению невозможно за разумное время даже на мощном компьютере. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

2.3. Взаимная простота. В кольце целых чисел $\mathbb{Z}$ условие $\text{нод}(a, b) = 1$ равносильно разрешимости в целых числах уравнения $ax + by = 1$, и числа a, b, обладающие этими свойствами, называются *взаимно простыми*.

В произвольном коммутативном кольце K с единицей из разрешимости уравнения $ax + by = 1$ вытекает отсутствие у элементов a и b необратимых общих делителей: если $a = d\alpha$, $b = d\beta$, и при этом $ax + by = 1$, то $d(\alpha + \beta) = 1$ и d обратим.

Однако, отсутствие у a и b необратимых общих делителей, вообще говоря, не гарантирует разрешимости уравнения $ax + by = 1$. Например, в кольце многочленов от двух переменных $\mathbb{Q}[x, y]$ одночлены x и y не имеют общих делителей, отличных от констант, однако равенство $f(x, y) \cdot x + g(x, y) \cdot y = 1$ невозможно ни при каких $f, g \in \mathbb{Q}[x, y]$.

Упражнение 2.7. Объясните почему.

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

Определение 2.2
Элементы a и b произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если уравнение $ax + by = 1$ разрешимо в K относительно x и y.

Лемма 2.3
В произвольном коммутативном кольце K с единицей для любого $c \in K$ и любых взаимно простых $a, b \in K$ справедливы импликации:

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

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

Кроме того, если $a \in K$ взаимно прост с каждым из элементов $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением $b_1 b_2 \ \dots \ b_m$.

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

Упражнение 2.8. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое целое число z является произведением конечного числа простых чисел[1], причём любые два таких представления $p_1 p_2 \cdots p_k = z = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\, i\ p_i = \pm q_i$.

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

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

2.4. Кольцо вычетов $\mathbb{Z}/(n)$. Напомним, что числа $a, b \in \mathbb{Z}$ называются *сравнимыми* по модулю n (что записывается как $a \equiv b \pmod{n}$), если их разность $a - b$ делится на n. Сравнимость по модулю n является отношением эквивалентности (см. n° 1.4) и разбивает множество целых чисел на непересекающиеся классы сравнимых по модулю n чисел. Эти классы называются *классами вычетов по модулю* n, а их совокупность обозначается через $\mathbb{Z}/(n)$. Мы будем писать $[a]_n \in \mathbb{Z}/(n)$ для обозначения класса, содержащего число $a \in \mathbb{Z}$. Такая запись как обозначение для класса неоднозначна: числа $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$ задают один и тот же класс $[x]_n = [y]_n$ тогда и только тогда, когда $x = y + dn$ для некоторого $d \in \mathbb{Z}$.

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

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

Согласно упр. 1.9 на стр. 11, эти операции определены корректно[1]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (2-17) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы кольца выполняются.

2.4.1. Делители нуля и нильпотенты. В $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(8)$ ненулевой класс $[2]$ имеет нулевой куб $[2]^3 = [8] = [0]$.

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

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

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

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

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

Проверить, обратим ли данный класс $[m]_n$ и вычислить $[m]_n^{-1}$ можно при помощи алгоритма Евклида из n° 2.2.2. К примеру, вычисление из формулы 2-16 на 20 показывает, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и $[10\,203]^{-1} = [147] \pmod{4\,687}$, а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $[4\,687]^{-1} = -[320] \pmod{10\,203}$.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют абелеву группу относительно умножения. Она называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Её порядок равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается через $\varphi(n)$ и называется *функцией Эйлера* числа n.

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

Пример 2.6 (бином Ньютона по модулю p)
В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

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

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

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

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

Лемма 2.4
При простом p и любом k в пределах $1 \leqslant k \leqslant (p - 1)$ биномиальный коэффициент $\binom{p}{k}$ делится на p.

Доказательство. Поскольку число p взаимно просто с каждым из чисел в пределах от 1 до $p - 1$, оно по лем. 2.3 взаимно просто с произведением $k!\,(p - k)!$. Поскольку $p!$ делится на $k!\,(p - k)!$, мы из того же лем. 2.3 заключаем, что $(p - 1)!$ делится на $k!\,(p - k)!$. Следовательно, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 2.1 (малая теорема Ферма)
Для любого $a \in \mathbb{Z}$ и любого простого $p \in \mathbb{N}$ выполняется сравнение $a^p \equiv a \pmod{p}$.

Доказательство. Надо показать, что $[a^p] = [a]$ в поле $\mathbb{F}_p$. Согласно (2-19), имеем

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

□

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

2.5. Прямые произведения. Прямое поизведение

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

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

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

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

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

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

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

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

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

Упражнение 2.12. Убедитесь, что $\prod K_x$ является кольцом, причём если все K_x были кольцами с единицей, то $\prod K_x$ также будет кольцом с единицей $(1, 1, \ldots, 1) \in \prod K_x$.

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

В прямом произведении колец любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0,\ 1,\ \ldots,\ 1)$ является делителем нуля, т. к. $(0,\ 1,\ \ldots,\ 1)(1,\ 0,\ \ldots,\ 0) = (0,\ 0,\ \ldots,\ 0) = 0$. Поэтому произведение нескольких[1] колец (в частности, произведение нескольких полей) никогда не является полем.

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

[1] т. е. как минимум двух

мультипликативную группу $\mathbb{F}_p^* \times \mathbb{F}_q^*$ и $p+q-2$ делителя нуля, имеющих вид $(a,0)$ и $(0,b)$ с $a,b \neq 0$.

В общем случае элемент $a = (a_1, a_2, \dots, a_m) \in K_1 \times K_2 \times \cdots \times K_m$ 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 $\prod K_\nu$ является прямым произведением групп обратимых элементов колец K_ν:

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

2.6. Гомомрфизмы. Отображение абелевых групп $\varphi : A \to B$ называется *гомоморфизмом*, если для любой пары элементов $a_1, a_2 \in A$ в B выполнено соотношение

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

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

Упражнение 2.13. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

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

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

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

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

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

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

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

Предложение 2.1
Слой любого гомоморфизма абелевых групп $\varphi : A \to B$ над произвольной точкой $b \in B$ либо пуст, либо равен $\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$, где $a \in A$ — какой-нибудь элемент, переходящий в b. В частности, инъективность гомоморфизма φ равносильна равенству $\ker\varphi = 0$.

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

2.6.2. Группа гомоморфизмов. Для абелевых групп A, B через $\operatorname{Hom}(A,B)$ мы обозначаем множество всех *гомоморфизмов* $A \to B$. Это множество является абелевой группой относительно операции поточечного сложения значений:

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

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

2.6.3. Гомоморфизмы колец. Отображение колец $\varphi : A \to B$ называется *гомоморфизмом колец*, если для любой пары элементов $a_1, a_2 \in A$ в B выполнены соотношения:

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

Поскольку гомоморфизм колец $\varphi : A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми перечисленными выше свойствами гомоморфизмов абелевых групп: $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, и все непустые слои φ представляют собою сдвиги слоя над нулём: если $\varphi(a) = b$, то

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

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

Ядро гомоморфизма колец $\varphi : A \to B$ вместе с каждым элементом $a \in \ker\varphi$ содержит и все кратные ему элементы aa', поскольку $\varphi(aa') = \varphi(a)\varphi(a') = 0$. В частности, $\ker\varphi$ является подкольцом в A.

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

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

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

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

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

Предложение 2.3
Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.

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

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

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

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

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

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

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

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

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

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

Из взаимной простоты числа n_i с остальными n_ν вытекает, что n_i взаимно просто с их произведением $m_i = \prod\limits_{\nu \neq i} n_\nu$ (см. лем. 2.3). Поэтому для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Число $b_i = m_i y_i$ даёт остаток 1 от деления на n_i и делится на все n_ν с $\nu \neq i$. Поэтому число $z = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m$ решает задачу.

Для демонстрации эффективности этого алгоритма найдём, к примеру, наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$.

Сначала найдём число, обратное к $91 \cdot 179$ по модулю 57. Так как $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, для этого достаточно применить алгоритм Евклида к $E_0 = 57$ и $E_1 = 13$. В результате получим $22 \cdot 13 - 5 \cdot 57 = 1$, откуда $-22 \cdot 91 \cdot 179 \equiv 1 \pmod{57}$. Число

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(см. прим. 2.6 и лем. 2.4 на стр. 23). Гомоморфизм (2-27) называется *гомоморфизмом Фробениуса*. В силу малой теоремы Ферма[1], он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$.

[1] см. сл. 2.1 на стр. 23

§3. Многочлены и расширения полей

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

3.1. Степенные ряды и многочлены. Бесконечное выражение вида

$$A(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \cdots \quad \text{с} \quad a_i \in K \tag{3-1}$$

называется *формальным степенным рядом* от переменной x с коэффициентами в кольце K. Два формальных степенных ряда

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \cdots \\ B(x) &= b_0 + b_1 x + b_2 x^2 + \cdots \end{aligned} \tag{3-2}$$

равны, если $a_i = b_i$ для всех i. Сложение и умножение рядов (3-2) определяется стандартными правилами раскрытия скобок и приведения подобных слагаемых: коэффициенты рядов $A(x) + B(x) = s_0 + s_1 x + s_2 x^2 + \cdots$ и $A(x)B(x) = p_0 + p_1 x + p_2 x^2 + \cdots$ суть[1]

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

Упражнение 3.1. Убедитесь, что операции (3-3) удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной x с коэффициентами в кольце K обозначается через $K[\![x]\!]$. Начальный коэффициент a_0 ряда (3-1) называется *свободным членом* этого ряда. Первый ненулевой коэффициент ряда A называется *младшим* коэффициентом.

Если в кольце K нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца тоже является целостным.

Кольцо $K[\![x_1, x_2, \ldots, x_n]\!]$ формальных степенных рядов от n переменных $x_1, x_2, \ldots, x_n$ определяется по индукции: $K[\![x_1, x_2, \ldots, x_n]\!] = K[\![x_1, x_2, \ldots, x_{n-1}]\!][\![x_n]\!]$ и представляет собой множество формальных сумм вида

$$F(x) = \sum_{\nu_1, \ldots, \nu_n \in \mathbb{Z}_{\geqslant 0}} a_{\nu_1 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}.$$

3.1.1. Алгебраические операции над формальными рядами. Назовём *n-арной алгебраической операцией* в $K[\![x]\!]$ всякое правило, сопоставляющее рядам $f_1, f_2, \ldots, f_n \in K[\![x]\!]$ новый ряд $g \in K[\![x]\!]$ так, что каждый коэффициент ряда g вычисляется по коэффициентам рядов $f_1, f_2, \ldots, f_n$ при помощи конечного числа сложений и умножений (возможно, зависящего от номера коэффициента).

[1] формально говоря, мы определяем здесь операции над *последовательностями* (a_ν) и (b_ν) элементов кольца K, а буква x используется лишь для облегчения восприятия этих операций

Например, сложение и умножение рядов — это алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[1]. Напротив, подстановка в ряд $f(x)$ вместо x любого ряда без свободного члена $g(x) = b_1x + b_2x^2 + \cdots$ — это алгебраическая операция, дающая ряд

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

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых. Ещё одним примером алгебраической операции является обращение рядов.

Предложение 3.1
Ряд $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[\![x]\!]$ тогда и только тогда обратим в $K[\![x]\!]$, когда его свободный член a_0 обратим в K. Если обратный ряд существует, то операция обращения $f \mapsto f^{-1}$ является алгебраической.

Доказательство. Если существует ряд $f^{-1}(x) = b_0+b_1x+b_2x^2+\cdots$, такой что $f(x)\cdot f^{-1}(x) = 1$, то $a_0b_0 = 1$, откуда a_0 обратим. Наоборот, допустим, что $a_0 \in K$ обратим. Приравнивая коэффициенты при одинаковых степенях x в правой и левой части равенства

$$\bigl(a_0 + a_1x + a_2x^2 + \cdots\bigr)\cdot\bigl(b_0 + b_1x + b_2x^2 + \cdots\bigr) = 1\,,$$

мы получаем на коэффициенты b_i бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots & \end{aligned} \tag{3-4}$$

из которой $b_0 = a_0^{-1}$ и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0)$ при $k \geqslant 1$. Это позволяет рекурсивно вычислить все коэффициенты. □

Упражнение 3.2. Вычислите в $\mathbb{Q}[\![x]\!]$ а) $(1-x)^{-1}$ б) $(1-x^2)^{-1}$ в) $(1-x)^{-2}$.

3.1.2. Многочлены. Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от переменных $x_1, x_2, \ldots, x_n$ с коэффициентами в кольце K образуют в кольце всех формальных степенных рядов подкольцо, которое обозначается

$$K[x_1, x_2, \ldots, x_n] \subset K[\![x_1, x_2, \ldots, x_n]\!]$$

Многочлен от одной переменной x представляет собой формальное выражение вида

$$f(x) = a_0 + a_1x + \cdots + a_nx^n\,.$$

[1]очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда; похожий эффект иногда возникает при вычислении значений некоторых очень специальных рядов в некоторых очень специальных точках α; но при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений

Последний ненулевой коэффициент этого выражения называется *старшим* коэффициентом многочлена f, а его номер называется *степенью* многочлена f и обозначается $\deg f$. Многочлены со старшим коэффициентом 1 называются *приведёнными*. Многочлены степени нуль называются *константами*.

Предложение 3.2
Если кольцо K целостное[1], то для любых многочленов $f_1, f_2 \in K[x]$ выполняется равенство $\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)$. В частности, кольцо $K[x]$ тоже целостное, и его обратимыми элементами являются только обратимые константы.

Доказательство. Все утверждения следуют из того, что старший коэффициент произведения равен произведению старших коэффициентов сомножителей. □

Упражнение 3.3. Покажите, что в кольце $\mathbb{Z}[x,y]$ двучлен $(y^n - x^n)$ делится нацело на двучлен $(y - x)$ и найдите частное.

3.1.3. Дифференциальное исчисление. Подставим в степенной ряд

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

вместо x сумму $x + t$, где t — ещё одна переменная. Получится ряд

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

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

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

Упражнение 3.4. Убедитесь, что $f_0(x) = f(x)$ совпадает с исходным рядом f.

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

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

и может быть вычислен при помощи упр. 3.3 как значение при $t = 0$ ряда

$$\frac{f(x+t)-f(x)}{t} = a_1\cdot\frac{(x+t)-t}{t} + a_2\cdot\frac{(x+t)^2-t^2}{t} + a_3\cdot\frac{(x+t)^3-t^3}{t} + \cdots = \\ = \sum_{k\geqslant 1} a_k\cdot\left((x+t)^{k-1} + (x+t)^{k-2}x + (x+t)^{k-3}x^2 + \cdots + x^{k-1}\right) .$$

Получаем хорошо известную формулу

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

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

Пример 3.1 (ряды с нулевой производной)
Из формулы (3-6) вытекает, что производная от константы равна нулю. Если $\operatorname{char} K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = \text{const}$. Однако, когда кольцо K имеет положительную характеристику, производная от всех мономов x^m, показатель которых делится на характеристику, обращается в нуль, поскольку согласно проделанному выше вычислению коэффициент m в формуле

$$\frac{d}{dx}\, x^m = \underbrace{x^{m-1} + \cdots + x^{m-1}}_{m} = m \cdot x^{m-1}$$

представляет собою сумму m единиц кольца. В частности, над полем $\Bbbk$ характеристики $p > 0$ производная от ряда $f(x)$ равна нулю тогда и только тогда, когда

$$\exists\, g \in \Bbbk[\![x]\!] \;:\; f(x) = g(x^p) = g(x)^p \tag{3-7}$$

(второе равенство справедливо, поскольку возведение в p-ю степень является гомоморфизмом).

Предложение 3.3 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[\![x]\!]$ справедливы равенства

$$(\alpha f)' = \alpha \cdot f'\,, \quad (f+g)' = f' + g'\,, \quad (fg)' = f' \cdot g + f \cdot g'\,. \tag{3-8}$$

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

$$\big(f(g(x))\big)' = g'(x) \cdot f'\big(g(x)\big)\,, \tag{3-9}$$

а если ряд f обратим, то

$$\frac{d}{dx} f^{-1} = -f'/f^2\,. \tag{3-10}$$

Доказательство. Первые два равенства в (3-8) вытекают прямо из формулы (3-6). Для доказательства третьего перемножим ряды

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

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

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

откуда $(fg)' = f' \cdot g + f \cdot g'$. Формула (3-9) доказывается похожим образом. Подставим в $f(x)$ вместо x ряд $g(x+t)$: $f\big(g(x+t)\big) = f\big(g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2)\big)$ и обозначим ряд, который прибавляется к $g(x)$ в аргументе f, через

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

Тогда

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

откуда $\bigl(f(g(x))\bigr)' = g'(x)\cdot f'\bigl(g(x)\bigr)$. Для доказательства формулы (3-10) продифференцируем обе части равенства $f\cdot f^{-1}=1$. Получим $f'\cdot f^{-1}+f\cdot\bigl(f^{-1}\bigr)'=0$, откуда $\bigl(f^{-1}\bigr)'=-f'/f^2$. □

Упражнение 3.5. Покажите, что в разложении (3-5) $f_m(x)=\frac{1}{m!}\frac{d^m}{dx^m}f(x)$ (здесь и далее через $\frac{d^m}{dx^m}=\left(\frac{d}{dx}\right)^m$ обозначается m-тая производная, т. е. результат m-кратного применения операции $\frac{d}{dx}$).

3.2. Делимость в кольце многочленов. Известная из школы процедура деления многочленов «уголком» может быть формализована следующим образом.

Предложение 3.4 (деление с остатком)
Пусть K — произвольное коммутативное кольцо с единицей, и многочлен $u\in K[x]$ имеет обратимый старший коэффициент. Тогда для любого многочлена $f\in K[x]$ существуют многочлены $q\in K[x]$ и $r\in K[x]$, такие что $f=u\cdot q+r$ и либо $\deg(r)<\deg(u)$, либо $r=0$. Если кольцо K целостное, то такие q и r определяются по f и u однозначно.

Доказательство. При $\deg f<\deg u$ можно взять $q=0$ и $r=f$. Далее по индукции можно считать, что q и r существуют для всех многочленов f степени $\deg f<n$, где $n\geqslant\deg u$. Если $f=a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$ и $u=b_0x^k+b_1x^{k-1}+\dots+b_{k-1}x+b_k$, то степень многочлена $f-a_0b_0^{-1}x^{n-k}u$ строго меньше n, и по индукции он представляется в виде $qu+r$ с $r=0$ или $\deg r<\deg u$. Тогда $f=(q+a_0b_0^{-1}x^{n-k})\cdot u+r$ также представляется в требуемом виде. Если кольцо K целостное, и p, s — другая пара многочленов, таких что $\deg(s)<\deg(u)$ и $up+s=f=uq+r$, то $u(q-p)=r-s$. При $p-q\neq 0$ степень многочлена в левой части не менее $\deg u$, т. е. строго больше, чем степень многочлена в правой части. Следовательно, $p-q=0$, откуда и $r-s=0$. □

Определение 3.1
Многочлены q и r, удовлетворяющие условиям предл. 3.4 называются *неполным частным остатком* от деления f на u в $K[x]$.

Следствие 3.1
Для любых многочленов $f,g\in\Bbbk[x]$ с коэффициентами в произвольном поле $\Bbbk$ существует единственная пара многочленов $q,r\in\Bbbk[x]$, таких что $f=g\cdot q+r$ и либо $\deg(r)<\deg(g)$, либо $r=0$.

Пример 3.2 (вычисление значения многочлена в точке)
Остаток от деления любого многочлена $f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$ на линейный двучлен $u(x)=x-\alpha$ — это константа, равная значению $f(\alpha)$ многочлена f при $x=\alpha$, в чём легко убедиться, подставляя $x=\alpha$ в равенство $f(x)=(x-\alpha)\cdot q(x)+r$. Отметим, что «деление уголком» является значительно более быстрым способом вычисления $f(\alpha)$, чем лобовая подстановка $x=\alpha$ в $a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$.

Упражнение 3.6 (схема Горнера). Убедитесь, что

$$f(\alpha)=a_0+\alpha\cdot\Bigl(a_1+\alpha\cdot\Bigl(a_2+\dots+\alpha\cdot\bigl(a_{n-2}+\alpha\cdot(a_{n-1}+\alpha\cdot a_n)\bigr)\cdots\Bigr)\Bigr)$$

Предложение 3.5
Пусть $\Bbbk$ — произвольное поле. Для любого набора многочленов $f_1, f_2, \dots, f_n \in \Bbbk[x]$ существует единственный приведённый многочлен $d \in \Bbbk[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i. Многочлен d представляется в виде

$$f_1 h_1 + f_2 h_2 + \dots + f_n h_n\,, \quad \text{где} \quad h_i \in \Bbbk[x]\,. \tag{3-11}$$

Произвольно взятый многочлен $g \in \Bbbk[x]$ представим в виде (3-11) тогда и только тогда, когда он делится на d.

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены.

Существование доказывается тем же рассуждением, что и в n° 2.4.2. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (3-11), через

$$(f_1, f_2, \dots, f_n) = \{f_1 h_1 + f_2 h_2 + \dots + f_n h_n \mid h_i \in \Bbbk[x]\}\,. \tag{3-12}$$

Это подкольцо в $\Bbbk[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg (с любым $h \in \Bbbk[x]$). Кроме того, $(f_1, f_2, \dots, f_n)$ содержит каждый из многочленов f_i, и все многочлены из $(f_1, f_2, \dots, f_n)$ делятся на любой общий делитель всех многочленов f_i. Возьмём в качестве d приведённый многочлен наименьшей степени в $(f_1, f_2, \dots, f_n)$. Остаток $r = g - qd$ от деления произвольного многочлена $g \in (f_1, f_2, \dots, f_n)$ на d лежит в $(f_1, f_2, \dots, f_n)$. Так как его степень не может быть строго меньше $\deg d$, он нулевой. Тем самым, все многочлены в $(f_1, f_2, \dots, f_n)$ делятся на d. □

Определение 3.2
Многочлен d из предл. 3.5 называется *наибольшим общим делителем* многочленов f_i и обозначается $\text{нод}(f_1, f_2, \dots, f_n)$.

3.2.1. Взаимная простота. Из предл. 3.5 вытекает, что в кольце $\Bbbk[x]$ многочленов с коэффициентами в поле *взаимная простота* многочленов $f_1, f_2, \dots, f_m$, т. е. возможность представить единицу в виде $1 = h_1 f_1 + h_2 f_2 + \dots + h_n f_n$, равносильна равенству $\text{нод}(f_1, f_2, \dots, f_n) = 1$, т. е. отсутствию у многочленов $f_1, f_2, \dots, f_n$ общих делителей положительной степени — точно так же, как это происходит в кольце целых чисел $\mathbb{Z}$.

Определение 3.3
Многочлен $f \in K[x]$ с коэффициентами в целостном[1] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 3.7. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: любой многочлен f является произведением конечного числа неприводимых многочленов, причём любые два таких представления $p_1 p_2 \cdots p_k = f = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\ i\ p_i = \lambda_i q_i$, где $\lambda_i \in \Bbbk$ — некоторые ненулевые константы.

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

Предложение 3.6 (китайская теорема об остатках)
Пусть $\Bbbk$ — произвольное поле, и многочлен $f \in \Bbbk[x]$ является произведением m сомножителей: $f = f_1 f_2 \cdots f_m$, таких что нод$(f_i, f_j) = 1 \ \forall\, i, j$. Отображение

$$\varphi : \Bbbk[x]/(f) \to \big(\Bbbk[x]/(f_1)\big) \times \big(\Bbbk[x]/(f_2)\big) \times \ \cdots \ \times \big(\Bbbk[x]/(f_m)\big)$$
$$\varphi : [g]_f \longmapsto \Big([g]_{f_1}, [g]_{f_2}, \ \dots\ , [g]_{f_m}\Big)$$

является корректно определённым изоморфизмом колец.

Доказательство. Проверки того, что φ корректно определён[1], является гомоморфизмом и имеет нулевое ядро, дословно повторяют рассуждения из n° 2.7, и мы оставляем их читателю. Покажем, что φ сюръективен. Для этого, как и в n° 2.7, построим для любого заданного набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f)$ многочлен $g \in \Bbbk[x]$, такой что $g \equiv r_i \pmod{f_i}$ при всех i. Для каждого i обозначим произведение всех сомножителей f_ν кроме f_i через

$$F_i = \prod_{\nu \neq i} f_\nu \,.$$

Поскольку f_i взаимно прост со всеми f_ν с $\nu \neq i$, он, согласно лем. 2.3, взаимно прост и с F_i, а значит, существует многочлен[2] $h_i \in \Bbbk[x]$, такой что

$$F_i \cdot h_i \equiv 1 \pmod{f_i}\,.$$

Итак, многочлен $g_i = F_i \cdot h_i \equiv 1 \pmod{f_i}$ и делится на все f_ν с $\nu \neq i$. Следовательно, $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m \equiv r_i \pmod{f_i}$ при всех i. □

3.2.2. **Алгоритм Евклида** из n° 2.2.2 дословно переносится на многочлены с коэффициентами в произвольном поле $\Bbbk$. А именно, для пары многочленов $f_1, f_2 \in \Bbbk[x]$ с $\deg(f_1) \geqslant \deg(f_2)$ положим $E_0 = f_1$, $E_1 = f_2$, $E_k =$ остатку от деления E_{k-2} на E_{k-1} при $k \geqslant 1$. Степени многочленов E_k строго убывают 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 $E_r =$ нод(f_1, f_2).

Упражнение 3.8. Докажите это.

Если при вычислении каждого E_k представлять его в виде $E_k = h_1^{(k)} f_1 + h_2^{(k)} f_2$, то $E_r = $ нод(f_1, f_2) и $E_{r+1} = 0$ тоже получатся представленными в таком виде, причём 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 3.9. Докажите это.

Вот как выглядит это вычисление для многочленов

$$f_1(x) = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \quad \text{и} \quad f_2(x) = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 \ :$$

[1] т. е. $\varphi\left([g]_f\right)$ не зависит от выбора представителя $g \in \Bbbk[x]$ в классе $[g]_f \subset \Bbbk[x]$

[2] 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

$$E_0 = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4$$
$$E_1 = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4$$
$$E_2 = -4x^4 - 13x^3 - 21x^2 - 10x - 8 = E_0 - \left(x^2 - 2x + 3\right) E_1$$

дальше делить на E_2 удобнее не E_1, а $16E_1$, а потом поделить результат на 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

$$E_4 = -16(x^2 + 3x + 4) = E_2 + 16\,(4x - 7)\,E_3 = 16\left(x^2 - 3\right)E_0 - 16\left(x^4 - 2x^3 + 2x - 2\right)E_1$$

поскольку $E_5 = E_3 + (x+2)\cdot E_4/256 = \left((x^3 + 2x^2 + x + 1)\cdot E_0 - (x^5 + x^2 + 1)\cdot E_1\right) = 0$. Откуда

$$\text{нод}(f_1, f_2) = x^2 + 3\,x + 4 = -\left(x^2 - 3\right)\,f_1(x) + \left(x^4 - 2\,x^3 + 2\,x - 2\right)\,f_2(x)$$
$$\text{нок}(f_1, f_2) = \left(x^3 + 2\,x^2 + x + 1\right)\,f_1(x) = \left(x^5 + x^2 + 1\right)\,f_2(x)\,.$$

3.3. Корни многочленов. Элемент $\alpha \in K$ называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в прим. 3.2, это условие равносильно тому, что $f(x)$ делится в $K[x]$ на $(x - \alpha)$.

Предложение 3.7
Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \alpha_2, \ldots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, если $f \neq 0$, то $\deg(f) \geqslant s$.

Доказательство. Так как в K нет делителей нуля и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в равенство $f(x) = (x - \alpha_1)\cdot q(x)$ значения $x = \alpha_2,\ \alpha_3,\ \ldots\ ,\ \alpha_s$, убеждаемся, что $\alpha_2,\ \alpha_3,\ \ldots\ ,\ \alpha_s$ являются корнями многочлена $q(x)$, и применяем индукцию. □

Следствие 3.2
Ненулевой многочлен f с коэффициентами из целостного кольца не может иметь в этом кольце более $\deg(f)$ различных корней.

Упражнение 3.10 (формула Лагранжа). Пусть $\Bbbk$ — поле, и $a_0, a_1, \ldots, a_n \in \Bbbk$ — любые $n + 1$ различных его элементов. Покажите, что для произвольного набора значений $b_0, b_1, \ldots, b_n \in \Bbbk$ существует единственный многочлен $f(x) \in \Bbbk[x]$ степени $\leqslant n$, такой что $f(a_i) = b_i$ при всех $i = 0,\ 1,\ \ldots\ n$.

Следствие 3.3
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. □

Упражнение 3.11. Пусть $\Bbbk$ — поле. Проверьте, что многочлен степени 2 или 3 неприводим в $\Bbbk[x]$ тогда и только тогда, когда у него нет корней в поле $\Bbbk$.

3.3.1. Общие корни нескольких многочленов. Пусть $\Bbbk$ — поле. Число α тогда и только тогда является общим корнем 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 по предл. 3.5 $(x-\alpha)$ делит нод$(f_1, f_2, \dots, f_m)$, и наоборот. Таким образом, отыскание общих корней набора многочленов сводится к отысканию корней их наибольшего общего делителя, что часто бывает проще, чем отыскание корней любого из f_i в отдельности, т. к. степень нод$(f_1, f_2, \dots, f_m)$ обычно меньше степени любого f_i.

Если многочлены $f_1, f_2, \dots, f_m \in \Bbbk[x]$ взаимно просты, то они не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$. В самом деле, поскольку существуют многочлены $h_i \in \Bbbk[x]$, такие что $f_1h_1 + f_2h_2 + \dots + f_mh_m = 1$, многочлены f_i не могут одновременно обратиться в нуль ни при каком значении x.

3.3.2. Кратные корни. Пусть $\Bbbk$ — произвольное поле. Число $\alpha \in \Bbbk$ называется m-кратным корнем многочлена $f \in \Bbbk[x]$, если $f(x) = (x-\alpha)^m \cdot g(x)$, где $g(\alpha) \neq 0$. Корни кратности $m \geqslant 2$ называются *кратными*.

Предложение 3.8
Для того, чтобы $\alpha \in \Bbbk$ был кратным корнем $f \in \Bbbk[x]$ необходимо и достаточно, чтобы $f(\alpha) = f'(\alpha) = 0$.

Доказательство. Если α — кратный корень многочлена f, то $f(x) = (x-\alpha)^2 g(x)$. Дифференцируя, получаем $f'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big)$, откуда $f'(\alpha) = 0$. Если α не является кратным корнем, то $f(x) = (x-\alpha)g(x)$, где $g(x) \neq 0$. Тогда $f'(x) = (x-\alpha)g'(x) + g(x)$ и $f'(\alpha) = g(\alpha) \neq 0$. □

Предложение 3.9
Если $\operatorname{char}\Bbbk = 0$, то $\alpha \in \Bbbk$ является m-кратным корнем многочлена $f \in \Bbbk[x]$ тогда и только тогда, когда α является корнем f и первых $(m-1)$ производных от f, но не является корнем m-той производной.

Доказательство. Если $f(x) = (x-\alpha)^m \cdot g(x)$ то $f'(x) = (x-\alpha)^{m-1} \cdot \big(m \cdot g(x) + (x-\alpha) \cdot g'(x)\big)$. При $g(\alpha) \neq 0$ второй сомножитель в этом равенстве отличен от нуля при $x = \alpha$. Поэтому α является m-кратным корнем f тогда и только тогда, когда α является $(m-1)$-кратным корнем f'. □

Предложение 3.10
Если $\operatorname{char}(\Bbbk) = p > 0$, то $f' = 0$ тогда и только тогда, когда $f = g^p$ для некоторого $g \in \Bbbk[x]$.

Доказательство. Согласно прим. 3.1, равенство $f' = 0$ равносильно тому, что $f(x) = g(x^p)$ для некоторого $g \in \Bbbk[x]$. Поскольку в характеристике p возведение в p-тую степень является гомоморфизмом (см. прим. 2.6), $g(x^p) = g(x)^p$. □

Следствие 3.4
Для произвольного поля $\Bbbk$ неприводимый многочлен $f \in \Bbbk[x]$ не имеет кратных корней ни в каком кольце $K \supset \Bbbk$.

Доказательство. Согласно предл. 3.10 производная неприводимого многочлена отлична от нуля над любым полем. Поскольку f неприводим, он взаимно прост с f'. В силу n° 3.3.1 у взаимно простых многочленов нет общих корней ни в каком кольце $K \supset \Bbbk$. □

3.3.3. Присоединение корней. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу $\mathbb{Z}/(n)$. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$ и обозначим через $(f) = \{fh \mid h \in \Bbbk[x]\}$ подкольцо всех многочленов, делящихся на f. Отношение $g_1 \equiv g_2 \pmod f$, означающее по определению, что $g_1 - g_2 \in (f)$, является отношением эквивалентности и разбивает $\Bbbk[x]$ в объединение непересекающихся классов $[g]_f = g + (f) = \{g + fh \mid h \in \Bbbk[x]\}$, которые называются *классами вычетов* по модулю f. Сложение и умножение этих классов задаётся формулами

$$[g] + [h] \stackrel{\text{def}}{=} [g+h]\,, \quad [g]\cdot[h] \stackrel{\text{def}}{=} [gh]\,. \tag{3-13}$$

Упражнение 3.12. Проверьте корректность[1] этого определения, 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 $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$ гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому для классов чисел $c \in \Bbbk$ мы всюду далее пишем c вместо $[c]_f$.

Упражнение 3.13. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Так как 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 $\deg(r) < \deg(f)$. Тем самым, каждый класс *однозначно* записывается как

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

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

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

Поэтому сложение и умножение классов по правилам (3-13) можно интерпретировать как формальное сложение и умножение записей

$$a_0 + a_1\vartheta + \ \cdots\ + a_{n-1}\vartheta^{n-1}\,, \tag{3-14}$$

по стандартным правилам раскрытия скобок и приведения подобных с учётом того, что символ ϑ удовлетворяет соотношению $f(\vartheta) = 0$. По этой причине кольцо $\Bbbk[x]/(f)$ часто обозначают через $\Bbbk[\vartheta] : f(\vartheta) = 0$ и называют *расширением* поля $\Bbbk$ посредством *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$.

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

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

Упражнение 3.14. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$.

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

Предложение 3.11
Пусть $\Bbbk$ — произвольное поле. 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 для любого $g \notin (f)$ $\text{нод}(f, g) = 1$, а значит, $fh + gq = 1$ для некоторых $h, q \in \Bbbk[x]$, откуда $[q] \cdot [g] = [1]$ в $\Bbbk[x]/(f)$. □

Упражнение 3.15. Напишите явную формулу для вычисления обратного элемента к числу $a_0 + a_1\vartheta$ в поле $\mathbb{Q}(\vartheta)$ с $\vartheta^2 + \vartheta + 1 = 0$.

Теорема 3.1
Для любого поля $\Bbbk$ и любого многочлена $f \in \Bbbk[x]$ существует такое поле $\mathbb{F} \supset \Bbbk$, что f разлагается в $\mathbb{F}[x]$ в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\Bbbk$ и для всех многочленов степени $< n$ из $\Bbbk[x]$ мы умеем строить такое поле[1]. Если f приводим: $f = gh$, где $\deg g < n$ и $\deg h < n$, мы можем построить поле $\mathbb{F}' \supset \Bbbk$ над которым g полностью разложится на линейные множители, а затем поле $\mathbb{F} \supset \mathbb{F}'$ над которым разложится h, а тем самым, и f. Если f неприводим, рассмотрим поле $\mathbb{F}' = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ в качестве классов констант, и многочлен f делится в $\mathbb{F}'[x]$ на $(x - \vartheta)$, где $\vartheta = [x] \pmod f$. Частное от этого деления имеет степень $n-1$ и по индукции раскладывается на линейные множители над некоторым полем $\mathbb{F} \supset \mathbb{F}'$. Тогда и f полностью разложится над $\mathbb{F}'$. □

3.4. Поле комплексных чисел $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2 + 1)$ является расширением поля $\mathbb{R}$ при помощи корня квадратного уравнения $x^2 + 1 = 0$ и состоит из классов $[x + yt] = x + y \cdot i$, где $x, y \in \mathbb{R}$ и $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2 = -1$. Поскольку многочлен $t^2 + 1$ не имеет вещественных корней, он неприводим в $\mathbb{R}[t]$, так что $\mathbb{C}$ действительно является полем: если $x + yi \neq 0$, то

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

Удобно изображать комплексное число $z = x + yi$ *радиус-вектором*, ведущим из начала координат $= (0, 0)$ в точку $z = (x, y)$ на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат XOY (см. рис. 3⋄1). Координаты (x, y) называются при этом *действительной* и *мнимой* частями числа комплексного числа $z \in \mathbb{C}$ и обозначаются через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ соответственно. Длина радиус вектора $|z| = \sqrt{x^2 + y^2}$ называется *модулем* (или *абсолютной величиной*) комплексного числа z. Множество всех $\vartheta \in \mathbb{R}$, таких что поворот плоскости $\mathbb{C}$ вокруг нуля на угол ϑ совмещает координатный луч OX с лучом, идущим в направлении радиус вектора z, называется *аргументом* числа z и обозначается

$$\mathrm{Arg}(z) = \{\varphi + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}\,,$$

[1] заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \Bbbk$

где φ — ориентированная длина дуги[1], идущей по единичной окружности из точки $(1,0)$ в точку $z/|z|$ (ср. с n° 1.6.1). Таким образом, $z = x + yi \in \mathbb{C}$ имеет $\mathrm{Re}(z) = |z| \cdot \cos\varphi$, $\mathrm{Im}(z) = |z| \cdot \sin\varphi$ и может быть записан как $z = |z| \cdot (\cos\varphi + i \cdot \sin\varphi i)$, где $\vartheta \in \mathrm{Arg}(z)$.

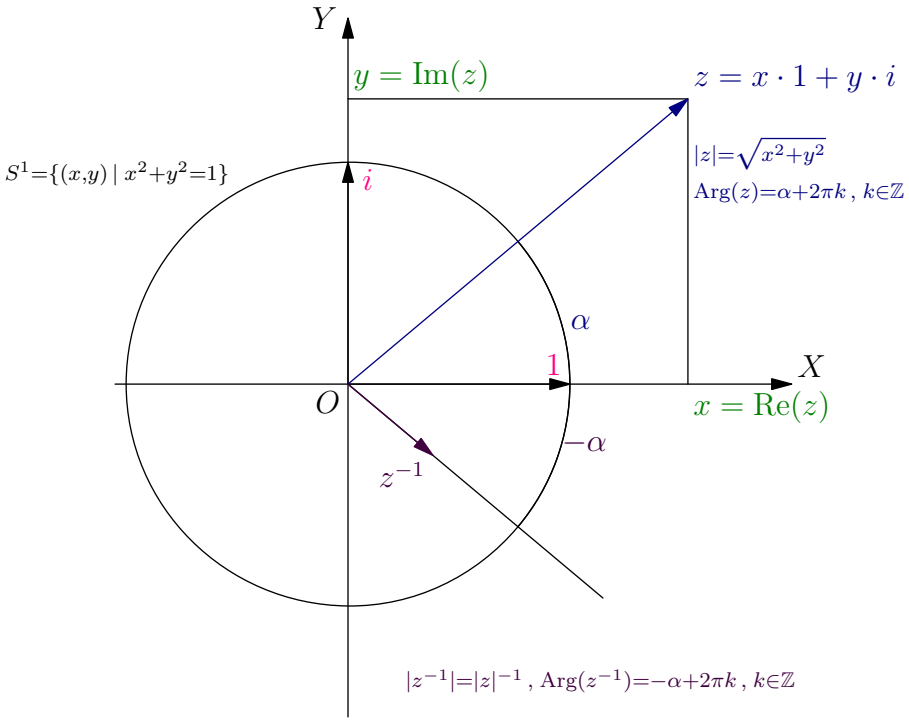


Рис. 3⋄1.

Лемма 3.1
Множество радиус-векторов точек z декартовой координатной плоскости $\mathbb{R}^2$ с операцией сложения векторов и операцией умножения, заданной правилами[2]

$$|z_1 z_2| \stackrel{\text{def}}{=} |z_1| \cdot |z_2| \tag{3-15}$$

$$\mathrm{Arg}(z_1 z_2) \stackrel{\text{def}}{=} \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2) = \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \mathrm{Arg}(z_1),\ \vartheta_2 \in \mathrm{Arg}(z_2)\} \tag{3-16}$$

образует поле, изоморфное полю $\mathbb{C}$. Изоморфизм сопоставляет числу $x + iy \in \mathbb{C}$ точку $z = (x, y) \in \mathbb{R}^2$.

Упражнение 3.16. Проверьте, что сложение аргументов (3-16) определено корректно.

Доказательство лем. 3.1. Векторы на плоскости образуют абелеву группу по сложению, а ненулевые векторы — абелеву группу относительно операции умножения, задаваемой правилами (3-15) и (3-16): единицей служит единичный направляющий вектор оси OX, а обратным к ненулевому вектору z является вектор z^{-1} с

$$|z^{-1}| = 1/|z|\,, \quad \mathrm{Arg}(z^{-1}) = -\mathrm{Arg}(z) \tag{3-17}$$

[1] отметим, что таких дуг имеется бесконечно много, но все они отличаются друг от друга на целое число оборотов; эпитет «ориентированная» означает, что длину следует брать со знаком «+», если движение происходит против часовой стрелки, и со знаком «−», если по часовой стрелке

[2] иначе говоря, при умножении комплексных чисел их модули перемножаются, а аргументы складываются

(см. рис. 3◇1). Для проверки дистрибутивности заметим, что отображение $\lambda_a : z \mapsto az$ умножения на фиксированный вектор a представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b+c) = ab + ac$ означает, что поворотная гомотетия перестановочна со сложением векторов: $\lambda_a(b+c) = \lambda_a(b)+\lambda_a(c)$. Это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы.

Таким образом векторы образуют поле. Векторы, параллельные прямой OX образут в нём подполе, изоморфное полю $\mathbb{R}$. Произвольный вектор $z = (x, y)$ записывается в виде $z = x + iy$, где i — единичный направляющий вектор оси OY, $x, y \in \mathbb{R}$ понимаются как точки оси OX, а сложение и умножение происходят по правилам из условия леммы. При этом $i^2 = -1$ и для любых векторов $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$

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

что полностью согласуется с умножением классов вычетов $[x + yt]$ в $\mathbb{R}[t]/(t^2 + 1)$. □

3.4.1. Сопряжение. Число $\overline{z} \stackrel{\text{def}}{=} x - iy$ 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 $z \mapsto \overline{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси OX. С алгебраической точки зрения сопряжение является инволютивным[2] автоморфизмом поля $\mathbb{C}$, т. е. $\forall\, z \in \mathbb{C}\ \ \overline{\overline{z}} = z$ и $\forall\ z_1, z_2 \in \mathbb{C}\ \ \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$ и $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$.

3.4.2. Тригонометрия. Большая часть школьной тригонометрии представляет собою не самую удобную для восприятия запись заурядных вычислений с комплексными числами z, лежащими на единичной окружности. Например, произведение $z_1 z_2$ двух таких чисел

$$z_1 = \cos\varphi_1 + i\sin\varphi_1 \quad \text{и} \quad z_2 = \cos\varphi_2 + i\sin\varphi_2$$

по лем. 3.1 равно $\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)$. С другой стороны,

$$z_1 z_2 = \Big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2\Big) + i\Big(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2\Big),$$

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, мы *доказали* тригонометрические формулы сложения аргументов.

Пример 3.3 (тригонометрические функции кратных углов)
По лем. 3.1 $z = \cos\varphi + i\sin\varphi$ имеет $z^n = \cos(n\varphi) + i\sin(n\varphi)$. Раскрывая в $(\cos\varphi + i\sin\varphi)^n$

[1] *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)

[2] отличный от тождественного эндоморфизм $\iota : X \to X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \mathrm{Id}_X$; по предл. 1.4 на стр. 14 всякая инволюция автоматически биективна

скобки по форм. (1-9) на стр. 8, получаем равенство

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

заключающее в себе сразу *все* мыслимые формулы для кратных углов:

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

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

Упражнение 3.17. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

3.4.3. Корни из единицы и круговые многочлены. Решим в поле $\mathbb{C}$ уравнение

$$z^n = 1\,.$$

Сравнивая модули левой и правой части, получаем $|z^n| = |z|^n = 1$, откуда $|z| = 1$. Сравнивая аргументы, получаем $n\operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k\in\mathbb{Z}\}$. Поскольку

$$n\varphi \in \{2\pi k \mid k\in\mathbb{Z}\} \quad\Longleftrightarrow\quad \varphi \in \{2\pi k/n \mid k\in\mathbb{Z}\}\,,$$

имеется ровно n различных классов эквивалентности вещественных чисел по модулю добавления целых кратных 2π, которые при умножении их представителей на n превращаются в класс $\{2\pi k \mid k\in\mathbb{Z}\}$. Это классы n геометрически различных углов $2\pi k/n$ с $0\leqslant k\leqslant n-1$. Таким образом, уравнение $z^n = 1$ имеет ровно n корней

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

расположенных в вершинах правильного n-угольника, вписанного в единичную окружность так, что вершина ζ_0 находится в точке 1 (см. рис. 3⋄2). Они образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-той степени из* единицы[1].

Корень $\zeta\in\boldsymbol{\mu}_n$ называются *первообразным корнем* степени n из единицы, если все остальные элементы группы $\boldsymbol{\mu}_n$ представляются в виде ζ^k с $k\in\mathbb{N}$. Например, корень с наименьшим положительным аргументом $\zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$ является первообразным. Но есть и другие: скажем, на рис. 3⋄2 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, а в группе $\boldsymbol{\mu}_6$ на рис. 3⋄3 на стр. 44 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1}$.

Упражнение 3.18. Покажите, что корень $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ является первообразным тогда и только тогда, когда $\text{нод}(k,n) = 1$.

[1] фактически мы уже встречались с ней в n° 1.6.1, где эта группа называлась *циклической группой порядка n*

Приведённый многочлен, имеющий корнями все первообразные корни степени n из единицы и только их

$$\Phi_n(z) = \prod_{\substack{1\leqslant k<n\,:\\ \text{нод}(k,n)=1}} (z - z_1^k)\,, \tag{3-18}$$

называется n-тым *круговым* (или *циклотомическим*) многочленом.

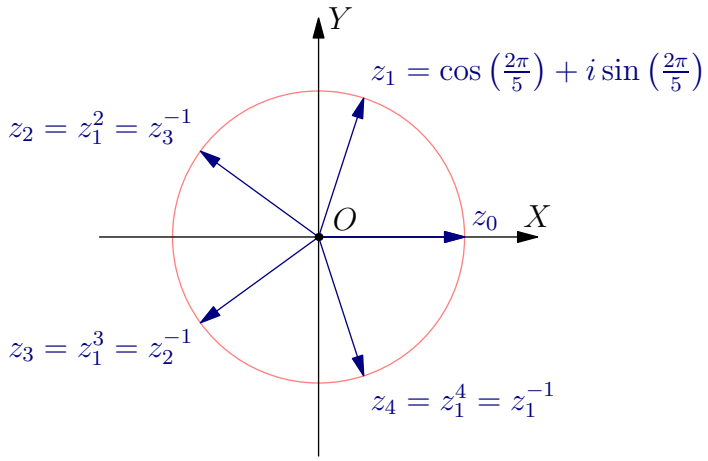


Рис. 3⋄2. Корни уравнения $z^5 = 1$.

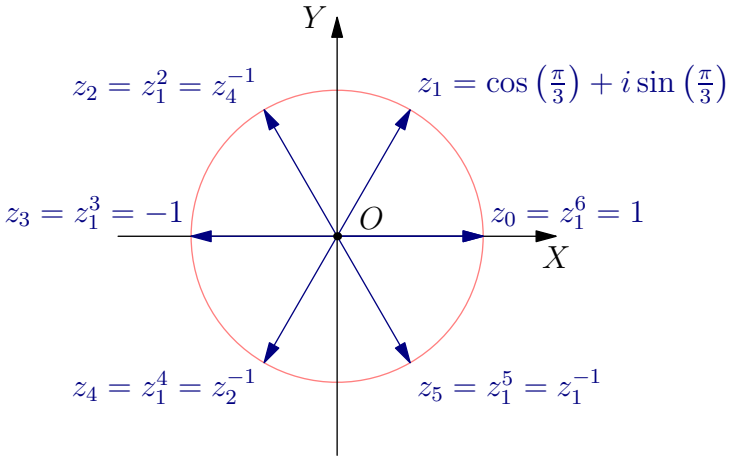


Рис. 3⋄3. Корни уравнения $z^6 = 1$.

Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4) = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z - z_1)(z - z_4) = z^2 - z + 1\,.$$

Упражнение 3.19*. Покажите, что $\forall\, n\ \Phi_n \in \mathbb{Z}[x]$ и *неприводим*[1] в $\mathbb{Q}[x]$.

[1] т. е. не являются произведениями многочленов строго меньшей степени

Пример 3.4 (уравнение $z^n = a$)
Корни уравнения $z^n = a$ это числа $z = |z| \cdot (\cos\varphi + i\sin\varphi)$ с $|z|^n = |a|$, а $n\varphi \in \operatorname{Arg}(a)$. При $a = |a| \cdot (\cos\alpha + i\sin\alpha) \neq 0$ имеется ровно n таких чисел

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

Они 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.

Пример 3.5 (гауссовы числа)
Рассмотрим в $\mathbb{C}$ подкольцо, состоящее из всех чисел с целыми координатами

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

Оно называется кольцом *гауссовых целых чисел* и часто используется в арифметике. Например, классическая задача о представлении натурального числа в виде суммы двух квадратов целых чисел существенно проясняется расширением кольца $\mathbb{Z}$ до кольца $\mathbb{Z}[i]$, в котором $x^2 + y^2 = (x+iy)(x-iy)$, так что разрешимость в кольце $\mathbb{Z}$ уравнения $x^2 + y^2 = n$ равносильна разрешимости в кольце $\mathbb{Z}[i]$ уравнения $n = z \cdot \overline{z}$. Из второго уравнения сразу же видно, что если числа m_1 и m_2 представляются в виде суммы двух квадратов

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

то их произведение $m = m_1 m_2$ также является суммой двух квадратов:

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

(это соотношение известно как *тождество Эйлера*). В сочетании с теоремой о единственности разложения на простые множители в кольце $\mathbb{Z}[i]$, которую мы докажем в §5, тождество Эйлера сводит вопрос о представимости произвольного натурального числа в виде суммы двух квадратов к анализу представимости простых чисел. Мы ещё вернёмся к этому в прим. 5.5 на стр. 78.

Упражнение 3.20. Покажите, что обратимыми элементами кольца $\mathbb{Z}[i]$ являются четыре числа: ± 1 и $\pm i$.

3.5. Конечные поля. Для конечного поля $\mathbb{F}_p = \mathbb{Z}/(p)$ из p элементов и неприводимого многочлена $f \in \mathbb{F}_p[x]$ степени n поле вычетов $\mathbb{F}_p[x]/(f)$ состоит из p^n элементов вида

$$a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}\,, \quad \text{где} \quad a_i \in \mathbb{F}_p \quad \text{и} \quad f(\vartheta) = 0\,.$$

Например, $x^2 + x + 1 \in \mathbb{F}_2[x]$ неприводим, поскольку не имеет корней в $\mathbb{F}_2$. Соответствующее поле $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \mathbb{F}_2[\omega] : \omega^2 + \omega + 1 = 0$ состоит из четырёх элементов[1]: $0\,,\ 1\,,\ \omega = x \pmod{x^2+x+1}$ и $1 + \omega = \omega^2 = \omega^{-1}$.

Упражнение 3.21. Убедитесь, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

[1] отметим, что в силу равенства $-1 = 1$ в поле $\mathbb{F}_2$ можно обходиться без «минусов»

Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ аналогично расширению $\mathbb{R} \subset \mathbb{C} \simeq \mathbb{R}[\omega] : \omega^2 + \omega + 1 = 0$, получающемуся присоединением к полю $\mathbb{R}$ первообразного комплексного кубического корня из единицы[1]. Аналогом комплексного сопряжения, переводящего ω в $\overline{\omega} = \omega^2$, в поле $\mathbb{F}_4$ является гомоморфизм Фробениуса[2] $F_2 : \mathbb{F}_4 \to \mathbb{F}_4$, $a \mapsto a^2$, который тождественно действует на простом подполе $\mathbb{F}_2 = \{0, 1\}$ и переводит корни многочлена $x^2 + x + 1$ друг в друга.

Рассмотрим ещё один пример. Многочлен $x^2 + 1 \in \mathbb{F}_3[x]$ не имеет корней в $\mathbb{F}_3$, и значит, неприводим. Соответствующее поле $\mathbb{F}_9 = \mathbb{F}_3[i]$ состоит из девяти элементов $a + bi$ где $a, b \in \{-1, 0, 1\} = \mathbb{F}_3$, а $i^2 = -1$. Автоморфизм Фробениуса $F_3 : a \mapsto a^3$ переводит элемент $a + bi$ в $a - bi$.

Упражнение 3.22. Составьте для поля $\mathbb{F}_9$ таблицу умножения и таблицу обратных элементов, перечислите все имеющиеся в $\mathbb{F}_9$ квадраты и кубы и выясните, не изоморфна ли мультипликативная группа $\mathbb{F}_9^*$ группе $\boldsymbol{\mu}_8$.

Теорема 3.2
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ существует конечное поле $\mathbb{F}_q$, состоящее из $q = p^n$ элементов.

Доказательство. Рассмотрим в $\mathbb{F}_p[x]$ многочлен $f(x) = x^q - x$. По теор. 3.1 существует такое поле $\mathbb{F} \supset \mathbb{F}_p$, что f полностью раскладывается в $\mathbb{F}[x]$ в произведение q линейных множителей. Поскольку производная $f'(x) \equiv 1$, все эти множители различны, т. е. в поле $\mathbb{F}$ имеется ровно q различных чисел α, таких что $\alpha^q = \alpha$. Они образуют поле: если $\alpha^q = \alpha$, то $(-\alpha)^q = -\alpha$ и $\left(\alpha^{-1}\right)^q = \alpha^{-1}$, и для любого $\beta = \beta^q$ имеем $\alpha\beta = \alpha^q\beta^q = (\alpha\beta)^q$ и

$$\alpha + \beta = \alpha^{p^n} + \beta^{p^n} = F_p^n(\alpha) + F_p^n(\beta) = F_p^n(\alpha + \beta) = (\alpha + \beta)^q,$$

где $F_p : \mathbb{F} \to \mathbb{F}$, $x \mapsto x^p$, это гомоморфизм Фробениуса. □

Упражнение 3.23. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

3.5.1. Конечные мультипликативные подгруппы в поле. Рассмотрим абелеву группу A, операцию в которой будем записывать мультипликативно.

Группа A называется *циклической*, если в ней имеется элемент $a \in A$, такой что все элементы группы A представляются в виде a^n с некоторым $n \in \mathbb{Z}$. Всякий элемент $a \in A$, обладающий этим свойством, называется *образующей* циклической группы A.

Например, группа комплексных корней из единицы $\boldsymbol{\mu}_n \subset \mathbb{C}$, рассматривавшаяся нами в n° 3.4.3, является циклической, а её образующими являются первообразные корни.

Если группа A конечна, то среди степеней любого элемента $b \in A$ будут встречаться одинаковые, скажем $b^k = b^m$ с $k > m$. Домножая обе части этого равенства на b^{-m}, получаем равенство $b^{k-m} = 1$. Таким образом, для каждого элемента $b \in A$ существует показатель $m \in \mathbb{N}$, такой что $b^m = 1$. Наименьший такой показатель называется *порядком* элемента b и обозначается $\operatorname{ord} b$.

Если $\operatorname{ord} b = n$, то элементы $b^0 = 1$, $b^1 = b$, b^2, …, b^{n-1} попарно различны, и любая целая степень b^m совпадает с одним из них: если $m = nq + r$, где r — остаток от деления m на n, то $b^m = (b^n)^q b^r = b^r$.

[1] т. е. комплексного корня того же самого многочлена $x^2 + x + 1$

[2] см. n° 2.8.2 на стр. 29

Предложение 3.12
Любая конечная подгруппа A в мультипликативной группе $\Bbbk^*$ произвольного поля $\Bbbk$ является циклической.

Доказательство. Обозначим через m максимальный из порядков элементов группы A. Достаточно убедиться, что порядок любого элемента группы A делит m: тогда все элементы группы A будут корнями многочлена $x^m - 1 = 0$, а значит, их не более m и все они исчерпываются степенями имеющегося в A элемента m-того порядка.

Чтобы увидеть, что порядки всех элементов группы являются делителями максимального порядка, достаточно для любых двух элементов $b_1, b_2 \in A$, имеющих порядки m_1, m_2, построить элемент $b \in A$, порядок которого равен нок(m_1, m_2).

Упражнение 3.24. Покажите, что при 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 согласно упр. 2.8 в произведение простых чисел, мы можем представить нок(m_1, m_2) в виде произведения $\ell_1 \ell_2$ так, что $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ и нод$(\ell_1, \ell_2) = 1$.

Упражнение 3.25. Убедитесь в этом.

Элементы $b_1' = b_1^{k_1}$ и $b_2' = b_2^{k_2}$ имеют взаимно простые порядки ℓ_1 и ℓ_2, а их произведение $b_1' b_2'$ по упр. 3.24 имеет порядок $\ell_1 \ell_2 =$ нок(m_1, m_2), что и требовалось. □

Теорема 3.3
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 3.2.

Доказательство. Если $\operatorname{char} \mathbb{F} = p$, то по упр. 3.23 поле $\mathbb{F}$ состоит из $q = p^n$ элементов (для подходящего $n \in \mathbb{N}$), а его ненулевые элементы образуют по предл. 3.12 циклическую группу по умножению, порождённую некоторым элементом $\zeta \in \mathbb{F}^*$, так что

$$\mathbb{F} = \{0,\ 1,\ \zeta,\ \zeta^2,\ \dots,\ \zeta^{q-2}\}.$$

Мы построим сейчас ещё одно поле из q элементов, которое будет изоморфно как полю $\mathbb{F}$, так и полю $\mathbb{F}_q$ из теор. 3.2.

Обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен наименьшей степени, такой что $g(\zeta) = 0$. Тогда правило $h(x) \pmod g \mapsto h(\zeta)$ корректно определяет сюръективный гомоморфизм колец $\mathrm{ev}_\zeta : \mathbb{F}_p[x]/(g) \twoheadrightarrow \mathbb{F}$.

Упражнение 3.26. Покажите, что g неприводим в $\mathbb{F}_p[x]$ и нацело делит любой многочлен $f \in \mathbb{F}_p[x]$, для которого $f(\zeta) = 0$.

Из упражнения вытекает, что кольцо вычетов $\mathbb{F}_p[x]/(g)$ является полем. Поэтому гомоморфизм ev_ζ инъективен и $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$.

С другой стороны, поскольку ζ является корнем многочлена $f(x) = x^q - x$, из упр. 3.26 вытекает, что $f = gu$ для некоторого $u \in \mathbb{F}_p[x]$. Подставляя в это равенство q элементов поля $\mathbb{F}_q$, построенного в теор. 3.2 и состоящего в точности из q корней многочлена f, заключаем, что хотя бы один из них — назовём его $\xi \in \mathbb{F}_q$ — является корнем и для g. Тогда правило $h(x) \pmod g \mapsto h(\xi)$ корректно задаёт вложение полей $\mathrm{ev}_\xi : \mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

3.5.2. Квадратичные вычеты. Зафиксируем целое простое $p > 2$. Ненулевые элементы поля $\mathbb{F}_p$, являющиеся квадратами, называются *квадратичными вычетами* по модулю p. Они образуют мультипликативную подгруппу в $\mathbb{F}_p^*$ — образ мультипликативного гомоморфизма $\mathbb{F}_p^* \to \mathbb{F}_p^*$ возведения в квадрат $x \mapsto x^2$. Ядро этого гомоморфизма состоит из двух элементов, поскольку уравнение $x^2 = 1$ имеет в поле $\mathbb{F}_p$ ровно два корня $x = \pm 1$. Тем самым, квадратичных вычетов имеется ровно $(p-1)/2$.

Судить о том, является ли данный элемент $a \in \mathbb{F}_p^*$ квадратом, можно при помощи малой теоремы Ферма[1], согласно которой $a^{p-1} = 1$ для любого $a \in \mathbb{F}_p^*$. Если $b = a^2$, то $b^{(p-1)/2} = a^{p-1} = 1$. Мультипликативный гомоморфизм

$$\mathbb{F}_p^* \to \mathbb{F}_p^*, \quad x \mapsto x^{(p-1)/2} \tag{3-19}$$

нетривиален, т. к. уравнение $x^{(p-1)/2} = 1$ имеет не более $(p-1)/2 < p-1$ корней в поле $\mathbb{F}_p$. Поскольку образ гомоморфизма (3-19) содержится среди корней всё того же уравнения $x^2 = 1$, он состоит в точности из двух элементов ± 1. Тем самым, ядро гомоморфизма (3-19) в точности совпадает с подгруппой квадратов, т. е. $a \in \mathbb{F}_p^*$ является квадратом тогда и только тогда, когда $a^{(p-1)/2} = 1$. Например, -1 является квадратом в $\mathbb{F}_p$ в точности тогда, когда $(p-1)/2$ чётно.

Для произвольного $n \in \mathbb{N}$ и простого $p > 2$ число

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} [n]_p^{(p-1)/2} = \begin{cases} 1 & \text{когда } n \text{ ненулевой квадрат по модулю } p \\ 0 & \text{когда } n \vdots p \\ -1 & \text{когда } n \text{ не является квадратом по модулю } p \end{cases} \tag{3-20}$$

называется *символом Лежандра – Якоби*. Из определения очевидно, что он зависит только от класса $[n]_p \in \mathbb{Z}/(p)$ и мультипликативен по n:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Упражнение 3.27*. Покажите, что для простого $p > 2$ символ $\left(\frac{2}{p}\right) = 1$ тогда и только тогда, когда $p \equiv \pm 1 \pmod 8$.

В общем случае символ Лежандра – Якоби легко вычисляется благодаря следующей замечательной теореме, открытой Гауссом.

Теорема 3.4 (квадратичный закон взаимности)
Для любых простых $p, q > 2$ $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Два доказательства этой теоремы, предложенные Эйзенштейном и Золотарёвым, намечены в задачах из необязательного листка № 3½. Вот пример того, как она работает:

$$\left(\frac{57}{179}\right) = \left(\frac{179}{57}\right) = \left(\frac{8}{57}\right) = \left(\frac{2}{57}\right)^3 = 1,$$

т. е. 57 это квадрат по модулю 179.

[1] см. сл. 2.1 на стр. 23

§4. Рациональные функции и степенные ряды

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

4.1. Кольца частных. Конструкция, изготавливающая поле $\mathbb{Q}$ из кольца $\mathbb{Z}$ как множество дробей с целым числителем и целым ненулевым знаменателем[1], имеет смысл в любом коммутативном кольце K с единицей.

Будем называть подмножество $S \subset K$ *мультипликативным*, если $1 \in S$, $0 \notin S$ и $st \in S$ для любых $s, t \in S$.

Например, если элемент $q \in K$ не является нильпотентным, то множество всех его целых неотрицательных степеней q^k мультипликативно[2].

Множество $K^\circ \subset K$, состоящее из всех ненулевых элементов, которые не являются делителями нуля, также мультипликативно. В частности, множество всех ненулевых элементов любого целостного кольца мультипликативно.

Свяжем с каждым мультипликативным подмножеством $S \subset K$ наименьшее отношение эквивалентности $\underset{S}{\sim}$ на множестве упорядоченных пар $K \times S$, содержащее все эквивалентности вида $(a, t) \sim (as, ts)$ с произвольными $s \in S$. Будем называть полученные классы эквивалентности *дробями со знаменателями из* S и обозначать $a\,/\,s$. Множество всех дробей со знаменателями в S обозначим KS^{-1} или $K[S^{-1}]$ и назовём *кольцом частных* (или *локализацией*) кольца K со знаменателями в S.

Лемма 4.1
$a/r = b/t$ в $KS^{-1} \iff \exists\, s \in S : ats = brs$ в K.

Доказательство. Будем писать $(a, r) \approx (b, t)$, если $\exists\, s \in S : (at - br)s = 0$ в K. В этом случае двухшаговая цепочка элементарных отождествлений $(a, r) \sim (ats, rts) = (brs, rts) \sim (b, t)$ показывает, что отношение $\approx$ содержится в отношении $\underset{S}{\sim}$. Остаётся убедиться, что $\approx$ является отношением эквивалентности — тогда оно совпадёт с $\underset{S}{\sim}$ в виду минимальности последнего. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a, r) \approx (b, t)$ и $(b, t) \approx (c, u)$, т. е. существуют такие $s_1, s_2 \in S$, что $ats_1 = brs_1$ и $bus_2 = cts_2$. Тогда $au(ts_1s_2) = brus_1s_2 = cr(ts_1s_2)$, т. е. $(a, r) \approx (c, u)$. □

Лемма 4.2
Операции $\frac{a}{r} + \frac{b}{s} \stackrel{\text{def}}{=} \frac{as+br}{rs}$ и $\frac{a}{r} \cdot \frac{b}{s} \stackrel{\text{def}}{=} \frac{ab}{rs}$ корректно задают на KS^{-1} структуру коммутативного кольца с единицей $1/1$ и нулём $0/1$.

Доказательство. Поскольку всякое отношение $\underset{S}{\sim}$ представляет собой одно- или двушаговую цепочку элементарных отождествлений $(a, r) \sim (au, ru)$ достаточно проверить, что результаты операций не меняются при замене $\frac{a}{r}$ на $\frac{au}{ru}$, а $\frac{b}{s}$ — на $\frac{bw}{sw}$,:

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

[1] см. прим. 1.5 на стр. 12 и прим. 2.2 на стр. 17

[2] мы по определению полагаем $q^0 = 1$

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

Теорема 4.1
Отображение $\iota_S : K \to KS^{-1}$, переводящее $a \in K$ в дробь $a/1$, является гомоморфизмом колец, причём $\iota_S(s)$ обратим в KS^{-1} для любого $s \in S$, и $\ker \iota = \{a \in K \mid \exists\, s \in S : as = 0\}$. Для любого гомоморфизма $\varphi : K \to R$ в целостное кольцо R, такого что $\varphi(s)$ обратим в R для всех $s \in S$, существует единственный гомоморфизм колец $\varphi_S : KS^{-1} \to R$, такой что $\varphi = \varphi_S \circ \iota$.

Доказательство. Гомоморфность ι очевидна. Обратной к дроби $\iota(s) = s/1$ является дробь $1/s$. Дробь $\iota(a) = a/1$ равна $0/1$ тогда и только тогда, когда найдётся $s \in S$, такой что $a \cdot 1 \cdot s = 0 \cdot 1 \cdot s = 0$. Докажем последнее утверждение. Чтобы продолжить гомоморфизм $\varphi : K \to R$ до гомоморфизма $\varphi_S : KS^{-1} \to R$, у нас нет иного выбора как положить $\varphi_S(1/s) = 1/\varphi(s)$, поскольку должны выполняться равенства $\varphi_S(1/s) \cdot \varphi(s) = \varphi_S\big(s \cdot (1/s)\big) = \varphi_S(1) = 1$. Тем самым, продолжение обязано задаваться формулой $\varphi_S(a/r) \stackrel{\text{def}}{=} \varphi(a) \cdot \frac{1}{\varphi(r)}$. Остаётся проверить, что она корректна и задаёт гомоморфизм. Заменяя $\frac{a}{r}$ на $\frac{as}{rs}$, получаем

$$\varphi_S\left(\frac{as}{rs}\right) = \frac{\varphi(as)}{\varphi(rs)} = \frac{\varphi(a)\,\varphi(s)}{\varphi(r)\,\varphi(s)} = \frac{\varphi(a)}{\varphi(r)}\,.$$

Аналогично проверяется, что φ_S перестановочен со сложением и умножением. □

Замечание 4.1. Кольцо KS^{-1} и гомоморфизм $\iota_S : K \to KS^{-1}$ определяются последним свойством из теор. 4.1 однозначно с точностью до единственного изоморфизма в следующем точном смысле. Пусть гомоморфизм $\iota' : K \to F$ делает все элементы из S обратимыми в F и обладает универсальным свойством из теор. 4.1: для любого гомоморфизма $\varphi : K \to R$ в целостное кольцо R, делающего все элементы из S обратимыми в R, существует единственный гомоморфизм колец $\varphi'_S : F \to R$, такой что $\varphi = \varphi'_S \circ \iota'$. Тогда существует единственный изоморфизм $\psi : KS^{-1} \xrightarrow{\sim} F$, такой что $\iota' = \psi \circ \iota$.

Действительно, 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 $\iota = \psi' \circ \iota'$. Композиция $\psi' \circ \psi$ доставляет разложение самого гомоморфизма ι в виде $\iota = \psi' \circ \psi \circ \iota$. Поскольку одновременно $\iota = \mathrm{Id}_{KS^{-1}} \circ \iota$, из единственности такого представления вытекает, что $\psi' \circ \psi = \mathrm{Id}_{KS^{-1}}$. По той же причине $\psi \circ \psi' = \mathrm{Id}_F$. Таким образом, ψ' и ψ являются взаимно обратными изоморфизмами.

Замечание 4.2. Если в определении мультипликативной системы отбросить требование $0 \notin S$, то всё сказанное выше не утратит формального смысла: эквивалентность $\underset{S}{\sim}$ и кольцо KS^{-1} будут по-прежнему определены, а лем. 4.1, лем. 4.2 и теор. 4.1 (как и их доказательства) останутся в силе. Однако, если $0 \in S$, кольцо KS^{-1} получится нулевым: все дроби a/s будут эквивалентны дроби $0/1 = 0$.

Упражнение 4.1. Убедитесь в этом.

4.1.1. Поле частных целостного кольца. Если кольцо K не имеет делителей нуля, его ненулевые элементы образуют мультипликативную систему. Кольцо частных со знаменателями в этой системе называется *полем частных* целостного кольца K и обозначается Q_K.

Упражнение 4.2. Проверьте, что это действительно поле.

Гомоморфизм $\iota : K \hookrightarrow Q_K$, переводящий $a \in K$ в $a/1 \in Q_K$ в этом случае инъективен, и для любого гомоморфизма $\varphi : K \to R$ в целостное кольцо R, переводящего все ненулевые элементы K в обратимые элементы R, единственным способом продолжается до инъективного гомоморфизма $\widetilde{\varphi} : Q_K \hookrightarrow R$.

Пример 4.1 (поле $\mathbb{Q}$)
Полем частных целостного кольца $\mathbb{Z}$ является поле рациональных чисел $\mathbb{Q} = Q_{\mathbb{Z}}$, которое канонически вкладывается в любое поле характеристики нуль в качестве простого подполя (ср. с n° 2.8.1).

Пример 4.2 (поле рядов Лорана)
Поле частных целостного кольца формальных степенных рядов $\Bbbk[\![x]\!]$ с коэффициентами в произвольном поле $\Bbbk$ называется полем *рядов Лорана* и обозначается $\Bbbk((x)) = Q_{\Bbbk[\![x]\!]}$. Название «ряд Лорана» объясняется тем, что каждый элемент $f \in \Bbbk((x))$ можно записать как формальный степенной ряд, в котором допускается конечное число отрицательных степеней переменной x

$$f(x) = \sum_{k \geqslant -m} a_k x^k = x^{-m} h(x), \quad \text{где} \quad h \in \Bbbk[\![x]\!]. \tag{4-1}$$

В самом деле, по определению поля частных $f(x) = p(x)/q(x)$, где $p, q \in \Bbbk[\![x]\!]$ и $q \neq 0$. Если младший член ряда q имеет степень m, то $q = x^m \cdot g(x)$, где $g \in \Bbbk[\![x]\!]$ имеет ненулевой свободный член и, стало быть обратим. Поэтому мы можем записать исходную дробь в виде $f(x) = x^{-m} h(x)$, где $h = p/g \in \Bbbk[\![x]\!]$ является обычным степенным рядом.

4.2. Поле рациональных функций. Поле частных кольца многочленов $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от одной переменной. Элементы этого поля представляют собой формальные отношения многочленов $f(x) = p(x)/q(x)$ с коэффициентами в поле $\Bbbk$. Если $\text{нод}(p, q) = 1$, то запись $f = p/q$ называется *несократимым представлением* дроби f. Каждая дробь имеет несократимое представление, которое получается из произвольной записи $f = g/h$ делением числителя и знаменателя на $\text{нод}(g, h)$.

Упражнение 4.3. Покажите, что несократимая запись любой дроби единственна с точностью до умножения числителя и знаменателя на ненулевую константу (в частности, имеется ровно одно несократимое представление с приведённым знаменателем).

Предложение 4.1
Если знаменатель несократимой записи f/g является произведением попарно взаимно простых многочленов $g = g_1 g_2 \ldots g_m$, то дробь f/g *единственным образом* представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_m}{g_m}, \tag{4-2}$$

в которой $\deg h = \deg f - \deg g$ и $\deg f_i < \deg g_i$.

Доказательство. Поделим f на g с остатком: $f = hg+r$, где $\deg r < \deg g$. Тогда $f/g = h+r/g$. Если $g = g_1 g_2$ и нод$(g_1, g_2) = 1$, то существует единственный такой многочлен f_1, что $\deg f_1 < \deg g_1$ и $[f_1]_{g_1} = [r]_{g_1} / [g_2]_{g_1}$ в кольце вычетов $\Bbbk[x]/(g)$. Тогда в $\Bbbk[x]$ мы имеем равенство $r = f_1 \cdot g_2 + f_2 \cdot g_1$ для некоторого многочлена f_2, причём сравнение степеней показывает, что $\deg f_2 < \deg g_2$. Таким образом, $r/g = f_1/g_1 + f_2/g_2$, и с каждой из этих дробей можно снова проделать аналогичную процедуру. Это доказывает существование разложения (4-2). Чтобы доказать его единственность, умножим обе части произвольного разложения (4-2) на g. Получим равенство $f = hg + f_1 G_1 + f_2 G_2 + \cdots + f_m G_m$, в котором

$$G_i = g_1 g_2 \ \dots\ g_{i-1} g_{i+1_1} g_{i+1_2} \ \dots\ g_{i+1_m} \quad \text{и} \quad \deg(f_1 G_1 + f_2 G_2 + \cdots + f_m G_m) < \deg g\,.$$

Тем самым, многочлен h является неполным частным от деления f на g, многочлен $r = f_1 G_1 + f_2 G_2 + \cdots + f_m G_m$ — остатком от этого деления, а каждый f_i — единственным многочленом степени $\deg f_i < \deg g_i$, представляющим в кольце вычетов $\Bbbk[x]/(g_i)$ класс $[f]_{g_i} \cdot [G_i]_{g_i}^{-1}$, т. е. все ингредиенты формулы (4-2) однозначно определяются многочленами f и $g_1, g_2, \dots, g_n$. □

Предложение 4.2
Любую дробь вида $f\,/\,g^m$, в которой $\deg f < \deg(g^m) = m \deg g$, можно *единственным образом* представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \cdots + \frac{f_m}{g^m}\,, \tag{4-3}$$

где каждый числитель f_i имеет степень $\deg f_i < \deg g$.

Доказательство. Представление (4-3) равносильно представлению многочлена f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \cdots + f_{m-1} g + f_m\,, \tag{4-4}$$

аналогичном представлению целого числа f в g-ичной позиционной системе исчисления: f_m равен остатку от деления на g самого многочлена f, f_{m-1} — остатку от деления на g частного $(f - f_m)/g$, f_{m-2} — остатку от деления на g частного $\big((f - f_m)/g - f_{m-1}\big)/g$ и т. д. □

4.2.1. Разложение на простейшие дроби. Из предыдущих двух лемм вытекает, что любая дробь $f/g \in \Bbbk(x)$ допускает *единственное* представление в виде суммы многочлена степени $\deg f - \deg g$ (неполного частного от деления f на g) и дробей вида $p\,/\,q^m$, где q пробегает множество неприводимых делителей знаменателя, m меняется от 1 до кратности вхождения неприводимого множителя q в разложение многочлена g на неприводимые множители, а каждый числитель p имеет степень $\deg p < \deg q$. Такое представление называется *разложением $f\,/\,g$ на простейшие дроби* и часто оказывается полезным при вычислениях с рациональными функциями.

Пример 4.3
Вычислим первообразную[1] и 2013-ю производную от $1/(1+x^2)$. Для этого разложим эту дробь в сумму простейших в поле $\mathbb{C}(x)$:

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

[1] точное (и чисто алгебраическое) определение первообразной от степенного ряда (и в частности, от рациональной функции) см. в n° 4.4 на стр. 55

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

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

Теперь уже легко вычислить как 2013-ю производную:

$$\left(\frac{d}{dx}\right)^{2013} \frac{1}{1+x^2} = \frac{2013!}{2}\left(\frac{(-i)^{2013}}{(1+ix)^{2014}} + \frac{i^{2013}}{(1-ix)^{2014}}\right) =$$
$$= \frac{i}{2}\cdot 2013!\cdot\frac{(1+ix)^{2014} - (1-ix)^{2014}}{(1+x^2)^{2014}} = 2013!\cdot\sum_{\nu=0}^{1006}\binom{2014}{2\nu+1}\cdot\frac{x^{2\nu+1}}{(1+x^2)^{2014}},$$

так и первообразную:

$$\int\frac{dx}{1+x^2} = \frac{1}{2}\int\frac{dx}{1+ix} + \frac{1}{2}\int\frac{dx}{1-ix} = \frac{1}{2}\bigl(\ln(1+ix) + \ln(1-ix)\bigr) = \ln\sqrt{1+x^2}.$$

Написанные равенства суть равенства в кольце $\mathbb{C}[\![x]\!]$, и их точный смысл мы ещё обсудим ниже.

4.3. Разложение рациональных функций в степенные ряды. В силу универсального свойства поля частных, поле рациональных функций $\Bbbk(x)$ единственным образом вкладывается в поле рядов Лорана $\Bbbk((x))$ так, что при этом многочлены переходят в многочлены. С практической точки зрения это вложение представляет собою разложение рациональных функций f/g в формальные степенные ряды. Если основное поле $\Bbbk$ алгебраически замкнуто, такое разложение можно описать довольно явными формулами.

А именно, пусть $\deg f < \deg g$ и знаменатель дроби f/g имеет вид:

$$g(x) = 1 + a_1x + a_2x^2 + \cdots + a_nx^n = \prod(1-\alpha_ix)^{m_i}, \tag{4-5}$$

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

Упражнение 4.4. Убедитесь, что при $a_n \neq 0$ числа α_i из разложения (4-5) суть корни многочлена $t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n = \prod(t-\alpha_i)^{m_i}$.

Тогда по предл. 4.1 и предл. 4.2 функция f/g является суммой простейших дробей вида

$$\frac{\beta_{ij}}{(1-\alpha_ix)^{k_{ij}}} \tag{4-6}$$

где при каждом i показатели k_{ij} лежат в пределах $1 \leqslant k_{ij} \leqslant m_i$, а $\beta_{ij} \in \Bbbk$. Если все кратности $m_i = 1$, константы β_i в получающемся разложении

$$\frac{f(x)}{(1-\alpha_1x)(1-\alpha_2x)\cdots(1-\alpha_nx)} = \frac{\beta_1}{1-\alpha_1x} + \frac{\beta_2}{1-\alpha_2x} + \cdots + \frac{\beta_n}{1-\alpha_nx} \tag{4-7}$$

легко указать явно: умножая обе части (4-7) на знаменатель и беря $x = \alpha_i^{-1}$, получаем

$$\beta_i = \frac{f\left(\alpha_i^{-1}\right)}{\prod\limits_{\nu\neq i}\left(1-(\alpha_\nu/\alpha_i)\right)} = \frac{\alpha_i^{n-1}f\left(\alpha_i^{-1}\right)}{\prod\limits_{\nu\neq i}\left(\alpha_i-\alpha_\nu\right)}. \tag{4-8}$$

Дробь f/g в этом случае равна сумме геометрических прогрессий (4-7)

$$\frac{f(x)}{g(x)} = \sum \left(\beta_1\alpha_1^k + \beta_2\alpha_2^k + \ \cdots\ + \beta_n\alpha_n^k\right)\cdot x^k\,.$$

Для произвольной кратности $m_i = m \in \mathbb{N}$ простейшая дробь (4-6) раскладывается в ряд по формуле Ньютона для бинома *с отрицательным показателем*

$$\frac{1}{(1-x)^m} = \sum_{k\geqslant 0} \frac{(k+m-1)(k+m-2)\,\cdots\,(k+1)}{(m-1)!}\cdot x^k = \sum_{k\geqslant 0}\binom{k+m-1}{m-1}\cdot x^k\,, \tag{4-9}$$

которая получается $(m-1)$-кратным дифференцированием обеих частей разложения геометрической прогрессии $(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \ldots$.

Упражнение 4.5. Убедитесь, что $\left(\frac{d}{dx}\right)^m (1-x)^{-1} = m!/(1-x)^{m+1}$.

Таким образом, разложение простейшей дроби (4-6) имеет вид

$$\frac{\beta}{(1-\alpha_i x)^m} = \beta\sum_{k\geqslant 0}\alpha_i^k\binom{k+m-1}{m-1}\cdot x^k\,, \tag{4-10}$$

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

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ \cdots\ + a_n z_{k-n} = 0\,, \tag{4-11}$$

где коэффициенты $a_1, a_2, \ldots, a_n \in \mathbb{C}$ — некоторые фиксированные заданные числа.

В самом деле, уравнению (4-11) при $k \geqslant n$ удовлетворяют коэффициенты z_k степенного ряда

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

Если подобрать $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ в числителе левой части так, чтобы первые n коэффициентов справа совпадали с начальным куском последовательности (4-11), и разложить полученную рациональную функцию в ряд, то мы получим явные выражения элементов последовательности z_k через k.

Пример 4.4 (числа Фибоначчи)
Найдём явное выражение через k для элементов последовательности

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

решающей рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ на коэффициенты ряда

$$\frac{b_0 + b_1 x}{1 - x - x^2} = x + z_2 x^2 + z_3 x^3 + \ \cdots \tag{4-12}$$

(мы подставили в правую часть данные по условию $z_0 = 0$ и $z_1 = 1$). Умножая обе части (4-12) на общий знаменатель и сравнивая коэффициенты при x^0 и x^1, получаем $b_0 = 0$ и $b_1 = 1$. Итак, нас интересуют коэффициенты ряда

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

где $\alpha_\pm = (1\pm\sqrt{5})/2$ суть корни многочлена t^2-t-1, а числа $\beta_\pm$ находятся по формуле (4-8) с учётом равенств $\alpha_+\alpha_- = -1$, $\alpha_+ + \alpha_- = 1$ и $\alpha_+ - \alpha_- = \sqrt{5}$: $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$. Получаем:

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

откуда

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

Предложение 4.3
Всякая последовательность z_k, удовлетворяющая при $k \geqslant n$ линейному рекуррентному уравнению n-того порядка

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \;\cdots\; + a_n z_{k-n} = 0\,, \tag{4-13}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, имеет вид

$$z_k = \alpha_1^k\cdot\varphi_1(k) + \alpha_2^k\cdot\varphi_2(k) + \;\cdots\; + \alpha_r^k\cdot\varphi_r(k)\,,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_r$ суть все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n\,, \tag{4-14}$$

а каждая из функций $\varphi_i \in \mathbb{C}[x]$ представляет собою многочлен степени на единицу меньшей, чем кратность соответствующего корня α_i.

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[\![x]\!]$, коэффициенты которого решают уравнение (4-13), является суммой дробей вида $\beta\cdot(1-\alpha x)^{-m}$, где α пробегает различные корни многочлена (4-14), показатель степени m может принимать любое значение от 1 до кратности соответствующего корня α, а $\beta = \beta(\alpha, m)$ — комплексное число, однозначно вычисляемое по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (4-10) k-тый член разложения такой дроби имеет вид $\alpha^k\varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ есть многочлен от k степени $m-1$. □

4.4. Логарифм и экспонента. Всюду в этом разделе мы рассматриваем ряды с коэффициентами в поле $\Bbbk$ характеристики $\operatorname{char}\Bbbk = 0$. В этом случае из формулы (3-6) для производной вытекает, что для любого ряда $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Этот ряд называется *первообразным рядом* или *интегралом* от f и обозначается

$$\int f(x)\,dx \;\stackrel{\text{def}}{=}\; a_0 x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \;\cdots\; = \sum_{k\geqslant 1}\frac{a_{k-1}}{k}x^k\,. \tag{4-15}$$

[1] он называется *характеристическим многочленом* рекуррентного уравнения (4-11)

Определение 4.1
Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\ln(1+x) \stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \cdots\right) dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k . \quad (4\text{-}16)$$

4.4.1. Логарифмирование рядов. Вместо $1+x$ в логарифм можно подставить любой ряд $u(x)$ с единичным свободным членом — это равносильно подстановке вместо x ряда $u(x)-1$ без свободного члена, что является алгебраической операцией. Обозначим через $N \subset \Bbbk[\![x]\!]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U \subset \Bbbk[\![x]\!]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом. Тогда операция *логарифмирования*, переводящая ряд $u(x) \in U$ в ряд $\ln(u(x)) \in N$, является алгебраической и задаёт отображение

$$\ln : U \to N, \quad u \mapsto \ln u . \quad (4\text{-}17)$$

Упражнение 4.6 (логарифмическая производная). Докажите для любого ряда $u \in U$ формулу $\frac{d}{dx} \ln u = u'/u$.

Лемма 4.3
Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $u'/u = w'/w$ попарно эквивалентны друг другу.

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

Упражнение 4.7. Покажите, что $\forall\, u \in U \;\; \ln(1/u) = -\ln u$.

Определение 4.2
Ряд $e^x \stackrel{\text{def}}{=} \sum_{k\geqslant 0} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \ldots$ называется *экспонентой*. Это единственный ряд в U, удовлетворяющий дифференциальному уравнению $f'(x) = f(x)$.

4.4.2. Экспоненцирование рядов. Подставляя в экспоненту вместо x любой ряд $\tau(x)$ без свободного члена, мы получаем ряд $e^{\tau(x)}$ со свободным членом 1, который называется *экспонентой* ряда $\tau(x)$. Этим определяется экспоненциальное отображение

$$\exp : N \to U, \quad \tau \mapsto e^{\tau} . \quad (4\text{-}18)$$

Теорема 4.2
Экспоненциальное и логарифмическое отображения (4-18) и (4-17) являются взаимно обратными изоморфизмами абелевых групп. В частности, для любых рядов $u, u_1, u_2 \in U$ и $\tau, \tau_1, \tau_2 \in N$ выполняются тождества:

$$\ln e^{\tau} = \tau , \quad e^{\ln u} = u , \quad \ln(u_1 u_2) = \ln(u_1) + \ln(u_2) , \quad e^{\tau_1+\tau_2} = e^{\tau_1} e^{\tau_2} .$$

Доказательство. Равенство $\ln e^\tau = \tau$ проверяется взятием производной, а $e^{\ln u} = u$ — логарифмической производной от обеих частей. Поэтому экспоненцирование и логарифмирование суть взаимно обратные биекции. Ряды $\ln(u_1u_2)$ и $\ln u_1 + \ln u_2$ совпадают, поскольку имеют нулевые свободные члены и равные производные:

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

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

Упражнение 4.8. Докажите в $\Bbbk[\![x, y]\!]$ равенство $e^{x+y} = e^x e^y$ непосредственным сравнением коэффициентов этих двух рядов.

4.5. Степенная функция и бином Ньютона. В этом разделе мы продолжаем считать, что $\operatorname{char}\Bbbk = 0$. Для любого числа $\alpha \in \Bbbk$ определим *биномиальный ряд* с показателем α формулой

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

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

$$u^\alpha \cdot u^\beta = e^{\alpha \ln u} \cdot e^{\beta \ln u} = e^{\alpha \ln u + \beta \ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta} \tag{4-19}$$

$$\big(u^\alpha\big)^\beta = e^{\beta \ln(u^\alpha)} = e^{\beta \ln\left(e^{\alpha \ln u}\right)} = e^{\alpha\beta \ln u} = u^{\alpha\beta} \tag{4-20}$$

$$(uv)^\alpha = e^{\alpha \ln(uv)} = e^{\alpha(\ln u + \ln v)} = e^{\alpha \ln u + \alpha \ln v} = e^{\alpha \ln u} \cdot e^{\alpha \ln v} = u^\alpha v^\alpha \tag{4-21}$$

В частности, для любого ряда u с единичным свободным членом $u^{1/n} = \sqrt[n]{u}$ в том смысле, что $\big(u^{1/n}\big)^n = u$. Для явного отыскания коэффициентов a_i биномиального ряда

$$(1+x)^\alpha = a_0 + a_1x + a_2x^2 + \cdots$$

вычислим его логарифмическую производную:

$$\frac{\big((1+x)^\alpha\big)'}{(1+x)^\alpha} = \big(\ln(1+x)^\alpha\big)' = \big(\alpha \ln(1+x)\big)' = \frac{\alpha}{1+x}\,.$$

Приводя левую и правую часть к общему знаменателю, получаем соотношение

$$\big(a_1 + 2a_2x + 3a_3x^2 + \cdots\big) \cdot (1+x) = \alpha \cdot (1 + a_1x + a_2x^2 + a_3x^3 + \cdots)\,.$$

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

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

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

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{4-22}$$

Нами доказано

Предложение 4.4 (формула Ньютона)
Для любого числа $\alpha \in \Bbbk$ имеется разложение

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

Пример 4.5 (бином с рациональным показателем)
При натуральном значении показателя $\alpha = n \in \mathbb{N}$ имеется лишь конечное число ненулевых биномиальных коэффициентов, поскольку при $k > n$ в числителе (4-22) образуется нулевой сомножитель. Поэтому разложение бинома в этом случае конечно:

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

При целом отрицательном $\alpha = -m$, $m \in \mathbb{N}$, мы снова получаем разложение (4-9) со стр. 54

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

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

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

Например, при $n = 2$ в качестве коэффициента при x^k мы получаем дробь вида

$$(-1)^{k-1}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(2k-3)}{2\cdot 4\cdot 6\cdot\cdots\cdot(2k)} = \frac{(-1)^{k-1}}{2k-1}\cdot\frac{(2k)!}{(2\cdot 4\cdot 6\cdot\cdots\cdot(2k))^2} =$$
$$= \frac{(-1)^{k-1}}{(2k-1)\cdot 4^k}\cdot\binom{2k}{k}.$$

Таким образом,

$$\sqrt{1+x} = \sum_{k\geqslant 0} \frac{(-1)^{k-1}}{2k-1}\cdot\binom{2k}{k}\cdot\frac{x^k}{4^k} . \tag{4-23}$$

Пример 4.6 (числа Каталана)
Воспользуемся разложением (4-23) для получения явной формулы для *чисел Каталана*, часто возникающих в различных комбинаторных задачах. Пусть при вычислении произведения $(n+1)$ сомножителей

$$a_0a_1a_2\ \cdots\ a_n \qquad \text{(всего } n \text{ умножений)} \tag{4-24}$$

в каждый момент времени разрешается делать не более одного умножения. Если на каждом шагу заключать вычисленное произведение в скобки, мы расставим в выражении (4-24) n пар скобок ( ). Количество всех различных расстановок скобок, возникающих таким образом, называется n-ым *числом Каталана* c_n. При $n=1$ есть лишь одна расстановка скобок: (a_1a_2), при $n=2$ — две: $(a_1(a_2a_3))$ и $((a_1a_2)a_3)$, при $n=3$ — пять:

$$(a_1(a_2(a_3a_4)),\ (a_1((a_2a_3)a_4)),\ ((a_1a_2)(a_3a_4)),\ ((a_1(a_2a_3))a_4),\ (((a_1a_2)a_3)a_4).$$

Множество всех возможных расстановок скобок в (4-24) распадается в дизъюнктное объединение n подмножеств, в которых конфигурации наружных скобок имеют вид

$$(a_0(a_2\dots a_n)),\ ((a_0a_1)(a_2\dots a_n)),\ ((a_0\dots a_2)(a_3\dots a_n)),\ ((a_0\dots a_3)(a_4\dots a_n)),\ \dots$$
$$\dots,\ ((a_0\dots a_{n-2})(a_{n-1}a_n)),\ ((a_0\dots a_{n-1})a_n)$$

и которые состоят, соответственно, из c_{n-1}, c_1c_{n-2}, c_2c_{n-3}, c_3c_{n-4}, …, $c_{n-2}c_1$, c_{n-1} элементов. Если добавить к числам Каталана число $c_0=1$, то мы получим рекурсивное соотношение $c_n=c_0c_{n-1}+c_1c_{n-2}+\dots+c_{n-2}c_1+c_{n-1}c_0$ на коэффициенты c_n *ряда Каталана*

$$c(x)=\sum_{k\geqslant 0}c_kx^k=1+c_1x+c_2x^2+c_3x^3+\ \cdots\ \in\mathbb{Z}[\![x]\!],$$

означающее, что $c(x)^2=(c(x)-1)/x$. Иначе говоря, $t=c(x)$ является решением квадратного уравнения $x\cdot t^2-t-1=0$ на неизвестную t в кольце $\mathbb{Z}[\![x]\!]$. В поле $\mathbb{Q}((x))\supset\mathbb{Z}[\![x]\!]$ это уравнение решается по обычной школьной формуле, дающей два корня $(1\pm\sqrt{1-4x})/(2x)$. Согласно (4-23), $\sqrt{1-4x}=-\sum\limits_{k\geqslant 0}\frac{1}{2k-1}\cdot\binom{2k}{k}\cdot x^k=1-2x-2x^2-4x^3-10x^4-\ \dots$. Поэтому $(1+\sqrt{1-4x})/(2x)$ не лежит в $\mathbb{Z}[\![x]\!]$: ряд $1+\sqrt{1-4x}$ имеет ненулевой свободный член и не делится на $2x$ в $\mathbb{Z}[\![x]\!]$. Тем самым, $c(x)=(1-\sqrt{1-4x})/(2x)$ и

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

Отметим, что с первого взгляда не вполне понятно, что это число — целое.

4.6. Ряд Тодда и числа Бернулли. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[\![x]\!]$ от переменной x и кольцо многочленов $\mathbb{Q}[t]$ от переменной t. Обозначим через

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

оператор дифференцирования, и для каждого степенного ряда $\Phi(x)=\sum\limits_{k\geqslant 0}\varphi_kx^k\in\mathbb{Q}[\![x]\!]$ определим результат подстановки в Φ вместо x оператора D как отображение

$$\Phi(D)\ :\ \mathbb{Q}[t]\to\mathbb{Q}[t],\quad f\mapsto\varphi_0\cdot f+\varphi_1\cdot f'+\varphi_2\cdot f''+\ \cdots=\sum_{k\geqslant 0}\varphi_k\cdot D^k(f). \tag{4-25}$$

Поскольку каждое дифференцирование уменьшает степень многочлена на единицу, все слагаемые в правой части (4-25) обратятся в нуль при $k > \deg f$. Таким образом, для каждого многочлена $f \in \mathbb{Q}[t]$, правая часть (4-25) является корректно определённым многочленом, каждый коэффициент которого вычисляется конечным числом арифметических операций над коэффициентами исходного многочлена f и первыми $\deg(f)$ коэффициентами ряда Φ. Отображение

$$\mathrm{ev}_D : \mathbb{Q}[\![x]\!] \to \mathrm{End}(\mathbb{Q}[t]), \quad \Phi(x) \mapsto \Phi(D), \tag{4-26}$$

является гомоморфизмом коммутативного кольца $\mathbb{Q}[\![x]\!]$ в (некоммутативную) алгебру *линейных эндоморфизмов* пространства многочленов в том смысле, что все отображения $\Phi(D)$ *линейны*:

$$\forall\, \alpha, \beta \in \mathbb{Q}\ \forall f, g \in \mathbb{Q}[t] \quad \Phi(D)(\alpha \cdot f + \beta \cdot g) = \alpha \cdot \Phi(D)f + \beta \cdot f(D)g \tag{4-27}$$

и суммы и произведения рядов переходят в суммы и *композиции* соответствующих отображений. Последнее означает, что при подстановке D в произведение $\Phi(x)\Psi(x) \in \mathbb{Q}[\![x]\!]$ получится *композиция* отображений $\Phi(D) \circ \Psi(D) = \Psi(D) \circ \Phi(D)$. В частности, все отображения $\Phi(D)$ перестановочны друг с другом, и отображение $\Phi(D)$ биективно тогда и только тогда, когда степенной ряд $\Phi(x) \in \mathbb{Q}[\![x]\!]$ имеет ненулевой свободный член.

Упражнение 4.9. Проверьте все эти утверждения.

В силу линейности (4-27) для вычисления значения отображения

$$\Phi(D) = \varphi_0 + \varphi_1 D + \varphi_2 D^2 + \cdots : \mathbb{Q}[t] \to \mathbb{Q}[t]$$

на произвольном многочлене достаточно уметь вычислять его на всех одночленах t^m:

$$\Phi(D)\left(a_0 + a_1 t + \cdots + a_n t^n\right) = a_0 + a_1 \Phi(D)t + a_2 \Phi(D)t^2 + \cdots + a_n \Phi(D)t^n .$$

Для каждого k многочлен $\Phi_k(t) \stackrel{\text{def}}{=} \Phi(D)t^k \in \mathbb{Q}[t]$ имеет степень $\leqslant k$ и зависит лишь от первых $k+1$ коэффициентов ряда Φ. Он называется k-тым *многочленом Аппеля* ряда Φ.

Пример 4.7 (операторы сдвига)
Экспонента $e^D = 1 + D + \frac{1}{2}D^2 + \frac{1}{6}D^3 + \ldots$ имеет многочлены Аппеля

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

Следовательно, оператор e^D действует на любой многочлен как *оператор сдвига*:

$$e^D : f(t) \mapsto f(t+1).$$

Так как ряды e^x и e^{-x} обратны друг другу в $\mathbb{Q}[\![x]\!]$, операторы e^D и e^{-D} тоже обратны друг другу, т. е.

$$e^{-D} : f(t) = f(t-1).$$

Упражнение 4.10. Убедитесь, что $e^{\alpha D} f(t) = f(t+\alpha)$ при любом $\alpha \in \mathbb{Q}$.

Пример 4.8 (вычисление степенных сумм)
Для произвольно зафиксированного $m \in \mathbb{Z}_{\geqslant 0}$ рассмотрим сумму

$$S_m(n) \stackrel{\text{def}}{=} 0^m + 1^m + 2^m + 3^m + \ \cdots \ + n^m = \sum_{k=0}^{n} k^m \tag{4-28}$$

как функцию от n. Так,

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

Применяя к этой функции *разностный оператор* $\nabla : \varphi(t) \mapsto \varphi(t) - \varphi(t-1)$, мы получим многочлен $\nabla S_m(t) = t^m$. Покажем, что в $\mathbb{Q}[t]$ существует единственный многочлен $S_m(t)$ с нулевым свободным членом, такой что $\nabla S_m(t) = t^m$. Тогда его значения при целых неотрицательных $t = 0, 1, 2, \ldots$ автоматически окажутся равными суммам (4-28).

Согласно прим. 4.7, действие ∇ на пространстве многочленов $\mathbb{Q}[t]$ задаётся рядом

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

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

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

называется *рядом Тодда*. Подставляя $x = D$ в равенство $\operatorname{td}(x) \cdot (1 - e^{-x}) = x$, получаем соотношение $\operatorname{td}(D) \circ \nabla = D$. Стало быть, производная

$$S'_m(t) = DS_m(t) = \operatorname{td}(D)\nabla S_m(t) = \operatorname{td}(D)t^m$$

является многочленом Аппеля ряда Тодда, а искомый многочлен $S_m(t)$ является его первообразной. Для её вычисления удобно записать ряд Тодда в «экспоненциальной форме», вынеся из коэффициентов обратные факториалы:

$$\operatorname{td}(x) = \sum_{k \geqslant 0} \frac{a_k}{k!}\, x^k. \tag{4-29}$$

Окончательно, сумма m-тых степеней первых t натуральных чисел равна[1]

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

Коэффициенты a_k находятся из соотношения $\operatorname{td}(x) \cdot (1 - e^{-x})/x = 1$:

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

[1] эту формулу иногда представляют в символическом виде $(m+1) \cdot S_m(t) = (a\!\downarrow + t)^{m+1} - a_{m+1}$, где стрелка у $a\!\downarrow$ предписывает заменять a^k на a_k при раскрытии бинома $(a + t)^{m+1}$

Упражнение 4.11. Найдите первую дюжину чисел a_k, напишите явные формулы для $S_4(n)$ и $S_5(n)$ и вычислите[1] $S_{10}(1000)$.

4.6.1. Числа Бернулли. Название «ряд Тодда» вошло в обиход во второй половине XX века после работ Хирцебруха и Гротендика, где он был применён для формулировки и доказательства теоремы Риана – Роха. Во времена Бернулли и Эйлера предпочитали пользоваться рядом

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

который отличается от ряда $\mathrm{td}(x)$ ровно одним коэффициентом:

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

т. е. член степени 1 в $\mathrm{td}(x)$ равен $x/2$, а в $\mathrm{td}(-x)$ равен $-x/2$, и это *единственный* ненулевой член нечётной степени в обоих рядах. Коэффициенты B_k в «экспоненциальной» записи ряда

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

называются *числами Бернулли*. Таким образом, $B_k = a_k$ при $k \neq 1$ и обращаются в нуль при всех нечётных $k \geqslant 3$, а $B_1 = -a_1 = -1/2$. Со времён своего открытия Яковом Бернули, числа B_k вызывают неослабевающий интерес. Им посвящена обширная литература[2] и даже специальный интернет-ресурс http://www.bernoulli.org/, на котором, среди прочего, имеется программа для быстрого вычисления чисел B_k в виде несократимых рациональных дробей. Однако, не смотря на огромное количество красивых теорем о числах Бернулли, никакой внятной формулы, явно выражающей B_n через n нет, и любой содержательный новый взгляд в этом направлении был бы интересен.

Упражнение 4.12. Получите для чисел Бернулли рекурсивную формулу

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

4.6.2. Разностные операторы на пространстве многочленов. Для каждого формального степенного ряда $\Phi(x) = \varphi_0 + \varphi_1 x + \varphi_2 x^2 + \dots \in \mathbb{Q}[\![x]\!]$ можно, как и выше, определить оператор

$$\Phi(\nabla) : \Bbbk[t] \to \Bbbk[t]\,, \quad f(x) \mapsto \sum_{\nu\geqslant 0} \varphi_\nu \nabla^\nu f\,. \tag{4-30}$$

Упражнение 4.13. Проверьте, что $\forall f \in \mathbb{Q}[t] \quad \deg(\nabla f) < \deg(f)$ (так что правая часть (4-30) является корректно определённым многочленом) и представьте оператор дифференцирования $D = d/dx$ в виде ряда (4-30) без свободного члена.

---

[1] Яков Бернулли (1654–1705) при помощи одних лишь пера и бумаги просуммировал десятые степени первой тысячи натуральных чисел примерно за 7 минут, о чём не без гордости написал в своём манускрипте «Ars Conjectandi», опубликованном в 1713 году уже после его кончины

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

Предложение 4.5
Следующие условия на линейный оператор $F : \mathbb{Q}[t] \to \mathbb{Q}[x]$ попарно эквивалентны:

1) $F \circ \nabla = \nabla \circ F$

2) $F \circ T = T \circ F$, где $T : f(x) \mapsto f(x-1)$

3) $\forall\, \alpha \in \mathbb{Q} \quad F \circ T_\alpha = T_\alpha \circ F$, где $T_\alpha : f(x) \mapsto f(x-\alpha)$

4) $F = \Phi(D)$ для некоторого $\Phi \in \mathbb{Q}[\![x]\!]$

5) $F = \Psi(\nabla)$ для некоторого $\Psi \in \mathbb{Q}[\![x]\!]$.

Определение 4.3
Оператор $F : \mathbb{Q}[t] \to \mathbb{Q}[t]$, удовлетворяющий условиям предл. 4.5, называется *разностным оператором* на пространстве многочленов.

Доказательство предл. 4.5. Импликации (5) ⇒ (4) ⇒ (3) ⇒ (2) ⇒ (1) очевидны. Докажем импликацию (1) ⇒ (5). Рассмотрим многочлены

$$\gamma_0 \equiv 1 \quad \text{и} \quad \gamma_k \stackrel{\text{def}}{=} \binom{x+k}{k} = \frac{1}{k!}(x+1)(x+2)\cdots(x+k) \quad (\text{при } k>0)\,. \tag{4-31}$$

Упражнение 4.14. Проверьте, что $\forall\, k \geqslant 1\ \nabla\gamma_k = \gamma_{k-1}$ и что любой многочлен $f \in \mathbb{Q}[x]$ однозначно записывается в виде $f = \sum\limits_k c_k\gamma_k$ с $c_k \in \mathbb{Q}$, причём константы $c_k = \nabla^k f(-1)$.

Пусть значение многочлена $F(\gamma_k)$ при $x=-1$ равно a_k. По упр. 4.14

$$F(\gamma_k) = \sum_{\nu\geqslant 0} \lambda_\nu \gamma_\nu\,,$$

где $\lambda_\nu = \nabla^\nu F\gamma_k\,(-1) = F\nabla^\nu\,\gamma_k\,(-1) = F\gamma_{k-\nu}(-1) = a_{k-\nu}$. Мы заключаем, что $a_\nu = 0$ при $\nu > k$ и $F(\gamma_k) = \sum\limits_{\nu=0}^{k} a_{k-\nu}\gamma_\nu = \sum\limits_{\alpha\geqslant 0} a_\alpha \nabla^\alpha\,\gamma_k$. Таким образом, F действует на многочлены γ_k точно также, как оператор $\sum\limits_\alpha a_\alpha\nabla^\alpha$. Поэтому $F = \sum\limits_\alpha a_\alpha\nabla^\alpha$. □

4.7. **Дробно степенные ряды**. Ряд Лорана от переменной $x^{1/q}$

$$\sum_{k\geqslant m} a_k x^{k/q}\,, \quad a_k \in \Bbbk\,,\ k \in \mathbb{Z}\,,$$

называется *дробно-степенным рядом* или *рядом Пюизо*. Иначе можно сказать, что ряд Пюизо — это степенной ряд с ограниченными снизу рациональными показателями степеней, имеющими общий знаменатель. Также как и ряды Лорана, дробно-степенные ряды с коэффициентами в поле $\Bbbk$ образуют поле. Основным результатом этого раздела является

Теорема 4.3
Если поле $\Bbbk$ алгебраически замкнуто и имеет характеристику нуль, то поле рядов Пюизо тоже алгебраически замкнуто.

Лемма 4.4 (лемма Гензеля)
Пусть $G(t,x) \in \Bbbk[\![t]\!]\,[x]$ является приведённым многочленом от переменной x с коэффициентами в формальных степенных рядах от переменной t над произвольным полем $\Bbbk$. Если при $t = 0$ многочлен $G(0,x) \in \Bbbk[x]$ раскладывается в $\Bbbk[x]$ в произведение взаимно простых приведённых множителей $a(x)$ и $b(x)$ положительных степеней, то и $G(t,x)$ раскладывается в $\Bbbk[\![t]\!][x]$ в произведение приведённых многочленов $A(t,x)$ и $B(t,x)$ тех же степеней по x, что $a(x)$ и $b(x)$, и таких, что $A(0,x) = a(x)$ и $B(0,x) = b(x)$.

Доказательство. Запишем данный ряд $G(t,x)$ и искомые ряды $A(t,x)$ и $B(t,x)$ в виде рядов от переменной t с коэффициентами в $\Bbbk[x]$:

$$\begin{aligned} G(t,x) &= g_0(x) + g_1(x)\,t + g_2(x)\,t^2 + \cdots \\ A(t,x) &= a_0(x) + a_1(x)\,t + a_2(x)\,t^2 + \cdots \\ B(t,x) &= b_0(x) + b_1(x)\,t + b_2(x)\,t^2 + \cdots \end{aligned}$$

и приравняем коэффициенты при t^k в равенстве $G_t(x) = A_t(x) \cdot B_t(x)$:

$$\begin{aligned} a_0(x)\,b_0(x) &= g_0(x) && (\text{при } k = 0) \\ a_0(x)\,b_k(x) + b_0(x)\,a_k(x) &= g_k(x) - \sum_{i=1}^{k-1} a_i(x)\,b_{k-i}(x) && (\text{при } k \geqslant 1)\,. \end{aligned} \tag{4-32}$$

Взаимно простые многочлены $a_0(x) = a(x)$ и $b_0(x) = b(x)$, удовлетворяющие первому равенству, даны по условию. Второе равенство однозначно определяет многочлены a_k и b_k степеней $\deg a_k < \deg a$ и $\deg b_k < \deg b$, как только известны все предыдущие многочлены a_i и b_i и известно, что $\deg a_i < \deg a$ и $\deg b_i < \deg b$ при всех $i < k$. В самом деле, раз G приведён как многочлен от x, то $\deg g_i < \deg g_0$ при всех $i > 0$ и степень многочлена из правой части формулы (4-32) строго меньше $\deg a_0 \cdot \deg b_0$. Тем самым, b_k — это единственный многочлен степени $< \deg b_0$ класс которого по модулю b_0 равен отношению класса правой части формулы (4-32) к классу $a_0 \pmod{b_0}$, а класс a_k играет аналогичную роль по модулю a_0 (ср. с доказательством предл. 4.1). □

Упражнение 4.15. Покажите, что построенные многочлены A и B взаимно просты в кольце $\Bbbk[\![t]\!]\,[x]$.

Лемма 4.5
Над алгебраически замкнутым полем $\Bbbk$ характеристики нуль для любого многочлена

$$F(t,x) = a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \cdots + a_0(x) \in \Bbbk((t))\,[x]$$

от переменной x с коэффициентами в поле $\Bbbk((t))$ существуют число $m \in \mathbb{N}$ и ряд Лорана $\vartheta(t) \in \Bbbk((t))$, такие что $F\left(t^m, \vartheta(t)\right) = 0$ в поле $\Bbbk((t))$. Иными словами, каждый многочлен с коэффициентами в поле рядов Лорана от t после замены параметра t параметром t^m с надлежащим[1] $m \in \mathbb{N}$ приобретает в поле $\Bbbk((t))$ корень.

Доказательство. Не ограничивая общности мы можем и будем далее считать, что многочлен F имеет коэффициенты в $\Bbbk[\![t]\!]$, причём старший коэффициент $a_n = 1$, а следующий

[1] т. е. после извлечения из параметра корня должной степени

за ним коэффициент $a_{n-1} = 0$: первого можно добиться, умножив F на подходящую степень t, второго — умножив полученный многочлен на a_n^{n-1} и заменив x на $y = a_n x$, третьего — заменив y на $z = y - a_{n-1}/n$.

Упражнение 4.16. Убедитесь, что в каждом из трёх случаев умение находить корень для изменённого многочлена позволяет найти его и для исходного многочлена.

Если $F(t,x) = x^n$, мы можем взять $q = 1$ и $\vartheta = 0$. Поэтому мы будем далее считать, что среди коэффициентов $a_0, a_1, \dots, a_{n-2}$ есть ненулевые ряды. Если F приводим, мы можем воспользоваться индукцией по $\dim F$ и подобрать m и ϑ для многочлена меньшей степени, делящего F. Таким образом, нам надо сделать многочлен F приводимым. По лемме Гензеля для этого достаточно, чтобы многочлен $F(0,x) \in \Bbbk[x]$ раскладывался в $\Bbbk[x]$ на два взаимно простых множителя положительной степени. Над алгебраически замкнутым полем этого нельзя сделать лишь тогда, когда $F(0,x) = (x-\alpha)^n$ для некоторого $\alpha \in \Bbbk$. Но многочлен $(x-\alpha)^n$ либо равен x^n, либо содержит член $n\alpha x^{n-1} \neq 0$ (здесь существенно, что $\operatorname{char} \Bbbk = 0$). По нашему предположению, F не содержит x^{n-1}, и нам остаётся добиться, чтобы хоть один из рядов $a_0, a_1, \dots, a_{n-2}$ не обращался в нуль при $t = 0$.

Для этого запишем ненулевые коэффициенты многочлена F в виде

$$a_m(t) = \alpha_{\mu_m}\, t^{\mu_m} + \text{члены большей степени по } t\ , \quad \text{где} \quad \alpha_{\mu_m} \neq 0\,,$$

выберем из дробей μ_m/m наименьшую, обозначим через p/q её несократимую запись и сделаем в многочлене

$$F(t,x) = x^n + \sum_{m=0}^{n-2} a_m(t)\, x^m$$

подстановку $t \leftarrow t^q$, $x \leftarrow t^p y$. Получим многочлен

$$G(t,y) = F(t^q, t^p y) = t^{pn}\, y^n + \sum_{m=0}^{n-2} a_m(t^q)\, t^{pm}\, y^m = \\ = t^{pn}\Big(y^n + \sum_{m=0}^{n-2} t^{q\mu_m - pm}\,(\alpha_{\mu_m} + \text{ члены, делящиеся на } t\,)\cdot y^m\Big)\,.$$

Так как $q\mu_m \geqslant pm$ для всех m, ряды-коэффициенты в правой сумме лежат в $\Bbbk[\![t]\!]$, и по крайней мере один из них — тот, у которого $q\mu_m = pm$, — отличен от нуля при $t = 0$.

Тем самым, приведённый многочлен $G(t,y)/(t^{pn})$ раскладывается в $\Bbbk[\![t]\!]\,[y]$ в произведение многочленов меньшей степени, и по индукции существуют число $d \in \mathbb{N}$ и ряд Лорана $\tau(t)$, для которых $G\left(t^d, \tau(t)\right) = 0$ в $\Bbbk((t))$. Тогда для $m = qd$ и $\vartheta(t) = t^p\,\tau(t)$ выполняется нужное нам равенство $F\left(t^m, \vartheta(t)\right) = F\left(t^{qd}, t^p\,\tau(t)\right) = G\left(t^d, \tau(t)\right) = 0$. □

Упражнение 4.17. Выведите теор. 4.3 из лем. 4.5.

Замечание 4.3. В доказательстве лем. 4.5 мы явно воспользовались условием $\operatorname{char} \Bbbk = 0$, и без этого предположения лем. 4.5 (а с нею и теор. 4.3) неверна.

Пример 4.9
Рассмотрим уравнение $x^p - x = t^{-1}$ над полем $\mathbb{F}_p((t))$, и будем искать его решение в виде $x(t) = a_1 t^{\lambda_1} + a_2 t^{\lambda_2} + \cdots$ с рациональными $\lambda_1 < \lambda_2 < \dots$ и $a_i \neq 0$. Поскольку $a^p = a$ для

всех $a \in \mathbb{F}_p$, подставляя ряд в домноженное на t уравнение $t\,x^p - t\,x = 1$, мы получаем

$$-a_1 t^{\lambda_1+1} + a_2 t^{\lambda_2+1} - a_1 t^{p\lambda_1+1} + a_3 t^{\lambda_3+1} - a_2 t^{p\lambda_2+1} + \text{ старшие члены}\,.$$

Поскольку младшему члену $a_1 t^{\lambda_1+1}$ не с чем сократиться кроме единицы в правой части, мы заключаем, что $\lambda_1 = -1$ и $a_1 = -1$. Следующие два члена обязаны сокращать друг друга, откуда $\lambda_2 = -1/p$ и $a_2 = a_1$, следующие два члена также обязаны сокращать друг друга, откуда $\lambda_3 = -1/p^2$ и $a_3 = a_2$, и т. д. В результате получаем ряд

$$x(t) = -t^{-1} - t^{-1/p} - t^{-1/p^2} - t^{-1/p^3} - \cdots = -\sum_{k\geqslant 0} t^{-p^k}\,,$$

который не является рядом Пиюзо, т. к. у его показателей нет общего знаменателя.

4.7.1. Метод Ньютона для явного отыскания рядов Пюизо $x_1(t)$, … , $x_n(t)$, являющихся корнями заданного многочлена

$$F(t,x) = a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \cdots + a_0(x) \in \Bbbk[\![t]\!][x] \tag{4-33}$$

заключается в следующем. Сначала находим все корни многочлена $F(0,x) \in \Bbbk[x]$, получающегося из F при $t = 0$, и для каждого такого корня ξ делаем замену $x \leftarrow\!\shortmid \xi + x$. После этого $x = 0$ становится корнем $F(0,x)$, и мы будем искать продолжающий этот нулевой корень ряд Пюизо в виде

$$x(t) = c_1 t^{\varepsilon_1} + c_2 t^{\varepsilon_1+\varepsilon_2} + c_3 t^{\varepsilon_1+\varepsilon_2+\varepsilon_3} + \cdots \tag{4-34}$$

с положительными $\varepsilon_i \in \mathbb{Q}$ и ненулевыми $c_i \in \Bbbk$. На координатной плоскости отметим все такие целые точки (p,q), что моном[1] $x^p t^q$ входит в $F(t,x)$ с ненулевым коэффициентом, и возьмём их выпуклую оболочку. Полученная фигура называется *многоугольником Ньютона* многочлена $F(t,x)$. Видимая из начала координат часть границы многоугольника Ньютона представляют собою ломаную, все вершины которой располагаются в некоторых из точек (m,μ_m), отвечающих младшим по t членам коэффициентов

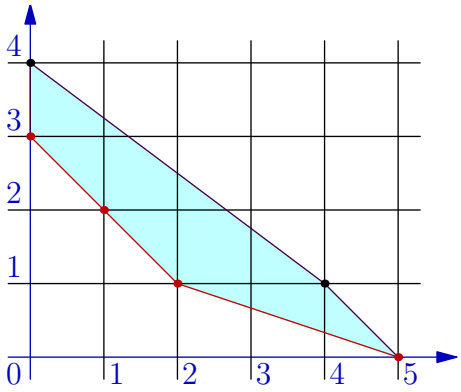


Рис. 4⋄1.

$$a_m(t) = \alpha_{\mu_m}\, t^{\mu_m} + \text{старшие степени } t$$

многочлена $F(t,x) = \sum\limits_m a_m(t)\,x^m$. Мы будем называть эту ломаную *ломаной Ньютона*. На рис. 4⋄1 показан многоугольник Ньютона многочлена

$$(-t^3 + t^4) - 2t^2\,x - t\,x^2 + 2t\,x^4 + x^5\,. \tag{4-35}$$

Его ломаная Ньютона состоит из двух красных отрезков.

Упражнение 4.18. Приведите пример такого многочлена, что не все точки (m,μ_m) лежат на ломаной Ньютона.

[1] обратите внимание, что мы откладываем показатели при x вдоль *горизонтальной* оси

Подставим ряд (4-34) вместо x в многочлен $F(t,x)$. Младшие по t члены в $x^m(t)$ и $a_m(t)$ перемножатся в одночлен

$$a_{\mu_m} c_1^m t^{m\varepsilon_1+\mu_m}\,. \tag{4-36}$$

Несколько таких одночленов можно сократить друг с другом за счёт надлежащего подбора коэффициента c_1 у ряда (4-34), если и только если они имеют один и тот же показатель при t, т. е. когда у них одно и то же значение $m\varepsilon_1+\mu_m$. Такие одночлены происходят из мономов $x^p t^q$, лежащих на прямой $p\varepsilon_1+q=\text{const}$, содержащей одно из звеньев ломаной Ньютона. Таким образом, в качестве показателя ε_1 должно выступать отношение α/β координат вектора $n=(\alpha,\beta)$, перпендикулярного какому-нибудь звену ломаной Ньютона. И чтобы одночлены (4-36), приходящие из всех лежащих на выбранном звене мономов $x^p t^q$, сократились друг с другом, константа c_1, отвечающая такому ребру, должна удовлетворять уравнению

$$a_{\mu_k} + b_{\mu_{k+1}} c_1 + b_{\mu_{k+2}} c_1^2 + \cdots + b_{\mu_{k+\ell-1}} c_1^{\ell-1} + a_{\mu_{k+\ell}} c_1^{\ell}\,, \tag{4-37}$$

где $k,\ k{+}1,\ \ldots\ ,\ k{+}\ell$ суть целые точки горизонтальной оси, накрываемые горизонтальной проекцией выбранного ребра, ℓ — длина этой проекции, а коэффициенты

$$b_{\mu_{k+i}} = \begin{cases} a_{\mu_{k+i}} & \text{когда точка } (k+i, a_{\mu_{k+i}}) \text{ лежит на ребре} \\ 0 & \text{когда точка } (k+i, a_{\mu_{k+i}}) \text{ лежит выше ребра.} \end{cases}$$

Если обозначить через γ значение линейной функции $p\varepsilon_1+q$ на выбранном ребре[1] и сгруппировать в F вместе мономы, расположенные на прямых $p\varepsilon_1+q=\text{const}$:

$$F(t,x)=\sum_{k\geqslant\gamma} f_k(t,x)\,,\quad \text{где}\quad f_k(t,x)=\sum_{\substack{p,q:\\ p\varepsilon_1+q=k}} a_{p,q}x^p t^q\,, \tag{4-38}$$

то уравнение (4-37) будет иметь вид $f_\gamma(1,c_1)=0$.

Чтобы найти следующие значения ε_2 и c_2 , мы выбираем один из корней этого уравнения, подставляем в F значение $x=t^{\varepsilon_1}(c_1+x_1)$. От такой подстановки каждое слагаемое $f_k(t,x)$ в сумме (4-38) превратится в $t^k f_k(1,c_1+x_1)$. В результате уравнение на x_1 можно будет сократить на t^γ. Если выбранный корень c_1 имеет кратность d, т. е.

$$f_\gamma(1,x)=(x-c_1)^d g(x)\,,\quad \text{где}\quad g(c_1)\neq 0\,,$$

то $f_\gamma(1,c_1+x_1)=x_1^d g(c_1)+$ старшие степени x_1 . Поэтому после сокращения на t^γ уравнение на x_1 будет содержать с ненулевым коэффициентом моном t^0x^d, а значит, его ломаная Ньютона выйдет на горизонтальную ось не правее точки $(d,0)$, и длины горизонтальных проекций всех её рёбер будут не больше кратности выбранного корня c_1.

Упражнение 4.19. Докажите лем. 4.5 непосредственно следуя методу Ньютона. Для этого проверьте, что а) знаменатель дроби $\varepsilon_1\in\mathbb{Q}$ не превосходит длины ℓ горизонтальной проекции выбранного звена ломаной Ньютона б) если в ломаной Ньютона для уравнения на x_1 окажется ребро с той же длиной ℓ горизонтальной проекции, то $\varepsilon_1\in\mathbb{N}$. Выведите из этих утверждений, что результатом вычисления по методу Ньютона является ряд Пюизо (4-34), являющийся корнем многочлена $F(t,x)$.

[1] т. е. общий показатель у t во всех сокращаемых мономах (4-36)

Итак, вычисление по методу Ньютона состоит в том, что для каждого из рёбер ломаной Ньютона многочлена $F(t,x)$ и каждого корня c_1 уравнения (4-37) мы подставляем $x = t^{\varepsilon_1}(c_1 + x_1)$ в многочлен F, делим результат на t^γ, и повторяем процедуру к полученному многочлену от x_1, находя следующие ε_2 и c_2 в разложении (4-34), и т. д.

Например, для многочлена (4-35) вектор нормали к левому звену ломаной Ньютона на рис. 4⋄1 равен $(1,1)$. Поэтому $\varepsilon_1 = 1$, а c_1 удовлетворяет уравнению $-1 - 2c_1 - c_1^2 = 0$, имеющему двукратный корень $c_1 = -1$. Подставляя $x = t(x_1 - 1)$ в (4-35) и деля на t^3, получаем[1] многочлен

$$-x_1^2 + t + t^2(-1+x_1)^4(1+x_1) = (t+t^2) - 3t^2\,x_1 + (-1+2t^2)\,x_1^2 + 2t^2\,x_1^3 - 3\,x^2\,x_1^4 + t^2\,x_1^5 \quad (4\text{-}39)$$

с многоугольником Ньютона, показанным на рис. 4⋄2. Его ломаная Ньютона состоит из единственного звена с вектором нормали $(1,2)$, что даёт $\varepsilon_2 = 1/2$ и уравнение $-1 - c_2^2 = 0$ с двумя корнями $c_2 = \pm 1$. Беря $c_2 = 1$ и подставляя $x_1 = x^{1/2}(1 + x_2)$ в 4-39, получаем многочлен вида

$$(t - 3t^{3/2} + \cdots) + (-2 - 3t^{3/2} + \cdots)\,x_2 + \\ + (-1 - 2t^3 + \cdots)\,x_2^2 + \cdots .$$

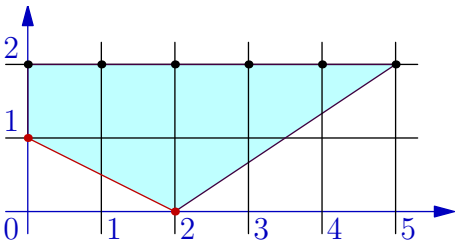


Рис. 4⋄2.

Его ломаная Ньютона состоит из единственного звена, соединяющего точки $(0,1)$ и $(1,0)$. По упр. 4.19, на всех последующих шагах ломаная Ньютона будет также состоять из единственного звена, соединяющего точки $(0,1)$ и $(1,0)$, так что получающееся на этом пути решение является степенным рядом от $t^{1/2}$. Теперь мы можем записать этот ряд с неопределёнными коэффициентами, подставить в F, и найти коэффициенты.

Вектор нормали к правому звену ломаной на рис. 4⋄1 равен $(1,3)$, что даёт $\varepsilon_1 = 1/3$ и уравнение $-1 + c_1^3 = 0$, имеющее корни $c_1 = 1$, ω, ω^2, где $\omega \in \Bbbk$ — первообразный кубический корень из единицы. Беря $c_2 = \omega$, подставляя $x = t^{1/3}(\omega + x_1)$ в (4-35) и сокращая на $t^{5/3}$, получаем многочлен

$$(-t^{4/3} + t^{7/3}) + (3\omega + 6t^{2/3})\,x_1 + (9 + 12\omega^2 t^{2/3})\,x_1^2 + (10\omega^2 + 8\omega t^{2/3})\,x_1^3 + (5\omega + 2t^{2/3})\,x_1^4 + x_1^5\,,$$

ломаная Ньютона которого опять-таки состоит из единственного звена, соединяющего точки $(0,1)$ и $(1,0)$, так что искомое решение является степенным рядом с натуральными показателями от $x^{1/3}$, и его можно вычислять методом неопределённых коэффициентов.

[1] в ходе этого вычисления удобно сгруппировать вместе мономы $x^p t^q$, лежащие на параллельных выбранному ребру прямых $p + q = \mathrm{const}$

§5. Идеалы, фактор кольца и разложение на множители

5.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 2.6.3 мы видели, что этими свойствами обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Этот идеал обозначается

$$(a) = \{ka \mid k \in K\}, \tag{5-1}$$

и называется *главным* идеалом, порождённым a. Мы встречались с главными идеалами при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра эпиморфизмов

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n),\ m \mapsto [m]_n, \qquad \text{и} \qquad \Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f),\ g \mapsto [g]_f,$$

сопоставляющих целому числу (соотв. многочлену) его класс вычетов. Ещё в любом кольце K имеются *тривиальные* идеалы $(0) = \{0\}$ и $(1) = K$.

Упражнение 5.1. 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 обратимый элемент.

Предложение 5.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.

Доказательство. Из упр. 5.1 вытекает, что ни в каком поле нетривиальных идеалов нет. Наоборот, если в кольце нет нетривиальных идеалов, то главный идеал (b), порождённый любым ненулевым элементом b, совпадает со всем кольцом и, в частности, содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент обратим. □

5.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде

$$b_1a_1 + b_2a_2 + \cdots + b_ma_m, \tag{5-2}$$

где $a_1, a_2, \ldots, a_m$ — произвольные элементы множества M, $b_1, b_2, \ldots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 5.2. Убедитесь, что $(M) \subset K$ это и в самом деле идеал

Всякий идеал $I \subset K$ имеет вид (M) для подходящего $M \subset K$: например, можно положить $M = I$. Идеал $I \subset M$ называется *конечно порождённым*, если его можно породить конечным множеством M, т. е. если существуют такие $a_1, a_2, \ldots, a_k \in I$, что

$$I = (a_1, a_2, \ldots, a_k) = \{b_1a_1 + b_2a_2 + \cdots + b_ka_k \mid b_i \in K\}.$$

Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 5.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов $a_1, a_2, \dots, a_k \in M$, порождающий тот же идеал, что и M

2) любой идеал $I \subset K$ конечно порождён

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

Доказательство. Ясно, что (1) $\Rightarrow$ (2). Чтобы из (2) вывести (3), заметим, что объединение $I = \bigcup I_\nu$ всех идеалов цепочки тоже является идеалом. Согласно (2), идеал I порождён конечным набором элементов. Все они принадлежат некоторому идеалу I_n. Тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3), будем по индукции строить цепочку идеалов $I_n = (a_1, a_2, \dots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \setminus I_{k-1}$ до тех пор, пока это возможно, т. е. пока $M \not\subset I_k$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий всё множество M, а значит, совпадающий с (M). □

Определение 5.1
Кольцо K, удовлетворяющее условиям лем. 5.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 5.1
Если кольцо K нётерово, то кольцо многочленов $K[x]$ также нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени $\leqslant d$ из I, объединённое с нулём, а через $L_\infty = \bigcup\limits_d L_d$ — множество старших коэффициентов вообще всех многочленов из I, также объединённое с нулём.

Упражнение 5.3. Убедитесь, что все L_d (включая L_∞) являются идеалами в K.

Поскольку кольцо K нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, f_2^{(d)}, \dots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$ (их старшие коэффициенты порождают идеал L_∞) равна $D \in \mathbb{N}$. Покажем, что идеал I порождается многочленами f_i^∞ и многочленами $f_j^{(d)}$ с $0 \leqslant d < D$.

Произвольный многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, поскольку старший коэффициент многочлена g лежит в идеале L_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in K$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности

$$m_i = \deg g - \deg f_i^{(\infty)} \geqslant 0\,,$$

так что мы можем образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{m_i}$, сравнимый с g по модулю I и имеющий строго меньшую, чем g степень. Заменим g на h и повторим эту процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем сокращать его старший член и строго уменьшать степень, вычитая из h подходящие комбинации многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 5.1
Если K нётерово, то кольцо многочленов $K[x_1, x_2, \dots, x_n]$ также нётерово. □

Упражнение 5.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 5.2
В нётеровом кольце любая бесконечная система полиномиальных уравнений эквивалентна некоторой своей конечной системе.

Доказательство. Пусть имеется бесконечный набор уравнений $f_\nu(x_1, x_2, \dots, x_n) = 0$, где $f_\nu \in K[x_1, x_2, \dots, x_n]$. Если K нётерово, то $K[x_1, x_2, \dots, x_n]$ тоже нётерово, и среди многочленов f_ν можно выбрать такой конечный набор $f_1, f_2, \dots, f_m$, что каждый из многочленов f_ν будет представляться в виде $f_\nu = g_1 f_1 + g_2 f_2 + \dots + g_m f_m$, а значит, обратится в нуль на любом решении конечной системы $f_1 = f_2 = \dots = f_m = 0$. □

5.1.2. Примеры ненётеровых колец. Кольцо многочленов от бесконечного числа переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементами которого, по определению, являются всевозможные конечные суммы взятых с рациональными коэффициентами конечных произведений вида $x_{\nu_1}^{m_1} x_{\nu_2}^{m_2} \cdots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 5.5. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \to \mathbb{R}$ всеми функциями, которые обращаются в нуле в нуль вместе со всеми своими производными.

Предостережение 5.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 5.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 5.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов с комплексными коэффициентами.

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

$$\pi : K \twoheadrightarrow X, \tag{5-3}$$

переводящее элемент $a \in K$ в его класс эквивалентности $\pi(a) = [a] \in X$. Мы хотим задать на множестве X структуру коммутативного кольца так, чтобы отображение (5-3) оказалось гомоморфизмом колец, или — что то же самое — так, чтобы сложение и умножение классов задавалось формулами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab]. \tag{5-4}$$

Из установленных нами в n° 2.6.3 свойств гомоморфизмов колец вытекает, что в этом случае класс $[0]$, содержащий $0 \in K$ и должный быть ядром гомоморфизма (5-3), с необходимостью является идеалом кольца K, а все остальные слои гомоморфизма (5-3) суть аддитивные сдвиги ядра на элементы кольца K, т. е.

$$\forall\, a \in K \quad [a] = a + [0] = \{a + b \mid b \in [0]\}\,.$$

Оказывается, что этих условий и достаточно: для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{5-5}$$

образует разбиение кольца K, и правила (5-4) корректно определяют на нём структуру коммутативного кольца с единицей $[1]_I$ и нулём $[0]_I = I$.

Упражнение 5.7. Убедитесь, что отношение сравнимости по модулю идеала

$$a_1 \equiv a_2 \pmod{I}\,,$$

означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, разбивающим K в точности на классы (5-5), и проверьте, что формулы (5-4) корректно определены на этих классах.

Определение 5.2
Классы эквивалентности (5-5) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (5-4) называется *фактор кольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм

$$K \twoheadrightarrow K/I\,, \quad a \mapsto [a]_I\,, \tag{5-6}$$

сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*

Пример 5.1 (кольца вычетов)
Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть фактор кольца кольца целых чисел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 5.2 (образ гомоморфизма)
Согласно n° 2.6.3, образ любого гомоморфизма коммутативных колец $\varphi : K_1 \to K_2$ канонически изоморфен фактор кольцу $K_1/\ker(\varphi)$. При этом изоморфизме элементу

$$b = \varphi(a) \in \operatorname{im}\varphi \subset K_2$$

отвечает класс вычетов $[a]_{\ker\varphi} = \varphi^{-1}(b)$.

Упражнение 5.8. Покажите, что фактор кольцо нётерова кольца тоже нётерово.

Пример 5.3 (максимальные идеалы и гомоморфизмы вычисления)
Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если фактор кольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что идеал $\mathfrak{m} \subset K$ максимален, если и только если он собственный[1] и не

[1] отличен от $(0) = 0$ и $(1) = K$

содержится ни в каком строго большем собственном идеале. В самом деле, обратимость класса элемента $a \in K \setminus \mathfrak{m}$ в фактор кольце $K/\mathfrak{m}$ означает существование таких элементов $b \in K$ и $x \in \mathfrak{m}$, что $ab = 1 + x$ в K. А это, в свою очередь, означает, что идеал, порождённый $\mathfrak{m}$ и любым элементом $a \in K \setminus \mathfrak{m}$ содержит 1.

Упражнение 5.9. При помощи леммы Цорна[1] покажите, что любой идеал произвольного коммутативного кольца с единицей содержится в некотором максимальном идеале.

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

Упражнение 5.10. Убедитесь, что каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$, и приведите пример максимального идеала $\mathfrak{m} \subset \mathbb{R}[x]$, отличного от всех идеалов $\ker \mathrm{ev}_p$ с $p \in \mathbb{R}$.

Упражнение 5.11. Покажите, что каждый максимальный идеал кольца непрерывных функций $[0, 1] \to \mathbb{R}$ имеет вид $\ker \mathrm{ev}_p$ для некоторой точки $p \in [0, 1]$.

Пример 5.4 (простые идеалы и гомомрфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*, если в фактор кольце $K/\mathfrak{p}$ нет делителей нуля. Иначе говоря, идеал $\mathfrak{p} \subset K$ прост, если и только если из $ab \in \mathfrak{p}$ вытекает, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, главные идеалы $(p) \subset \mathbb{Z}$ и $(q) \subset \Bbbk[x]$, где $\Bbbk$ — поле, просты тогда и только тогда, когда число p просто, а многочлен q неприводим.

Упражнение 5.12. Убедитесь в этом.

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

Упражнение 5.13. Докажите, что простой идеал $\mathfrak{p} \subset A$ содержит пересечение конечного набора произвольных идеалов только тогда, когда он содержит хотя бы один из них.

[1] напомним, что *лемма Цорна* утверждает, что если в частично упорядоченном множестве X любое линейно упорядоченное подмножество $Y \subset X$ имеет верхнюю грань (т. е. $\exists\, x \in X : \forall\, y \in Y\ y \leqslant x$), то в X существует такой элемент μ, что $\forall\, x \in X\ \ \mu \leqslant x \Rightarrow x = \mu$

5.2.1. Конечно порождённые коммутативные алгебры. Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида $A = K[x_1, x_2, \dots, x_n]/I$, где $I \subset K[x_1, x_2, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[1]. Классы $a_i = x_i \pmod I$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями* между этими образующими.

Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв $a_1, a_2, \dots, a_n$ при помощи операций сложения и умножения, которые совершаются с учётом полиномиальных соотношений $f(a_1, a_2, \dots, a_n) = 0$, где f пробегает I. Из упр. 5.8 и сл. 5.1 мы получаем

Следствие 5.3
Всякая конечно порождённая коммутативная алгебра над нётеровым кольцом нётерова и все соотношения между её образующими являются следствиями конечного числа соотношений. □

5.3. Кольца главных идеалов. Целостное кольцо с единицей называется *кольцом главных идеалов*, если каждый его идеал является главным. Параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, который мы наблюдали выше, объясняется тем, что оба эти кольца являются кольцами главных идеалов. Мы фактически доказали это, когда строили в этих кольцах наибольший общий делитель. Ниже мы воспроизведём это доказательство ещё раз таким образом, чтобы оно годилось для чуть более широкого класса колец, допускающих *деление с остатком*.

5.3.1. Евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если существует *функция высоты* (или *евклидова норма*) $\nu : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$, сопоставляющая каждому ненулевому элементу $a \in K$ целое неотрицательное число $\nu(a)$ так, что $\forall\, a, b \in K \setminus \{0\}$ выполняются два свойства:

$$\nu(ab) \geqslant \nu(a) \tag{5-7}$$

$$\exists\, q, r \in K \ : \ a = bq + r \ \text{ и либо } \nu(r) < \nu(b), \text{ либо } r = 0\,. \tag{5-8}$$

Элементы q и r из (5-8), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Упражнение 5.14. Докажите евклидовость колец: а) $\mathbb{Z}$, $\nu(z) = |z|$ б) $\Bbbk[x]$, $\nu(f) = \deg f$
в) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mid a, b \in \mathbb{Z},\ i^2 = -1\}$, $\nu(z) = |z|^2$
г) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\,\}$, $\nu(z) = |z|^2$.

Все четыре кольца из предыдущего упражнения являются кольцами главных идеалов в силу следующей теоремы.

Предложение 5.2
Любое евклидово кольцо является кольцом главных идеалов[2].

[1] или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K

[2] отметим, что обратное неверно, но контрпримеры приходят из достаточно продвинутой арифметики и геометрии, и для их содержательного обсуждения требуется техника, которой мы пока не владеем (впрочем, см. замечание 3 на стр. 365 книги *Э. Б. Винберг.* Курс алгебры. М. «Факториал», 1999)

Доказательство. Пусть $I \subset K$ — идеал, и $d \in I$ — ненулевой элемент наименьшей высоты. Покажем, что каждый элемент $a \in I$ делится на d. Поделим a на d с остатком: $a = dq + r$. Так как $a, d \in I$, остаток $r = a - dq \in I$. Поскольку строгое неравенство $\nu(r) < \nu(d)$ невозможно, мы заключаем, что $r = 0$. □

Упражнение 5.15. Покажите, что в любом евклидовом кольце равенство $\nu(ab) = \nu(a)$ в свойстве (5-7) равносильно тому, что элемент b обратим.

5.3.2. НОД и взаимная простота. В кольце главных идеалов K у любого набора элементов $a_1, a_2, \dots, a_n$ есть наибольший общий делитель $d = \text{нод}(a_1, a_2, \dots, a_n) \in K$, делящий каждый из элементов a_i и делящийся на любой другой общий делитель. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным. В самом деле, поскольку

$$(a_1, a_2, \dots, a_n) = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in K\} = (d)$$

для некоторого $d \in K$, элемент 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.

Отметим, что наибольший общий делитель d определён не однозначно, а с точностью до умножения на произвольный обратимый элемент кольца.

Упражнение 5.16. В любом целостном коммутативном кольце K равенство ненулевых главных идеалов $(a) = (b)$ равносильно тому, что $a = sb$, где $s \in K$ обратим.

Поэтому всюду в дальнейшем обозначение $\text{нод}(a_1, a_2, \dots, a_n)$ подразумевает некоторый класс элементов, рассматриваемых с точностью до умножения на обратимую константу, и все формулы, которые будут писаться, будут относиться к произвольно выбранному конкретному представителю этого класса.

Из наличия представления $\text{нод}(a_1, a_2, \dots, a_n) = x_1a_1 + x_2a_2 + \cdots + x_na_n$ вытекает, что в любом кольце главных идеалов отсутствие необратимых общих делителей у элементов $a_1, a_2, \dots, a_n$ равносильна их *взаимной простоте*, т. е. возможности представить единицу кольца в виде[1] $1 = x_1a_1 + x_2a_2 + \cdots + x_na_n$ с подходящими $x_i \in K$.

5.4. Факториальность. Всюду в этом разделе мы обозначаем через K *целостное*[2] кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Из равенств $a = mb$ и $b = na = nmb$ вытекает равенство $b(1 - nm) = 0$, откуда $mn = 1$. Таким образом, ассоциированность элементов означает, что они 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 $a = \pm b$.

5.4.1. Неприводимые элементы. Напомним, что элемент $q \in K$ называется *неприводимым*, если он необратим, и из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, главный идеал q не содержится строго ни в каком другом главном идеале, т. е. максимален в множестве главных идеалов. Например, неприводимыми элементами в кольце целых чисел являются простые числа, а в кольце многочленов — неприводимые многочлены.

[1] иначе взаимную простоту $a_1, a_2, \dots, a_n$ можно описать равенством $(a_1, a_2, \dots, a_n) = K$

[2] т. е. с единицей и без делителей нуля

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[1], либо ассоциированы, поскольку порождённый ими идеал $(p, q) = (d)$ для некоторого $d \in K$, и в силу сказанного выше из $(p) \subset (d)$ и $(q) \subset (d)$ вытекает, что либо $(d) = (K) = (1)$, либо $(d) = (p) = (q)$.

В произвольном кольце два неассоциированных неприводимых элемента могут не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ элементы x и y не взаимно просты и не ассоциированы.

Предложение 5.3
В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:

1) фактор кольцо $K/(p)$ является полем

2) в фактор кольце $K/(p)$ нет делителей нуля

3) p неприводим, т. е. $p = ab \Rightarrow a$ или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) тривиальна и имеет место в любом кольце[2] K. Покажем, что в любом целостном кольце[3] K 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). Коль скоро в K нет никаких иных идеалов, кроме главных, максимальность идеала (p) в множестве главных идеалов означает, что он максимален в множестве всех собственных идеалов. Согласно прим. 5.3 на стр. 72, это равносильно тому, что $K/(p)$ — поле. □

Упражнение 5.17. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

Предложение 5.4
В любом нётеровом кольце всякий элемент является произведением конечного числа неприводимых.

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

[1] в смысле опр. 2.2 на стр. 21, т. е. найдутся $x, y \in K : px + qy = 1$

[2] см. n° 2.4.1 на стр. 22

[3] не обязательно являющемся кольцом главных идеалов

Определение 5.3
Целостное кольцо называется *факториальным*, если каждый его необратимый элемент является произведением конечного числа неприводимых элементов, причём любые два таких разложения $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_k$ состоят из одинакового числа сомножителей $k = m$, и после надлежащей их перенумерации найдутся такие обратимые элементы s_ν, что $q_\nu = p_\nu s_\nu$ при всех ν.

5.4.2. Простые элементы. Элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в фактор кольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ из того, что произведение ab делится на p, вытекает, что a или b делится на p.

Всякий простой элемент p автоматически неприводим: если $p = xy$, то один из сомножителей, скажем x, делится на p, и тогда $p = pyz$, откуда $yz = 1$ и y обратим. Согласно предл. 5.3 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты.

Однако, в общей ситуации простота является более сильным свойством, чем неприводимость. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ число 2 неприводимо, но не просто, поскольку в фактор кольце

$$\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) = \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\left((x+1)^2\right)$$

есть делитель нуля $(x+1) \pmod{(2, x^2+1)}$. Это означает, что число $1+\sqrt{5}$ не делится на 2 в $\mathbb{Z}[\sqrt{5}]$, а его квадрат $(1+\sqrt{5})^2 = 6 + 2\sqrt{5}$ — делится, несмотря на то, что 2 является *неприводимым* элементом кольца $\mathbb{Z}[\sqrt{5}]$.

Упражнение 5.18. Убедитесь, что 2, $\sqrt{5}+1$, $\sqrt{5}-1$ неприводимы и попарно неассоциированы в кольце $\mathbb{Z}[\sqrt{5}]$. Из этого вытекает, в частности, что 4 имеет в $\mathbb{Z}[\sqrt{5}]$ два *различных* разложения на неприводимые множители: $2 \cdot 2 = 4 = \left(\sqrt{5}+1\right)\cdot\left(\sqrt{5}-1\right)$.

Предложение 5.5
Целостное нётерово кольцо K факториально тогда и только тогда, когда все его неприводимые элементы просты.

Доказательство. Покажем, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Таким образом, разложение ab на неприводимые множители содержит множитель, ассоциированный с q. В силу единственности, разложение произведения ab является произведением разложений a и b. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q, что и требовалось.

Пусть теперь все неприводимые элементы просты. В нётеровом кольце каждый элемент является произведением конечного числа неприводимых. Покажем, что в любом целостном кольце равенство

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m\,, \tag{5-9}$$

где все сомножители просты, возможно только если $k = m$ и каждый p_i ассоциирован с q_i (может быть, после надлежащей перенумерации). Коль скоро произведение в правой части (5-9) делится на p_1, один из сомножителей этого произведения делится на p_1.

Будем считать, что это $q_1 = sp_1$. Поскольку q_1 неприводим, элемент s обратим. Пользуясь целостностью кольца K, сокращаем равенство (5-9) на p_1 и получаем более короткое равенство $p_2 p_3 \cdots p_k = (sq_2)q_3 \cdots q_m$, к которому применимы те же рассуждения. □

Следствие 5.4
Всякое кольцо главных идеалов факториально. □

Пример 5.5 (суммы двух квадратов, продолжение прим. 3.5 на стр. 45)
Согласно упр. 5.14, 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. В $\mathbb{Z}[i]$ разложение любого целого вещественного числа, будучи инвариантным относительно комплексного сопряжения, содержит вместе с каждым невещественным неприводимым множителем также и сопряжённый ему множитель. Поэтому простое $p \in \mathbb{Z}$, не являющееся простым в $\mathbb{Z}[i]$, представляется в виде

$$p = (a + ib)(a - ib) = a^2 + b^2 \quad \text{с ненулевыми } a, b \in \mathbb{Z}\,.$$

Таким образом, простое $p \in \mathbb{Z}$ тогда и только тогда приводимо в $\mathbb{Z}[i]$, когда p является суммой двух квадратов. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что фактор кольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[1], что равносильно неприводимости многочлена $x^2 + 1$ над $\mathbb{F}_p$, т. е. отсутствию у него корней в $\mathbb{F}_p$. Мы заключаем, что простое $p \in \mathbb{Z}$ является суммой двух квадратов, если и только если -1 квадратичный вычет по модулю p. Как мы видели в n° 3.5.2 на стр. 48, это происходит в точности тогда, когда $(p-1)/2$ чётно, т. е. для простых $p = 4k + 1$ и $p = 2$.

Упражнение 5.19. Покажите, что натуральное число n тогда и только тогда является квадратом или суммой двух квадратов натуральных чисел, когда в его разложение на простые множители простые числа $p = 4k + 3$ входят лишь в чётных степенях.

5.4.3. НОД в факториальном кольце. В факториальном кольце K наибольший общий делитель набора элементов $a_1, a_2, \ldots, a_m \in K$ допускает следующее описание. Для каждого класса ассоциированных неприводимых элементов $q \in K$ обозначим через m_q максимальное целое число, такое что q^{m_q} делит каждое из чисел a_i. Тогда, с точностью до умножения на обратимые константы,

$$\text{нод}(a_1, a_2, \ldots, a_m) = \prod_q q^{m_q}\,.$$

Так как любой элемент факториального кольца является произведением конечного числа неприводимых, числа m_q отличны от нуля лишь для конечного числа классов q. Поэтому написанное произведение корректно определено и, в силу факториальности K, делится на любой общий делитель чисел a_i.

[1] см. предл. 5.3 на стр. 76

5.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо многочленов $K[x]$ является подкольцом в кольце многочленов $Q_K[x]$. Назовём *содержанием* многочлена

$$f = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in K[x]$$

наибольший общий делитель $\operatorname{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \ldots, a_n)$ его коэффициентов.

Лемма 5.2
$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ для любых $f, g \in K[x]$.

Доказательство. Достаточно для каждого неприводимого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg, если и только если q делит все коэффициенты одного из многочленов f, g. Поскольку неприводимые элементы факториального кольца просты, фактор кольцо $R = K/(q)$ целостное. Применим к произведению fg гомоморфизм

$$K[x] \to R[x], \quad f \mapsto [f]_q,$$

редукции по модулю q, заменяющий коэффициенты многочленов на их классы вычетов по модулю q. Так как кольцо $R[x]$ тоже целостное, произведение $[fg]_q = [f]_q [g]_q$ обращается в нуль, если и только если один из сомножителей $[f]_q$, $[g]_q$ равен нулю. □

Лемма 5.3 (редуцированное представление)
Каждый многочлен $f(x) \in Q_K[x]$ представляется в виде $f(x) = \frac{a}{b} \cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$, и $\operatorname{cont}(f_{\text{red}}) = \text{нод}(a, b) = 1$, причём числа a, b и многочлен f_{red} определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Вынесем из коэффициентов f их общий знаменатель, потом вынесем из всех коэффициентов полученного многочлена их наибольший общий делитель. В результате мы получим многочлен содержания 1, умноженный на число из Q_K, которое запишем несократимой дробью a/b. Докажем единственность такого представления.

Если $(a/b) \cdot f_{\text{red}}(x) = (c/d) \cdot g_{\text{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, получаем $ad = bc$. В виду отсутствия общих неприводимых множителей и у a и b, и у c и d, это возможно, только если a ассоциирован с c, а b — с d. Но тогда с точностью до умножения на обратимую константу и $f_{\text{red}}(x) = g_{\text{red}}(x)$. □

Следствие 5.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в кольце $Q_K[x]$ тогда и только тогда, когда он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в редуцированном виде из лем. 5.3 и сокращая возникающую дробь, приходим к равенству

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

в котором $g_{\text{red}}, h_{\text{red}} \in K[x]$ имеют содержание 1, и $\text{нод}(a, b) = 1$ несократима. По лем. 5.2 содержание произведения $g_{\text{red}} h_{\text{red}}$ также равно 1, так что написанное выше равенство даёт редуцированное представление для многочлена f. В силу его единственности, элементы a и b обратимы в K, а $f = g_{\text{red}} h_{\text{red}}$ с точностью до умножения на обратимую константу. □

Теорема 5.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Так как кольцо главных идеалов $Q_K[x]$ факториально, всякий многочлен $f \in K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в редуцированном виде из лем. 5.3 и сокращая числовую дробь, получаем равенство $f = \frac{a}{b}\prod f_{\nu,\mathrm{red}}$, в котором $f_{\nu,\mathrm{red}} \in K[x]$ — многочлены содержания 1, неприводимые в $Q_K[x]$ (и, тем более, в $K[x]$), а $a, b \in K$ взаимно просты. Поскольку $\operatorname{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$, это равенство даёт редуцированное представление для $f = \operatorname{cont}(f)\cdot f_{\mathrm{red}}$. В силу его единственности, $b = 1$ и $f = a\prod f_{\nu,\mathrm{red}}$ с точностью до умножения на обратимые константы из K. Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$.

Докажем единственность такого разложения. Пусть в $K[x]$ выполняется равенство

$$a_1a_2\cdots a_k\cdot p_1p_2\cdots p_s = b_1b_2\cdots b_m\cdot q_1q_2\cdots q_r\,,$$

в котором $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ — неприводимые многочлены. Поскольку неприводимые многочлены имеют содержание 1, сравнивая содержание обеих частей, приходим к равенству $a_1a_2\cdots a_k = b_1b_2\cdots b_m$ в K. В силу факториальности K, имеем $k = m$ и (после надлежащей перенумерации сомножителей) $a_i = s_ib_i$, где s_i обратимы. Следовательно, с точностью до умножения на обратимую константу из K в кольце многочленов $K[x]$ выполняется равенство $p_1p_2\cdots p_s = q_1q_2\cdots q_r$. В силу факториальности $Q_K[x]$ и неприводимости p_i и q_i также и в $Q_K[x]$, мы заключаем, что $r = s$ и (после надлежащей перенумерации сомножителей) $p_i = q_i$ с точностью до постоянного множителя из Q_K. Из единственности редуцированного представления (лем. 5.3) вытекает, что эти постоянные множители являются обратимыми константами из K. □

Следствие 5.6
Если K — факториальное кольцо (скажем, область главных идеалов или поле), то кольцо многочленов $K[x_1, x_2, \dots, x_n]$ от любого числа переменных факториально. □

5.6. Разложение многочленов с целыми коэффициентами. Разложение многочлена $f \in \mathbb{Z}[x]$ на множители в $\mathbb{Q}[x]$ разумно начать с отыскания его рациональных корней, что делается за конечное число проб.

Упражнение 5.20. Покажите, что несократимая дробь $a = p/q \in \mathbb{Q}$ может быть корнем многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$, только если p делит a_0, а q делит a_n.

Точное знание комплексных корней f тоже весьма полезно при разложении в $\mathbb{Z}[x]$.

Упражнение 5.21. Разложите x^4+4 в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения исчерпаны, можно попробовать более трудоёмкие способы.

5.6.1. Редукция коэффициентов многочлена $f \in \mathbb{Z}[x]$ по модулю m

$$\mathbb{Z}[x] \to \big(\mathbb{Z}/(m)\big)[x]\,, \quad f \mapsto [f]_m \tag{5-10}$$

переводит полином $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ с целыми коэффициентами в полином $\big[a_n\big]_m x^n + \big[a_{n-1}\big]_m x^{n-1} + \cdots + \big[a_1\big]_m x + \big[a_0\big]_m$ с коэффициентами в $\mathbb{Z}/(m)$ и является

гомоморфизмом колец[1]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$, так что из неприводимости многочлена $[f]_m$ хотя бы при одном m вытекает его неприводимость в $\mathbb{Z}[x]$.

Если число $m = p$ простое, кольцо коэффициентов $\mathbb{Z}/(m) = \mathbb{F}_p$ является полем, и кольцо многочленов $\mathbb{F}_p[x]$ в этом случае факториально. При малых p разложение многочлена небольшой степени на неприводимые множители в $\mathbb{F}_p[x]$ можно осуществить простым перебором, и анализ полученного разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

Пример 5.6
Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Сделаем редукцию по модулю 2. Так как у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Но единственный неприводимый многочлен второй степени в $\mathbb{F}_2[x]$ это $x^2 + x + 1$, и $x^5 + x^2 + 1$ на него не делится. Тем самым, $[f]_2$ неприводим над $\mathbb{F}_2$, а значит, и над $\mathbb{Z}$.

Пример 5.7 (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. Покажем, что f неприводим в $\mathbb{Z}[x]$. В силу сделанных предположений об f при редукции по модулю p от него остаётся только старший моном $[f(x)]_p = x^n$. Если $f(x) = g(x)h(x)$ в $\mathbb{Z}[x]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[x]$ оба сомножителя g, h тоже должны редуцироваться в чистые степени $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все их коэффициенты кроме старшего, делятся на p. Но тогда младший коэффициент f, будучи произведением младших коэффициентов g, h, должен делиться на p^2, что не так.

Пример 5.8 (неприводимость кругового многочлена Φ_p)
Покажем, что круговой многочлен $\Phi_p(x) = x^{p-1} + x^{p-2} + \ \cdots\ + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$ при простом p. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = \frac{(t+1)^p - 1}{t} = t^p + \binom{p}{1} t^{p-1} + \ \cdots\ + \binom{p}{p-1} t$$

и применим критерий Эйзенштейна из прим. 5.7.

5.6.2. Алгоритм Кронекера позволяет путём эффективного, но довольно трудоёмкого вычисления либо явно найти разложение заданного многочлена с целыми коэффициентами в кольце $\mathbb{Z}[x]$, либо убедиться, что его нет[2]. Пусть $\deg f = 2n$ или $\deg f = 2n + 1$. Тогда в любом нетривиальном разложении $f = gh$ в $\mathbb{Z}[x]$ степень одного из делителей, скажем h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени $\leqslant n$, достаточно подставить в f любые $n+1$ различных чисел $z_0, z_1, \ldots, z_n \in \mathbb{Z}$ и рассмотреть все возможные наборы чисел $d_0, d_1, \ldots, d_n$, в которых d_i делит $f(z_i)$. Таких наборов имеется конечное число, и набор значений $h(z_i)$ многочлена h (буде такой многочлен существует) является одним из этих наборов $d_0, d_1, \ldots, d_n$. По упр. 3.10 в $\mathbb{Q}[x]$ есть

[1] мы уже пользовались этим в доказательстве лем. 5.2 на стр. 79

[2] откуда, по лемме Гаусса, будет следовать, что его нет и в $\mathbb{Q}[x]$

ровно один многочлен степени $\leqslant n$ принимающий значения d_i в точках z_i. Это *интерполяционный многочлен Лагранжа*

$$f_d(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)} \tag{5-11}$$

Таким образом, если h существует, то находится среди тех из многочленов (5-11), что имеют целые коэффициенты. Остаётся явно разделить f на все эти многочлены и либо убедиться, что они не делят f, либо найти среди них делитель f.

§6. Векторы

6.1. Векторные пространства. Зафиксируем произвольное поле $\Bbbk$, которое мы будем далее называть *основным*, а его элементы — *числами*. Определение векторного пространства формализует свойства алгебраических операций над геометрическими векторами — сложение векторов и умножение векторов на числа. Эти свойства присущи объектам самой разной природы: от расширений полей и пространств функций до пространств решений линейных уравнений и пространств подмножеств. Тем не менее, векторы продуктивно представлять себе именно геометрически, как направленные отрезки («стрелочки»), рассматриваемые с точностью до параллельного переноса.

Определение 6.1
Аддитивная абелева группа V называется *векторным пространством* (а её элементы — *векторами*) над полем $\Bbbk$, если на ней задана операция *умножения векторов на числа*

$$\Bbbk \times V \to V \ : \ (\lambda, v) \mapsto \lambda v \,,$$

которая обладает следующими свойствами:

$$\forall\, \lambda, \mu \in \Bbbk\,, \ \ \forall\, v \in V \qquad \lambda(\mu v) = (\lambda\mu)v \tag{6-1}$$

$$\forall\, \lambda, \mu \in \Bbbk\,, \ \ \forall\, v \in V \qquad (\lambda + \mu)v = \lambda v + \mu v \tag{6-2}$$

$$\forall\, v, w \in V\,, \ \ \forall\, \lambda \in \Bbbk \qquad \lambda(v + w) = \lambda v + \lambda w \tag{6-3}$$

$$\forall\, \lambda, \mu \in \Bbbk\,, \ \ \forall\, v \in V \qquad 1 \cdot v = v\,. \tag{6-4}$$

Групповая операция в векторном пространстве V называется *сложением векторов*. Нейтральный элемент 0 группы V называется *нулевым вектором*, а векторы v и $-v$ — *противоположными* векторами. Подмножество $U \subset V$, являющееся векторным пространством относительно имеющихся в V операций, называется *подпространством* в V.

Определение 6.2
Если в предыдущем опр. 6.1 заменить поле $\Bbbk$ а произвольное коммутативное кольцо K, то абелева группа V с умножением $K \times V \to V$, которое удовлетворяет свойствам (6-1) – (6-3), называется *модулем* над K (или K*-модулем*). Если K — кольцо с единицей, а умножение векторов на числа обладает также и последним свойством (6-4), K-модуль V называется *унитальным*. Таким образом, векторные пространства являются специальными примерами модулей.

Упражнение 6.1. Выведите из свойств (6-1) – (6-3), что в любом K-модуле V для всех $v \in V$ и $\lambda \in K$ выполняются равенства $0 \cdot v = 0$ и $\lambda \cdot 0 = 0$, и что в унитальном модуле над коммутативным кольцом с единицей результатом умножения произвольного вектора v на число $-1 \in K$ является противоположный к v вектор, т. е. $(-1) \cdot v = -v$.

Замечание 6.1. Иногда мы будем записывать произведение вектора $v \in V$ на число $\lambda \in K$ не как λv, а как $v\lambda$. Мы по определению считаем обе эти записи равнозначными.

Пример 6.1 (нулевое пространство)
Простейший пример векторного пространства — это *нулевое* (или *тривиальное*) пространство 0, состоящее из одного нулевого вектора 0, обратного самому себе и такого, что

$\forall\,\lambda\in\Bbbk\quad \lambda\cdot 0=0$. Точно так же над любым коммутативным кольцом K имеется нулевой K-модуль.

Пример 6.2 (основное поле)
Основное поле $\Bbbk$, в котором сложение векторов и умножение векторов на числа суть сложение и умножение, которые имеются в поле $\Bbbk$, также является векторным пространством над $\Bbbk$. Аналогично, любое коммутативное кольцо является модулем над собой.

Пример 6.3 (координатная плоскость)
Простейшее векторное пространство, отличное от нуля и основного поля — это *координатная плоскость* $\Bbbk^2 = \Bbbk\times\Bbbk$, векторами которой по определению являются столбцы чисел $v=\begin{pmatrix}x_1\\x_2\end{pmatrix}$, $x_1,\ x_2\in\Bbbk$. Сложение векторов и умножение векторов на числа определяются покоординатно: $\lambda\begin{pmatrix}a_1\\a_2\end{pmatrix}+\mu\begin{pmatrix}b_1\\b_2\end{pmatrix}\stackrel{\text{def}}{=}\begin{pmatrix}\lambda a_1+\mu b_1\\ \lambda a_2+\mu b_2\end{pmatrix}$.

6.1.1. Линейные отображения. Отображение $F: U\to W$ из векторного пространства U в векторное пространство W называется *линейным отображением*[1], если оно перестановочно со сложением векторов и умножением векторов на числа, т. е.

$$\forall\,a,b\in U\quad\text{и}\quad\forall\,\alpha,\beta\in\Bbbk\qquad F(\alpha a+\beta b)=\alpha F(a)+\beta F(b)\,.$$

Мы уже сталкивались с линейными отображениями $\Bbbk[x]\to\Bbbk[x]$ в n° 4.6 на стр. 59, когда изучали разностные операторы на пространстве многочленов.

Векторные пространства, между которыми имеется взаимно однозначное линейное отображение, называются *изоморфными*, а само отображение называется в этом случае *изоморфизмом* векторных пространств.

Будучи гомоморфизмом абелевых групп, всякое линейное отображение $F: V\to W$ обладает всеми свойствами, перечисленными нами в n° 2.6 на стр. 25. В частности, $F(0)=0$ и $\forall\ v\quad F(-v)=-F(v)$. Образ $\operatorname{im}F=F(V)$ — это подпространство в V, а ядро

$$\ker F=F^{-1}(0)=\{v\in V\mid F(v)=0\}$$

является подпространством в V, и слой отображения F над каждым вектором $w\in\operatorname{im}F$ представляет собой параллельный сдвиг ядра на произвольно выбранный вектор из этого слоя: если $F(v)=w$, то $F^{-1}(w)=v+\ker F$. В частности, линейное отображение инъективно тогда и только тогда, когда его ядро нулевое.

Предостережение 6.1. Обратите внимание, что отображение $\varphi:\Bbbk\to\Bbbk$, заданное формулой $\varphi(x)=a\cdot x+b$, которое в школе принято называть «линейной функцией», линейно в смысле n° 6.1.1 только при $b=0$. Если же $b\neq 0$, то

$$\varphi(\lambda x)\neq\lambda\varphi(x)\quad\text{и}\quad\varphi(x+y)\neq\varphi(x)+\varphi(y)\,,$$

и φ *не* является линейным отображением.

[1] а также *линейным оператором* или *гомоморфизмом векторных пространств*

6.1.2. Пропорциональность. Векторы a и b произвольного векторного пространства V называются *пропорциональными*[1], если $x \cdot a = y \cdot b$ для некоторых чисел $x, y \in \Bbbk$, не равных одновременно нулю. Таким образом, нулевой вектор пропорционален любому вектору, а пропорциональность ненулевых векторов a и b означает, что $a = \lambda b$ и $b = \lambda^{-1} a$ для некоторого ненулевого $\lambda \in \Bbbk$.

Пример 6.4 (определитель 2×2)
В координатном пространстве $\Bbbk^2$ из прим. 6.3 пропорциональность векторов

$$a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \qquad \text{и} \qquad b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

равносильна равенству перекрёстных произведений: $a_1 b_2 = a_2 b_1$. Величина

$$\det(a, b) \stackrel{\text{def}}{=} a_1 b_2 - a_2 b_1$$

называется *определителем* векторов a и b из $\Bbbk^2$. Очевидно, что

$$\det(a, b) = 0 \iff a \text{ и } b \text{ пропорциональны} \tag{6-5}$$

$$\det(a, b) = -\det(b, a) \qquad \forall\, a, b \in \Bbbk^2 \tag{6-6}$$

$$\det(\lambda a, b) = \lambda \det(a, b) = \det(a, \lambda b) \qquad \forall\, a, b \in \Bbbk^2 \text{ и } \forall\, \lambda \in \Bbbk \tag{6-7}$$

$$\begin{aligned} \det(a_1 + a_2, b) &= \det(a_1, b) + \det(a_2, b) \\ \det(a, b_1 + b_2) &= \det(a, b_1) + \det(a, b_2) \end{aligned} \qquad \forall\, a, a_1, a_2, b, b_1, b_2 \in \Bbbk^2 \tag{6-8}$$

Свойство (6-6) называется *кососимметричностью*, свойство (6-7) — *однородностью*, свойство (6-8) — *аддитивностью*. Вместе однородность и аддитивность означают, что определитель *линеен* по каждому из двух своих аргументов и для любых векторов $a, b, c, d \in \Bbbk^2$ и чисел $\alpha, \beta, \gamma, \delta \in \Bbbk$ имеет место *дистрибутивность*:

$$\det(\,\alpha a + \beta b\,,\ \gamma c + \delta d\,) = \alpha\gamma \det(a, c) + \alpha\delta \det(a, d) + \beta\gamma \det(b, c) + \beta\delta \det(b, d)\,. \tag{6-9}$$

Важное геометрическое следствие этих формул заключается в том, что любая пара непропорциональных векторов $a, b \in \Bbbk^2$ образует *базис* пространства $\Bbbk^2$ в том смысле, что каждый вектор $v \in \Bbbk^2$ единственным образом представляется в виде

$$v = x \cdot a + y \cdot b \quad \text{с} \quad x, y \in \Bbbk\,, \tag{6-10}$$

причём коэффициенты x, y этого разложения можно вычислять по *правилу Крамера*

$$\begin{aligned} x &= \det(v, b) / \det(a, b) \\ y &= \det(a, v) / \det(a, b)\,. \end{aligned} \tag{6-11}$$

В самом деле, т. к. $\det(a, a) = \det(b, b) = 0$, для любого разложения (6-10)

$$\begin{aligned} \det(a, v) &= \det(a, x \cdot a + y \cdot b) = x \cdot \det(a, a) + y \cdot \det(a, b) = y \cdot \det(a, b) \\ \det(v, b) &= \det(x \cdot a + y \cdot b, b) = x \cdot \det(a, b) + y \cdot \det(b, b) = x \cdot \det(a, b)\,, \end{aligned}$$

[1] а также *коллинеарными* или *линейно зависимыми*

что даёт для x и y выражения (6-11). С другой стороны, для любого $v \in \Bbbk^2$ равенство

$$v = \frac{\det(v,b)}{\det(a,b)} \cdot a + \frac{\det(a,v)}{\det(a,b)} \cdot b$$

и в самом деле выполнено: разность $v - \det(v,b) \cdot a\,/\det(a,b)$ пропорциональна b, т. к.

$$\det\left(v - \frac{\det(v,b)}{\det(a,b)} \cdot a\,,\ b \right) = \det(v,b) - \frac{\det(v,b)}{\det(a,b)} \cdot \det(a,b) = 0\,,$$

а это означает, что $v = \det(v,b) \cdot a/\det(a,b) + \lambda \cdot b$ для некоторого $\lambda \in \Bbbk$, откуда по правилу Крамера $\lambda = \det(a,v)/\det(a,b)$.

6.2. Базисы и размерность. Рассмотрим произвольное векторное пространство V над полем $\Bbbk$. Скажем, что вектор v *линейно выражается* через векторы $w_1, w_2, \ldots, w_m$, если

$$v = \lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_m w_m$$

для некоторых $\lambda_i \in \Bbbk$. Правая часть этой формулы называется *линейной комбинацией* векторов $w_i \in V$ с коэффициентами $\lambda_i \in \Bbbk$.

Семейство[1] векторов $\{w_\nu\}$ называется *порождающим* векторное пространство V, если каждый вектор $v \in V$ линейно выражается через какое-нибудь *конечное* множество векторов из этого семейства[2]. Векторное пространство, в котором имеется конечный порождающий набор векторов, называется *конечномерным*.

Порождающий векторное пространство V набор векторов $\{e_\nu\}$ называется *базисом* этого пространства пространства, если любой вектор $v \in V$ имеет *единственное* представление в виде конечной линейной комбинации базисных векторов. Коэффициенты x_i единственного линейного выражения $v = \sum x_i e_i$ вектора v через базисные векторы e_ν называются *координатами* вектора v в базисе $\{e_\nu\}$.

Ниже, в сл. 6.1, мы покажем, что любое конечномерное векторное пространство V обладает базисом, причём все базисы состоят из одно и того же числа векторов. Это число называется *размерностью* векторного пространства V и обозначается $\dim V$ или $\dim_{\Bbbk} V$, если надо подчеркнуть, о каком основном поле $\Bbbk$ идёт речь.

Пример 6.5 (координатное пространство $\Bbbk^n$)
Координатное пространство $\Bbbk^n$ является непосредственным обобщением координатной плоскости $\Bbbk^2$ из прим. 6.3. По определению, векторами пространства $\Bbbk^n$ являются упорядоченные наборы из n чисел[3]

$$(x_1, x_2, \ldots, x_n)\,, \quad x_i \in \Bbbk\,.$$

Сложение векторов и умножение векторов на числа задаётся правилами

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) \stackrel{\text{def}}{=} (x_1 + y_1,\ x_2 + y_2,\ \ldots\ ,\ x_n + y_n)$$
$$\lambda \cdot (x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)\,.$$

[1] возможно, бесконечное

[2] это конечное множество может быть разным для разных $w \in V$

[3] для экономии бумаги мы пишем их в строчку, но часто бывает удобно представлять векторы пространства $\Bbbk^n$ в виде столбцов

Векторы $e_1, e_2, \dots, e_n$ с единицей на i-том месте и нулями в остальных

$$e_i = (0, \dots, 0, 1, 0, \dots, 0), \tag{6-12}$$

образуют базис пространства $\Bbbk^n$, поскольку произвольный вектор

$$v = (x_1, x_2, \dots, x_n) \in \Bbbk^n$$

линейно выражается через них единственным способом:

$$v = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n . \tag{6-13}$$

Таким образом, $\dim \Bbbk^n = n$. Базис (6-12) называются *стандартным* базисом координатного пространства $\Bbbk^n$.

Пример 6.6 (пространство матриц)
Полезной разновидностью координатного пространства является *пространство* $m \times n$*–матриц* $\mathrm{Mat}_{m\times n}(\Bbbk)$. Его векторы — это прямоугольные таблицы из m строк и n столбцов, заполненные числами из поля $\Bbbk$:

$$\left(a_{ij}\right) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Сложение векторов и умножение векторов на числа определяется поэлементно: если матрица $A = \left(a_{ij}\right)$ имеет в i-той строке и j-том столбце элемент a_{ij}, а матрица $B = \left(b_{ij}\right)$ — элемент b_{ij}, то их линейная комбинация $\lambda A + \mu B$ с коэффициентами $\lambda, \mu \in \Bbbk$, по определению, имеет в i-той строке и j-том столбце элемент $\lambda a_{ij} + \mu b_{ij}$. Например, в пространстве $\mathrm{Mat}_{2\times 3}(\Bbbk)$ имеем равенство

$$2 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 2 & -1 & 3 \end{pmatrix} - 3 \cdot \begin{pmatrix} -1 & 1 & 0 \\ 3 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & -3 & -2 \\ 5 & -2 & -9 \end{pmatrix}.$$

Таким образом, координатное пространство $\Bbbk^n$ можно воспринимать как пространство $\mathrm{Mat}_{1\times n}(\Bbbk)$ (матрицы, состоящие из единственной строки) или как пространство $\mathrm{Mat}_{n\times 1}(\Bbbk)$ (матрицы, состоящие из единственного столбца).

Мы будем обозначать через E_{ij} матрицу, имеющую единицу в пересечении i-той строки и j-того столбца и нули во всех остальных клетках. Матрицы E_{ij} называются *стандартными базисными матрицами* (или *матричными единицами*) и образуют базис в пространстве матриц, поскольку произвольная матрица $A = \left(a_{ij}\right)$ единственным образом линейно выражается через них: $A = \sum_{ij} a_{ij} E_{ij}$. В частности, $\dim \mathrm{Mat}_{m\times n}(\Bbbk) = mn$.

Пример 6.7 (пространство функций)
Пусть X — произвольное множество. Множество $\Bbbk^X$ всех функций $f : X \to \Bbbk$ образует векторное пространство относительно поточечного сложения значений функций и умножения их на константы: $f_1 + f_2 : x \mapsto f_1(x) + f_2(x)$ и $\lambda f : x \mapsto \lambda f(x)$. Если множество X конечно и состоит из n элементов: $X = \{1, 2, \dots, n\}$, пространство функций $X \to \Bbbk$ изоморфно координатному пространству $\Bbbk^n$. В самом деле, отображение, сопоставляющее

функции f набор её значений $\big(f(1),\, f(2),\, \ldots,\, f(n)\big) \in \Bbbk^n$ линейно и биективно. Обратное отображение переводит стандартный базисный вектор $e_i \in \Bbbk^n$ в *δ-функцию* $\delta_i : X \to \Bbbk$, действующую по правилу

$$\delta_i : k \mapsto \begin{cases} 1 & \text{при } k = i \\ 0 & \text{при } 0 \neq i\,. \end{cases}$$

Замечание 6.2. Координатный модуль K^n, модуль матриц $\mathrm{Mat}_{m\times n}(K)$ и модуль функций K^X можно рассматривать над любым коммутативным кольцом K и описанные выше базисы будут их базисами над K.

Пример 6.8 (пространство подмножеств)
Если в предыдущем примере взять в качестве $\Bbbk$ двухэлементное поле $\mathbb{F}_2$ и сопоставить каждому подмножеству $Z \subset X$ его *характеристическую функцию* $\chi_Z : X \to \mathbb{F}_2$, принимающую значение 1 всюду на Z и значение 0 всюду на $X \smallsetminus Z$, мы получим взаимно однозначное соответствие между пространством функций и множеством всех подмножеств в X. Эта биекция наделяет множество подмножеств структурой векторного пространства над полем $\mathbb{F}_2$, изоморфного пространству функций $X \to \mathbb{F}_2$.

Упражнение 6.2. Укажите а пространстве подмножеств какой-нибудь базис.

Пример 6.9 (многочлены и ряды)
Многочлены с коэффициентами в поле $\Bbbk$ очевидным образом образуют векторное пространство над $\Bbbk$ относительно операций сложения многочленов и умножения их на константы. Счётный набор мономов $1,\, x,\, x^2,\, \ldots$ является базисом этого пространства, поскольку по определению каждый многочлен является конечной линейной комбинацией таких мономов и равенство двух многочленов означает равенство их коэффициентов.

Многочлены степени не выше n образуют в $\Bbbk[x]$ векторное подпространство, которое мы будем обозначать $\Bbbk[x]_{\leqslant n}$. Первые $n+1$ мономов $1,\, x,\, x^2,\, \ldots,\, x^n$ образуют в $\Bbbk[x]_{\leqslant n}$ базис.

Упражнение 6.3. Покажите, что любой набор многочленов $f_0, f_1, \ldots, f_n \in \Bbbk[x]$, в котором $\deg f_m = m$ и каждый $f_m = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ имеет ненулевой старший коэффициент a_0, является базисом векторного пространства $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n.

В пространстве формальных степенных рядов $\Bbbk[\![x]\!]$ счётный набор мономов $1,\, x,\, x^2,\, \ldots$ базисом *не является*, поскольку ряд с бесконечным числом ненулевых коэффициентов не является *конечной* линейной комбинацией мономов.

Упражнение 6.4. Покажите, что в $\Bbbk[\![x]\!]$ нет счётного базиса.

6.2.1. Линейная зависимость. Векторы $v_1, v_2, \ldots, v_m$ в произвольном векторном пространстве V называются *линейно независимыми*, если из равенства

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0 \tag{6-14}$$

вытекает, что все $\lambda_i = 0$. Наоборот, если существует конечная линейная комбинация (6-14), равная нулевому вектору и имеющая хоть один ненулевой коэффициент λ_i, то векторы $v_1, v_2, \ldots, v_m$ называются *линейно зависимыми*. Отметим, что любой набор векторов, содержащий нулевой вектор, линейно зависим.

Наличие между векторами линейной зависимости позволяет линейно выразить любой из входящих в неё с ненулевым коэффициентом векторов через остальные. Например, при $\lambda_m \neq 0$

$$v_m = -\frac{\lambda_1}{\lambda_m} v_1 - \frac{\lambda_2}{\lambda_m} v_2 - \cdots - \frac{\lambda_{m-1}}{\lambda_m} v_{m-1}\,.$$

Наоборот, всякое линейное выражение вида $v_m = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1}$ можно воспринимать как линейную зависимость

$$\mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1} - v_m = 0\,.$$

Лемма 6.1
Набор векторов $\{e_v\}$, порождающий векторное пространство V, тогда и только тогда является базисом, когда он линейно независим.

Доказательство. Если $\sum \lambda_i e_i = 0$ и не все λ_i нулевые, то любой вектор $v = \sum x_i e_i$ допускает *другое* выражение $v = \sum (x_i + \lambda_i) e_i$ через векторы e_i. Наоборот, если какой-нибудь вектор допускает два различных представления $v = \sum x_i e_i = \sum y_i e_i$, то перенося правую часть в середину, получаем линейную зависимость $\sum (x_i - y_i) v_i = 0$. □

Замечание 6.3. Понятия линейной зависимости, линейной порождаемости и базиса дословно сохраняют свой смысл для любых модулей над произвольным коммутативным кольцом K и лем. 6.1 при этом остаётся справедливой.

Упражнение 6.5. Убедитесь в последнем.

Однако над кольцом, которое не является полем, наличие линейной зависимости между векторами обычно *не позволяет* линейно выразить один из векторов через остальные, поскольку для этого требуется деление. Например, в кольце $K = \mathbb{Q}[x, y]$, рассматриваемом как модуль над собой, векторы $u = x$ и $v = y$ линейно зависимы: $yu - xv = 0$, но ни один из них не выражается через другой. По этой причине следующая ниже лемма и её многочисленные следствия будут справедливы только для векторных пространств над полем.

Лемма 6.2 (лемма о замене)
Если векторы $w_1, w_2, \ldots, w_m$ порождают V, а векторы $u_1, u_2, \ldots, u_k$ линейно независимы, то $m \geqslant k$ и векторы w_i можно перенумеровать так, что набор $u_1, u_2, \ldots, u_k, w_{k+1}, w_{k+2}, \ldots, w_m$ (получающихся заменой первых k векторов w_i векторами u_i) также будет порождать пространство V.

Доказательство. Пусть $u_1 = x_1 w_1 + x_2 w_2 + \cdots + x_m w_m$. Поскольку $u_1 \neq 0$ (иначе векторы u_i линейно зависимы), среди коэффициентов x_i есть хоть один ненулевой. Перенумеруем векторы w_i так, чтобы $x_1 \neq 0$. Тогда вектор w_1 линейно выражается через u_1 и $w_2, \ldots, w_m$:

$$w_1 = \frac{1}{x_1} u_1 - \frac{x_2}{x_1} w_2 - \cdots - \frac{x_m}{x_1} w_m\,.$$

Следовательно, векторы $u_1, w_2, w_3, \ldots, w_m$ порождают V.

Далее действуем по индукции. Пусть для очередного i в пределах $1 \leqslant i < k$ векторы $u_1, u_2, \ldots, u_i, w_{i+1}, w_{i+2}, \ldots, w_m$ порождают V. Тогда

$$u_{i+1} = y_1 u_1 + y_2 u_2 + \cdots + y_i u_i + x_{i+1} w_{i+1} + x_{i+2} w_{i+2} + \cdots + x_m w_m\,. \tag{6-15}$$

Поскольку векторы u_ν линейно независимы, вектор u_{i+1} нельзя линейно выразить только через векторы $u_1, u_2, \ldots, u_i$, и значит, в разложение (6-15) входит с ненулевым коэффициентом хотя бы один из оставшихся векторов w_j. Следовательно, $m > i$ и мы можем занумеровать оставшиеся w_j так, чтобы в $x_{i+1} \neq 0$. Теперь, как и на первом шагу, вектор w_{i+1} линейно выражается через векторы $u_1, u_2, \ldots, u_{i+1}, w_{i+2}, w_{i+3}, \ldots, w_m$, и, значит, этот набор порождает V, что воспроизводит индуктивное предположение. □

Упражнение 6.6. Покажите, что векторное пространство V тогда и только тогда бесконечномерно, когда в нём имеются линейно независимые наборы из сколь угодно большого числа векторов.

Следствие 6.1 (теорема о базисе)
В каждом векторном пространстве V любой порождающий набор векторов содержит в себе некоторый базис, а любой линейно независимый набор векторов можно дополнить до базиса. При этом все базисы равномощны.

Доказательство. Мы докажем теорему в предположении, что пространство V конечномерно. Доказательство для общего случая намечено в зам. 6.4. — оно совершенно аналогично, но привлекает некоторые факты из курса математической логики.

Пусть пространство V порождается векторами $v_1, v_2, \ldots, v_m$. По очереди выкидывая из него те векторы, которые линейно выражаются через остальные, мы в конце концов получим линейно независимый порождающий набор векторов, который по лем. 6.1 является базисом.

Поскольку число векторов в любом линейно независимом наборе не больше, чем в любом порождающем, все базисы состоят из одинакового количества векторов.

Добавляя к произвольно взятому линейно независимому набору векторов вектор, который не выражается через него линейно, мы получаем линейно независимый набор векторов. В силу леммы о замене, повторив эту процедуру не более m раз, мы придём к линейно независимому набору, порождающему всё пространство, т. е. получим базис. □

Следствие 6.2
В n-мерном векторном пространстве V всякий линейно независимый набор из n векторов, а также всякий порождающий набор из n векторов является базисом.

Доказательство. Пусть векторы $e_1, e_2, \ldots, e_n$ составляют базис V, а векторы $v_1, v_2, \ldots, v_n$ линейно независимы. По лемме о замене (лем. 6.2) порождающие векторы e_i можно заменить векторами v_i так, что набор $v_1, v_2, \ldots, v_n$ останется порождающим. Тем самым, он — базис. Пусть теперь векторы $w_1, w_2, \ldots, w_n$ порождают V. Тогда этот набор векторов содержит в себе некоторый базис. По теореме о базисе в нём должно быть ровно n векторов, т. е. этот базис совпадает со всем набором $w_1, w_2, \ldots, w_n$. □

Следствие 6.3
Всякое n-мерное векторное пространство V над полем $\mathbb{k}$ изоморфно координатному пространству $\mathbb{k}^n$. Множество изоморфизмов между V и $\mathbb{k}^n$ взаимно однозначно соответствует множеству базисов в V.

Доказательство. Если отображение $F : \Bbbk^n \xrightarrow{\sim} V$ является изоморфизмом, то образы $v_i = F(e_i)$ стандартных базисных векторов $e_i \in \Bbbk^n$ из (6-12) образуют базис пространства V. Наоборот, для любого базиса $v_1, v_2, \dots, v_n$ пространства V отображение $F : \Bbbk^n \to V$, заданное правилом $(x_1, x_2, \dots, x_n) \mapsto x_1 v_1 + x_2 v_2 + \cdots + x_n v_n$, линейно, биективно и переводит стандартный базис (6-12) пространства $\Bbbk^n$ в базис v_i пространства V. □

Пример 6.10 (конечные расширения полей)
Всякое поле $\mathbb{F}$ является векторным пространством над любым своим подполем $\Bbbk \subset \mathbb{F}$. Расширение полей $\Bbbk \subset \mathbb{F}$ называется *конечным*, если объемлющее поле $\mathbb{F}$ конечномерно как векторное пространство над $\Bbbk$. Например, любое конечное поле $\mathbb{F}$ характеристики $p = \operatorname{char} \mathbb{F}$ является конечным расширением своего простого подполя $\mathbb{F}_p \subset \mathbb{F}$. Поэтому, по сл. 6.3 $\mathbb{F} \simeq \mathbb{F}_p^n$ как векторное пространство над $\mathbb{F}_p$. В частности, $\mathbb{F}$ состоит из p^n элементов, где $n = \dim_{\mathbb{F}_p} \mathbb{F}$, что даёт простое геометрическое решение упр. 3.23.

Упражнение 6.7. Может ли поле из 9 элементов быть подполем поля из 27 элементов?

Замечание 6.4. Без предположения о том, что пространство V линейно порождается конечным набором векторов, сл. 6.1 доказывается следующим образом. Множество всех линейно независимых наборов векторов в V, частично упорядоченное отношением включения, является *полным* в том смысле, что для каждого линейно упорядоченного по включению множества линейно независимых наборов векторов существует линейно независимый набор векторов, содержащий в себе все наборы из рассматриваемого множества.

Упражнение 6.8. Убедитесь, что в качестве такого мажорирующего набора можно взять объединение всех наборов из рассматриваемого множества.

Поэтому, согласно *лемме Цорна*[1], любой линейно независимый набор векторов содержится в некотором *максимальном* линейно независимом наборе $\{e_\nu\}$ — таком, который сам уже не содержится ни в каком строго большем линейно независимом наборе. Этот максимальный линейно независимый набор $\{e_\nu\}$ является порождающим, т. к. при добавлении к нему любого вектора v будет получаться линейно зависимый набор, и в силу линейной независимости векторов e_ν линейная зависимость между векторами v и e_i будет содержать вектор v с ненулевым коэффициентом, т. е. v будет линейно выражаться через e_i. Таким образом, любой линейно независимый набор векторов содержится в некотором базисе.

Если в проделанном рассуждении ограничиться рассмотрением линейно независимых наборов векторов, содержащихся в произвольно заданном множестве векторов $\mathcal{G} \subset V$, линейно порождающем пространство V, мы получим базис пространства V, являющийся подмножеством в $\mathcal{G}$.

Доказательство того, что любые два базиса равномощны, требует трансфинитного расширения лем. 6.2.

Упражнение 6.9. Пусть множество векторов $\mathcal{G} \subset V$ порождает V, а множество векторов $\mathcal{E} \subset V$ линейно независимо. Покажите, что в $\mathcal{G}$ имеется равномощное $\mathcal{E}$ подмноже-

[1] напомним, что *лемма Цорна* утверждает, что всякое полное частично упорядоченное множество содержит хоть один максимальный элемент, см. *Ван Дер Варден*, «Алгебра» (М., «Мир», 1976, стр. 246 – 249) или *П. С. Александров*, «Введение в теорию множеств и общую топологию» (М., «Наука», 1977, стр. 80 – 83)

ство, такое что после замены векторов этого подмножества множеством векторов $\mathcal{E}$ полученный набор векторов останется порождающим.

Из этого упражнения вытекает, любая линейно независимая система векторов равномощна некоторому подмножеству любой порождающей системы. Отсюда по теореме Кантора – Бернштейна[1] мы заключаем, что любые два базиса равномощны.

6.3. Линейные отображения $F : U \to W$ между двумя векторными пространствами U и W тоже образуют векторное пространство относительно операций поточечного сложения значений и умножения их на числа: $F+G : v \mapsto F(v)+G(v)$ и $\lambda F : v \mapsto \lambda \cdot F(v)$. Пространство линейных отображений обозначается через $\mathrm{Hom}_{\Bbbk}(U, W)$, или просто $\mathrm{Hom}(U, W)$, если основное поле не существенно.

Предложение 6.1
Если V конечномерно, то для любого линейного отображения $F : V \to W$

$$\dim \ker F + \dim \operatorname{im} F = \dim V . \tag{6-16}$$

Доказательство. Выберем в подпространстве $\ker F$ базис $u_1, u_2, \dots, u_k$ и дополним его векторами $e_1, e_2, \dots, e_m$ до базиса всего пространства V. Достаточно показать, что векторы $F(e_1)$, $F(e_2)$, … , $F(e_m)$ составляют базис в $\operatorname{im} F$. Они порождают образ, т. к. для любого вектора $v = \sum y_i u_i + \sum x_j e_j$ выполняется равенство $F(v) = \sum y_i F(u_i) + \sum x_j F(e_j) = \sum x_j F(e_j)$. Они линейно независимы, поскольку равенство $0 = \sum \lambda_i F(e_i) = F(\sum \lambda_i e_i)$ означало бы, что вектор $\sum \lambda_i e_i$ лежит в $\ker F$, а значит, является линейной комбинацией векторов u_i, что возможно только когда все $\lambda_i = 0$. □

Следствие 6.4
Следующие свойства линейного отображения $F : V \to V$ из пространства V в себя эквивалентны друг другу: (1) F изоморфизм (2) $\ker F = 0$ (3) $\operatorname{im} F = V$.

Доказательство. Свойства (2) и (3) равносильны друг другу по предл. 6.1, а их одновременное выполнение равносильно (1). □

6.3.1. Матричная запись. Если пространства U и W конечномерны, то выбирая в них базисы

$$u_1, u_2, \dots, u_n \in U \quad \text{и} \quad w_1, w_2, \dots, w_m \in W \tag{6-17}$$

и выражая образы $F(u_j)$ базисных векторов пространства U через базис пространства W в виде

$$F(u_j) = \sum_{i=1}^{m} w_i \cdot f_{ij} \in W \tag{6-18}$$

[1] напомним, что *теорема Кантора – Бернштейна* утверждает, что если множество A инъективно отображается в множество B, а множество B инъективно отображается в множество A, то между множествами A и B существует биекция

мы получаем набор коэффициентов $\left(f_{ij}\right)$, который организуем в таблицу, отправив координаты вектора $F(u_j)$ в её j-тый столбец. Получающаяся таким образом матрица

$$\left(F(u_1),\, F(u_2),\, \dots\, ,\, F(u_n)\right) = \begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{pmatrix} \in \mathrm{Mat}_{m\times n} \tag{6-19}$$

называется *матрицей оператора F в базисах* (6-17) и обозначается[1] $F_{wu} = \left(f_{ij}\right)$.

Упражнение 6.10. Убедитесь, что при сложении линейных отображений и умножении линейных отображений на числа их матрицы (в зафиксированных базисах) складываются и умножаются на числа.

Предложение 6.2
При любом выборе базисов $u_1, u_2, \dots, u_n \in U$ и $w_1, w_2, \dots, w_m \in W$ отображение

$$\mathrm{Hom}_{\Bbbk}(U, W) \to \mathrm{Mat}_{m\times n}(\Bbbk), \quad F \mapsto F_{wu} \tag{6-20}$$

является линейным изоморфизмом векторных пространств. В частности,

$$\dim \mathrm{Hom}(U, W) = \dim U \cdot \dim W\,.$$

Доказательство. Если отображение $F : U \to W$ линейно, то его действие на произвольный вектор $v = \sum u_j x_j$ однозначно восстанавливается по значениям F на базисных векторах u_i пространства U:

$$F(v) = F\Big(\sum_{j=1}^{n} u_j x_j\Big) = \sum_{j=1}^{n} F(u_j)\cdot x_j = \sum_{j=1}^{n}\sum_{i=1}^{m} w_i \cdot f_{ij} x_j\,. \tag{6-21}$$

Поэтому, отображение (6-20) инъективно. С другой стороны, любая матрица $\left(f_{ij}\right)$ задаёт по формуле (6-21) отображение $F : U \to W$.

Упражнение 6.11. Проверьте, что это отображение линейно, и его матрица в базисах u и w есть матрица $\left(f_{ij}\right)$.

Таким образом, отображение (6-20) сюръективно. Его линейность вытекает из упр. 6.10 □

Пример 6.11 (качественная теория линейных уравнений)
Всякая система линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \qquad \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{6-22}$$

[1] индексы w и u в обозначении F_{wu} указывают на зависимость этой матрицы от выбранных базисов; для элемента, стоящего в пересечении i-той строки и j-того столбца матрицы F_{wu}, мы всегда будем использовать обозначение f_{ij}, в котором для экономии места не будет указаний на то, в каких именно базисах написана матрица

констатирует тот факт, что вектор $b \in \Bbbk^m$, столбец координат которого стоит в правой части системы (6-22), является образом неизвестного вектора $x = (x_1, x_2, \dots, x_n) \in \Bbbk^n$ под действием линейного оператора $A : \Bbbk^n \to \Bbbk^m$, переводящего стандартные базисные векторы координатного пространства $\Bbbk^n$ в столбцы матрицы $\left(a_{ij}\right)$, составленной коэффициентов левых частей уравнений (6-22). Таким образом, речь идёт об одном уравнении $A(x) = b$ на вектор x, качественное устройство решений которого мы уже много раз описывали: если $b \notin \operatorname{im} A$, то множество решений пусто, а если $b \in \operatorname{im} A$, множество решений является параллельным сдвигом подпространства $\ker A$ на произвольный вектор $v \in \Bbbk^n$, являющийся решением. Иначе говоря, разность любых двух решений x и x' является решением однородной системы линейных уравнений, получающейся из (6-22), если положить все $b_i = 0$. Из предл. 6.1 и сл. 6.4 вытекают

Следствие 6.5
Размерность пространства решений системы из m однородных[1] линейных уравнений от n переменных не меньше, чем $n - m$. В частности, любая система однородных линейных уравнений, в которой число переменных строго больше числа уравнений, всегда обладает ненулевым решением.

Следствие 6.6 (альтернатива Фредгольма)
Если в системе (6-22) число уравнений равно числу неизвестных, то либо она имеет единственное решение при любых значениях правых частей, либо система однородных уравнений, возникающих, когда все $b_i = 0$, обладает ненулевым решением.

6.4. Подпространства. Согласно теореме о базисе вытекает, что базис любого подпространства $U \subset V$ можно дополнить до базиса во всём пространстве, откуда, в частности, следует, что любое подпространство U в конечномерном пространстве V тоже конечномерно, и $\dim U \leqslant \dim V$.

Для подпространства U в конечномерном пространстве V разность размерностей

$$\operatorname{codim}_V U \stackrel{\text{def}}{=} \dim V - \dim U$$

называется *коразмерностью* подпространства U в V. Например, по предл. 6.1 размерность образа линейного отображения равна коразмерности его ядра.

Пример 6.12 (гиперплоскости)
Векторные подпространства коразмерноси 1 в V называются *гиперплоскостями*. Если $\xi : V \to \Bbbk$ — ненулевое линейное отображение, то оно сюръективно, и по предл. 6.1 его ядро $\ker \xi \subset V$ является гиперплоскостью в V. Например, многочлены степени не выше n, имеющие заданный корень $a \in \Bbbk$, образуют гиперплоскость в пространстве $\Bbbk[x]_{\leqslant n}$ всех многочленов степени не выше n. Эта гиперплоскость является ядром ненулевого линейного отображения $\mathrm{ev}_a : f \mapsto f(a)$, сопоставляющего многочлену его значение в точке a.

Упражнение 6.12*. Покажите, что всякая гиперплоскость $W \subset V$ представляется в виде $W = \ker \xi$ для некоторого ненулевого линейного отображения $\xi : V \to \Bbbk$, причём ξ определяется по W однозначно с точностью до умножения на ненулевую константу.

[1] т. е. с нулевыми правыми частями

6.4.1. Линейные оболочки. Пересечение любого семейства подпространств произвольного векторного пространства V является подпространством в V. Пересечение всех подпространств, содержащих заданное множество векторов $M \subset V$, называется *линейной оболочкой* множества M и обозначается

$$\operatorname{span}(M) = \bigcap_{U \supset M} U\,. \tag{6-23}$$

Это наименьшее по включению векторное подпространство в V, содержащее M. Иначе его можно описать как множество всех конечных линейных комбинаций векторов из M. В самом деле, такие линейные комбинации составляют векторное подпространство в V, которое содержатся в любом подпространстве, содержащем M.

Упражнение 6.13*. Покажите, что линейная оболочка любого множества векторов $M \subset V$ совпадает с пересечением всех содержащих M гиперплоскостей в V.

6.4.2. Сумма подпространств. Объединение подпространств, как правило, подпространством не является. Например многочлены вида ax^2 и многочлены вида bx образуют два одномерных подпространства в пространстве многочленов, но сумма $x^2 + x$ не лежит в их объединении.

Упражнение 6.14. Покажите, что объединение двух подпространств является подпространством только когда одно из подпространств содержится в другом.

Линейная оболочка объединения $\bigcup\limits_{\nu} U_\nu$ заданного набора подпространств $U_\nu \subset V$ называется *суммой* подпространств U_ν и обозначается $\sum U_\nu$. Таким образом, сумма подпространств состоит из всевозможных конечных сумм векторов, принадлежащих этим подпространствам. Например,

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1,\ u_2 \in U_2\}$$
$$U_1 + U_2 + U_3 = \{u_1 + u_2 + u_3 \mid u_1 \in U_1,\ u_2 \in U_2,\ u_3 \in U_3\} \quad \text{и т. д.}$$

Предложение 6.3
Если подпространства U_1, U_2 произвольного векторного пространства V конечномерны, то $\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

Доказательство. Выберем какой-нибудь базис $u_1, u_2, \ldots, u_k$ в $U_1 \cap U_2$ и дополним его векторами $v_1, v_2, \ldots, v_r$ и $w_1, w_2, \ldots, w_s$ до базисов в подпространствах U_1 и U_2 соответственно. Достаточно показать, что векторы $u_1, u_2, \ldots, u_k,\ v_1, v_2, \ldots, v_r,\ w_1, w_2, \ldots, w_s$ образуют базис пространства $U_1 + U_2$. Ясно, что они его порождают. Допустим, что они линейно зависимы. Поскольку каждый из наборов $u_1, \ldots, u_k, v_1, \ldots, v_r$ и $u_1, \ldots, u_k, w_1, \ldots, w_s$ в отдельности линейно независим, в линейной зависимости

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k + \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_r v_r + \eta_1 w_1 + \eta_2 w_2 + \cdots + \eta_s w_s = 0$$

присутствуют как векторы v_i, так и векторы w_j. Перенося $u_1, u_2, \ldots, u_k,\ v_1, v_2, \ldots, v_r$ в одну часть, а $w_1, w_2, \ldots, w_s$ — в другую, получаем равенство между вектором из U_1 и вектором из U_2, означающее, что этот вектор лежит в пересечении $U_1 \cap U_2$. Но тогда в его разложении по базисам пространств U_1 и U_2 нет векторов v_i и w_j — противоречие. □

Следствие 6.7
Для любых подпространств U_1, U_2 конечномерного векторного пространства V выполняется неравенство $\dim(U_1 \cap U_2) \geqslant \dim(U_1) + \dim(U_2) - \dim(V)$. В частности, $U_1 \cap U_2 \neq 0$ при $\dim(U_1) + \dim(U_2) > \dim V$.

Доказательство. Это вытекает из предл. 6.3 и неравенства $\dim(U_1 + U_2) \leqslant \dim V$. □

Следствие 6.8
Следующие три условия на подпространства $U_1, U_2 \subset V$ равносильны друг другу:

1) $\dim(U_1 + U_2) = \dim U_1 + \dim U_2$ 2) $U_1 \cap U_2 = 0$

3) любой вектор $w \in U_1 + U_2$ имеет *единственное* представление в виде $w = u_1 + u_2$ с $u_1 \in U_1$ и $u_2 \in U_2$

Доказательство. По сл. 6.7 (1) $\Longleftrightarrow$ (2). Покажем, что (2) $\Longleftrightarrow$ (3). Если $U_1 \cap U_2 \ni u \neq 0$, то нулевой вектор $0 \in U_1 + U_2$ имеет как минимум два разложения в виде $w = u_1 + u_2$ с $u_1 \in U_1$ и $u_2 \in U_2$: можно взять $u_1 = u_2 = 0$, а можно взять $u_1 = u$, $u_2 = -u$. Если же $U_1 \cap U_2 = 0$, то из равенства $u_1' + u_2' = u_1'' + u_2''$, в котором $u_1', u_1'' \in U_1$ и $u_2', u_2'' \in U_2$, следует равенство $u_1' - u_1'' = u_2'' - u_2'$, левая часть которого лежит в U_1, а правая — в U_2. Поэтому вектор $u_1' - u_1'' = u_2'' - u_2'$ лежит в $U_1 \cap U_2 = 0$ и, стало быть, равен нулю, т. е. $u_1' = u_1''$ и $u_2' = u_2''$. □

6.4.3. Трансверсальные подпространства. Подпространства $U_1, U_2 \subset V$, удовлетворяющие условиям из сл. 6.8, называются *трансверсальными*. Сумма трансверсальных подпространств называется *прямой* и обозначается $U_1 \oplus U_2$. Трансверсальные подпространстваназываются *дополнительными*, если $U_1 \oplus U_2 = V$. По сл. 6.8 для этого необходимо и достаточно, чтобы $\dim(U_1) + \dim(U_2) = \dim(V)$.

Упражнение 6.15. Пусть $\xi : V \to \Bbbk$ — линейное отображение, и $v \in V$ таков, что $\xi(v) \neq 0$. Покажите, что порождённое вектором v одномерное подпространство $\Bbbk \cdot v \subset V$ трансверсально к гиперплоскости $\ker \xi$ и $V = \Bbbk \cdot v \oplus \ker \xi$.

Более общим образом, сумма подпространств $U_1, U_2, \ldots, U_n \subset V$ называется *прямой* и обозначается $U_1 \oplus U_2 \oplus \cdots \oplus U_n$, если каждый вектор $w \in U_1 + U_2 + \cdots + U_n$ имеет единственное представление в виде $w = u_1 + u_2 + \cdots + u_n$ с $u_i \in U_i$. Иначе можно сказать, что сумма подпространств $U_1, U_2, \ldots, U_m \subset V$ прямая тогда и только тогда, когда любой набор ненулевых векторов $u_1, u_2, \ldots, u_m$, где $u_i \in U_i$, линейно независим.

Например, если векторы $\{e_i\}$ образуют базис пространства V, то V является прямой суммой одномерных подпространств, порождённых векторами e_i.

Упражнение 6.16. Покажите, что для того, чтобы сумма подпространств U_i была прямой, необходимо и достаточно, чтобы каждое из подпространств U_i было трансверсально сумме остальных подпространств.

6.4.4. Прямые суммы и прямые произведения. Для любого семейства векторных пространств V_ν, где индекс ν пробегает произвольное фиксированное множество X, прямое произведение абелевых групп[1] $\prod_{\nu \in X} V_\nu$, элементами которого являются семейства векторов (v_ν), в которых $v_\nu \in V_\nu$, имеет естественную структуру векторного пространства с

[1] см. n° 2.5 на стр. 24

покомпонентными операциями $\lambda\cdot\big(v_\nu\big)+\mu\cdot\big(w_\nu\big)=\big(\lambda v_\nu+\mu w_\nu\big)$. Оно называется *прямым произведением* пространств V_ν.

Подпространство прямого произведения, состоящее из семейств $\big(v_\nu\big)$, содержащих лишь конечное число ненулевых векторов, называется *прямой суммой* векторных пространств V_ν и обозначается $\bigoplus\limits_\nu V_\nu$.

Если набор пространств $V_1, V_2, \dots, V_n$ конечен, то прямая сумма совпадает с прямым произведением: $V_1\oplus V_2\oplus\dots\oplus V_n = V_1\times V_2\times\dots\times V_n$.

Упражнение 6.17. Пусть векторное пространство V является прямой суммой своих подпространств $U_1, U_2, \dots, U_m \subset V$ в смысле n° 6.4.3. Покажите, что V изоморфно прямой сумме пространств U_i, рассматриваемых как абстрактные векторные пространства.

Если набор подпространств бесконечен, прямое произведение строго мощнее прямой суммы и линейно ею не порождается. Например, прямая сумма счётного семейства одномерных пространств изоморфна пространству многочленов $\Bbbk[x]$, а прямое произведение счётного семейства одномерных пространств изоморфно пространству степенных рядов $\Bbbk[[x]]$ (ср. с прим. 6.9 на стр. 88).

6.5. Аффинные пространства. Множество A называется *аффинным*[1] *пространством* над заданным векторным пространством V, если каждому вектору $v\in V$ сопоставлено *преобразование сдвига* (или *параллельный перенос*) $\tau_v : A\to A$ так, что выполняются следующие три свойства:

$$1)\ \tau_0=\mathrm{Id}_A\,,\qquad 2)\ \forall\, v,w\in V\quad \tau_u\circ\tau_w=\tau_{u+w} \tag{6-24}$$

$$3)\ \forall\, p,q\in A\ \exists\ \text{единственный } v\in V : \tau_v(p)=q \tag{6-25}$$

Размерностью аффинного пространства A называется размерность $\dim V$ векторного пространства V.

Первые два условия (6-24) означают, что параллельные переносы на всевозможные векторы $v\in V$ образуют абелеву группу преобразований пространства A. Отметим, что обратным к преобразованию сдвига τ_v на вектор v является сдвиг τ_{-v} на противоположный вектор $-v$.

Третье условие (6-25) означает, что любую точку q можно получить из любой точки p *единственным* преобразованием сдвига τ_v. Задающий этот сдвиг вектор v обозначается через $\overrightarrow{pq}$. Продуктивно представлять его себе как стрелку с началом в точке $p\in A$ и концом в точке $q\in A$. Из (6-24) вытекает, что

$$\overrightarrow{pp}=0\quad\text{и}\quad\overrightarrow{pq}+\overrightarrow{qr}=\overrightarrow{pr}\quad\forall\, p,q,r\in A\,.$$

Упражнение 6.18. Убедитесь, что $\overrightarrow{pq}=-\overrightarrow{qp}$ и что $\overrightarrow{pq}=\overrightarrow{rs}\iff\overrightarrow{ps}=\overrightarrow{qr}$.

Параллельный перенос τ_v можно воспринимать как операцию «откладывания» фиксированного вектора $v\in V$ от всевозможных точек $p\in A$, и мы часто будем писать $p+v$ вместо $\tau_v(p)$.

Пример 6.13
Множество всех многочленов степени m со старшим коэффициентом 1 представляет собою аффинное пространство над векторным пространством $\Bbbk[x]_{\leqslant(m-1)}$ всех многочленов

[1] это слово является бесхитростной калькой с английского *affine* (ассоциированный)

степени не выше $m-1$.

Упражнение 6.19. Докажите это.

Отметим, что размерность этого аффинного пространства равна m.

6.5.1. Аффинизация и векторизация. Из всякого векторного пространства V можно изготовить аффинное пространство $\mathbb{A}(V)$, точками которого являются «концы» *радиус векторов* $v \in V$, отложенных от нуля. Оно называется *аффинизацией* векторного пространства V. Формально, точками пространства $\mathbb{A}(V)$, по определению, являются векторы пространства V, а параллельный перенос $\tau_w : \mathbb{A}(V) \to \mathbb{A}(V)$ переводит v в $v+w$.

Упражнение 6.20. Убедитесь, что свойства (6-24) и (6-25) выполняются.

Наоборот, если в произвольном аффинном пространстве A над V зафиксировать какую-нибудь «начальную» точку p и сопоставить каждой точке $q \in A$ вектор $\overrightarrow{pq} \in V$, мы, согласно (6-25), получим биекцию между точками из A и векторами из V. Эта биекция называется *векторизацией* аффинного пространства A с *началом* (или с *центром*) в точке $p \in A$. Набор $p,\ e_1, e_2, \dots, e_n$, где $p \in A$, а $e_1, e_2, \dots, e_n$ — какой-нибудь базис в V, называется *аффинной системой координат* (или *реперо́м*) в пространстве A. Коэффициенты разложения вектора $\overrightarrow{pq}$ по базису $e_1, e_2, \dots, e_n$ называются *аффинными координатами* точки q относительно репера $p,\ e_1, e_2, \dots, e_n$.

6.5.2. Аффинные подпространства. Пусть A является аффинным точечным пространством над векторным пространством V. Для любой точки $p \in A$ и любого векторного подпространства $U \subset V$ множество точек

$$\Pi(p, U) = p + U = \{\tau_u(p) \mid u \in U\}$$

называется *аффинным подпространством*. Векторное подпространство U называется в этом случае *направляющим подпространством* аффинного пространства $\Pi(p, U)$, а его размерность $\dim U$ называется *размерностью* аффинного пространства $\Pi(p, U)$.

Пример 6.14 (прямые и плоскости)
Аффинные подпространства $p + U$, где $\dim U = 1, 2$ называются *прямыми* и *плоскостями* соответственно. Таким образом, аффинная прямая представляет собою ГМТ вида $p + vt$, где p — некоторая точка, v — ненулевой вектор, а t пробегает $\Bbbk$. Аналогично, аффинная плоскость есть ГМТ вида $p + \lambda u + \mu w$, где p — некоторая точка, u, w — пара непропорциональных векторов, а λ, μ независимо пробегают $\Bbbk$.

Предложение 6.4
Следующие условия на аффинные подпространства $\Pi(p, U)$ и $\Pi(q, U)$ с одним и тем же направляющим подпространством $U \subset V$ равносильны друг другу:

$$\begin{array}{ccccc} 1)\ \overrightarrow{pq} \in U & & 2)\ \Pi(p,U) = \Pi(q,U) & & \\ 3)\ \Pi(p,U) \cap \Pi(q,U) \neq \varnothing & & 4)\ p \in \Pi(q,U) & & 5)\ q \in \Pi(p,U)\,. \end{array}$$

Доказательство. Покажем, что из (1) следует (2). Если $\overrightarrow{pq} \in U$, то любая точка вида $q+u$ с $u \in U$ может быть записана в виде $p+w$ с $w = \overrightarrow{pq}+u \in U$, и обратно, любая точка вида $p+w$ с $w \in U$ может быть записана в виде $p+u$ с $u = w - \overrightarrow{pq} \in U$. Тем самым, $\Pi(p, U) = \Pi(q, U)$.

Если выполнено (2), то тем более выполнены (3), (4), (5), а выполнение условий (4) или (5) автоматически означает выполнение условия (3). Таким образом, для завершения доказательства достаточно проверить, что из (3) вытекает (1).

Пусть точка $r = p + u' = q + u'' \in \Pi(p, U) \cap \Pi(q, U)$, где $u' = \overrightarrow{pr}$ и $u'' = \overrightarrow{qr}$ лежат в U. Тогда и $\overrightarrow{pq} = \overrightarrow{pr} + \overrightarrow{rq} = u' - u'' \in U$. □

Предложение 6.5
Следующие условия на $k + 1$ точек $p_0, p_1, \ldots, p_k$ любого аффинного пространства A над произвольным векторным пространством V равносильны друг другу:

1) точки $p_0, p_1, \ldots, p_k$ не содержатся ни в каком $(k-1)$-мерном аффинном подпространстве

2) векторы $\overrightarrow{p_0p}_1, \overrightarrow{p_0p}_2, \ldots, \overrightarrow{p_0p}_k$ линейно независимы

3) через $p_0, p_1, \ldots, p_k$ проходит единственное k-мерное аффинное подпространство

Доказательство. Покажем, что (1) равносильно (2). Линейная зависимость k векторов из (2) равносильна тому, что их линейная оболочка имеет размерность не больше $k - 1$, что в свою очередь означает, что в V найдётся $(k-1)$-мерное векторное подпространство U, содержащее все векторы $\overrightarrow{p_0p}_i$. По предл. 6.4 последнее означает, что $(k-1)$-мерное аффинное подпространство $p_0 + U$ содержит все точки p_i.

Покажем, что (2) равносильно (3). По предл. 6.4 прохождение аффинного пространства $p_0 + U$ через все точки p_i означает, что все векторы $\overrightarrow{p_0p}_i$ содержатся в U. А линейная независимость этих векторов означает, что они составляют базис в любом содержащем их k-мерном подпространстве $U \subset V$, а значит, любое такое подпространство представляет собою их линейную оболочку. □

Предложение 6.6
Если векторное подпространство $U \subset V$ является множеством решений системы однородных линейных уравнений $\xi(x) = 0$, где ξ пробегает некоторое подмножество $M \subset V^*$, то аффинное подпространство $\Pi(p, U) = p + U \subset \mathbb{A}(V)$ является множеством решений системы неоднородных линейных уравнений вида $\xi(x) = \xi(p)$, где ξ пробегает то же самое подмножество $M \subset V^*$. Наоборот, всякая система неоднородных линейных уравнений на переменную точку $x \in \mathbb{A}(V)$ вида $\xi(x) = c_\xi$, где ξ пробегает какое-нибудь подмножество $M \subset V^*$, а $c_\xi \in \Bbbk$ — некоторые константы, либо несовместна, либо множество её решений представляет собою аффинное подпространство вида $p + U$, где $U = \operatorname{Ann} M \subset V$, а p — любое фиксированное решение системы (т. е. такая точка p, что $\xi(p) = c_\xi$ для всех $\xi \in M$).

Доказательство. В силу линейности функций $\xi : V \to \Bbbk$ уравнения $\xi(x) = \xi(p)$ и $\xi(\overrightarrow{px}) = 0$ равносильны друг другу. □

6.6. Фактор пространства. Со всяким подпространством $U \subset V$ связано разбиение пространства V на *смежные классы* подпространства U

$$[v]_U = v \,(\mathrm{mod}\ U) = v + U = \{w \in V \mid w - v \in U\}$$

которые представляют собой классы эквивалентности по отношению $v \underset{U}{\sim} w$, означающему, что $w - v \in U$. Сложение классов и их умножение на числа определяются обычными формулами $[v] + [w] = [v + w]$ и $\lambda[v] = [\lambda v]$.

Упражнение 6.21. Проверьте, что эти определения корректны и задают на множестве классов структуру векторного пространства над полем $\Bbbk$.

Пространство смежных классов подпространства U обозначается V/U и называется *фактор пространством* пространства V по подпространству U. Отображение факторизации $V \twoheadrightarrow V/U$, переводящее каждый вектор $v \in V$ в его класс $[v]$, линейно и сюръективно.

Иначе смежный класс $[v]$ вектора $v \in V$ по подпространству $U \subset V$ можно воспринимать как проходящее через точку $v \in \mathbb{A}(V)$ параллельно подпространству $U \subset V$ аффинное подпространство в аффинизации $\mathbb{A}(V)$ пространства V: $[v] = v + U = \Pi(v, U) \subset \mathbb{A}(V)$. Таким образом, векторы фактор пространства V/U биективно соответствуют аффинным подпространствам в $\mathbb{A}(V)$ с заданным направляющим подпространством $U \subset V$.

Пример 6.15 (фактор по ядру)
Каждый линейный оператор $F : V \to W$ задаёт канонический изоморфизм

$$V/\ker F \xrightarrow{\sim} \operatorname{im} F,$$

сопоставляющий классу $[v] \in V/\ker F$ вектор $F(v) \in \operatorname{im} F$. Это переформулировка того, что

$$F(v) = F(w) \iff v - w \in \ker F.$$

Следствие 6.9
Если векторы $v_1, v_2, \ldots, v_k$ дополняют некоторый базис $u_1, u_2, \ldots, u_m$ подпространства U до базиса во всём пространстве $V \supset U$, то их классы $[v_1]$, $[v_2]$, … , $[v_k]$ образуют базис фактор пространства V/U. В частности, $\dim U + \dim V/U = \dim V$.

Доказательство. Это частный случай предл. 6.1 на стр. 92 (и её доказательства), относящийся к отображению факторизации $V \twoheadrightarrow V/U$. □

Пример 6.16 (линейная оболочка как фактор)
Линейная оболочка $W = \operatorname{span}(w_1, w_2, \ldots, w_n) \subset V$ любого набора из n векторов w_i произвольного пространства V является образом линейного оператора $F : \Bbbk^n \to V$, переводящего стандартный базисный вектор $e_i \in \Bbbk^n$ в вектор $w_i \in W$. Ядро этого оператора $U = \ker F \subset \Bbbk^n$ представляет собою *пространство линейных соотношений* между векторами w_i в W в том смысле, что вектор $u = (\lambda_1, \lambda_2, \ldots, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n \in \Bbbk^n$ лежит в U тогда и только тогда, когда $\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n = 0$ в W. Изоморфизм $W = \operatorname{im} F \simeq \Bbbk^n/U$ из предыдущего прим. 6.15 означает в этом случае, что векторы $w \in W$ суть классы вычетов линейных комбинаций $x_1 w_1 + x_2 w_2 + \cdots + x_n w_n$ по модулю тех комбинаций, которые являются линейными зависимостями между векторами w_i.

Предложение 6.7
Для любого r-мерного подпространства $U \subset \Bbbk^n$ существует такое разбиение стандартного базиса $e_1, e_2, \ldots, e_n$ координатного пространства $\Bbbk^n$ на два непересекающихся подмножества

$$\{e_1, e_2, \ldots, e_n\} = \{e_{i_1}, e_{i_2}, \ldots, e_{i_r}\} \sqcup \{e_{j_1}, e_{j_2}, \ldots, e_{j_{n-r}}\}, \tag{6-26}$$

что натянутые на них дополнительные друг другу координатные подпространства

$$E_I = \operatorname{span}(e_{i_1}, e_{i_2}, \dots, e_{i_r}) \simeq \Bbbk^r \quad \text{и} \quad E_J = \operatorname{span}(e_{j_1}, e_{j_2}, \dots, e_{j_{n-r}}) \simeq \Bbbk^{n-r},$$

удовлетворяют условиям:

1) $U \cap E_J = 0$
2) факторизация $\Bbbk^n \twoheadrightarrow \Bbbk^n/U$ изоморфно отображает E_J на $\Bbbk^n/U$
3) проекция $c_I : \Bbbk^n \twoheadrightarrow E_I$ вдоль E_J изоморфно отображает U на E_I
4) в U найдётся r векторов $u_1, u_2, \dots, u_r$ вида $u_\nu = e_{i_\nu} + w_\nu$, где $w_\nu \in E_J$.

Выполнение любого из этих условий влечёт за собою выполнение всех остальных, причём для заданных подпространства U и разбиения базиса в $\Bbbk 6n$, удовлетворяющего условиям (1) – (4), набор векторов u_i, о котором идёт речь в (4), единственен и является базисом в U.

Доказательство. Существование разбиения вытекает из леммы о замене[1]: для любого базиса $w_1, w_2, \dots, w_r$ в пространстве U в стандартном базисе пространства $\Bbbk^n$ некоторые r векторов можно заменить на векторы w_i так, что оставшиеся векторы e_{j_1}, e_{j_2}, …, $e_{j_{n-r}}$ вместе с $w_1, w_2, \dots, w_r$ составят базис в $\Bbbk^n$. Это означает, что линейная оболочка E_J векторов e_{j_1}, e_{j_2}, …, $e_{j_{n-r}}$ удовлетворяет условию (1).

Покажем, что условия (1) – (4) эквивалентны друг другу. Из (1) следует, что пространство U имеет нулевое пересечение с ядром проекции $c_I : \Bbbk^n \twoheadrightarrow E_J$, а пространство E_J — с ядром факторизации $\Bbbk^n \twoheadrightarrow \Bbbk^n/U$. Поэтому ограничение этой факторизации на подпространство E_J и ограничение проекции вдоль E_J на подпространство U инъективны. Из соображений размерности оба этих ограничения — изоморфизмы. Наоборот, каждое из условий (2), (3) влечёт трансверсальность соответствующего пространства ядру рассматриваемого отображения, т. е. условие (1). Условие (4) говорит, что $c_I(u_\nu) = e_{i_\nu}$. Если это так, то c_I изоморфизм. Наоборот, если c_I изоморфизм, то векторы $u_\nu \in U$, проектирующиеся в базисные векторы e_{i_ν} пространства E_I существуют, единственны и образуют базис в U. □

Замечание 6.5. Для заданного подпространства $U \subset \Bbbk^n$ разбиение пространства $\Bbbk^n$ в прямую сумму дополнительных координатных подпространств E_I и E_J, такое что U изоморфно проектируется на E_I вдоль E_J как правило не единственно: над бесконечным полем $\Bbbk$ случайно взятое подпространство $U \subset \Bbbk^n$ почти наверняка изоморфно проектируется *на каждое* из $\binom{n}{r}$ r-мерных координатных подпространств E_I, так что условия предл. 6.7 оказываются выполненными для любого разбиения.

6.6.1. Фактор группы абелевых групп. Конструкция фактора векторного пространства по его подпространству, как и конструкция фактор кольца по идеалу из опр. 5.2 на стр. 72 являются надстройками над конструкцией фактора абелевой группы A по её подгруппе $B \subset A$. А именно, назовём элементы $a_1, a_2 \in A$ сравнимыми по модулю подгруппы B, если $a_1 - a_2 \in B$, и будем записывать это одним из наших обычных способов:

$$[a_1]_B = [a_2]_B \quad \text{или} \quad a_1 \underset{B}{\sim} a_2 \quad \text{или} \quad a_1 \equiv a_2 \,(\mathrm{mod}\, B)\,.$$

[1] см. лем. 6.2 на стр. 89

Тогда правило $[a_1]_B + [a_2]_B \stackrel{\text{def}}{=} [a_1 + a_2]_B$ корректно задаёт на множестве классов $A\,/\,B$ структуру абелевой группы.

Упражнение 6.22. Проверьте, что $\underset{B}{\sim}$ является отношением эквивалентности и что предыдущая формула корректна, а все аксиомы абелевой группы для $A\,/\,B$ выполнены.

Факторы векторных пространств и факторы колец являются частными случаями этой конструкции. В обоих случаях оказывается, что имеющаяся на абелевой группе дополнительная структура (соответственно, умножение на скаляры и кольцевое умножение) корректно переносятся на фактор, при условии, что абелева подгруппа, по которой производится факторизация, является для дополнительной структуры «идеалом» в том смысле, что выдерживает умножение на все скаляры и, соответственно, кольцевое умножение на *все* элементы объемлющей группы.

Упражнение 6.23. Докажите, что подгруппа абелевой группы тогда и только тогда содержится в объединении конечного набора подгрупп, когда она целиком содержится в одной из них.

§7. Двойственность

7.1. Двойственное пространство. Линейное отображение $\xi : V \to \Bbbk$ из векторного пространства над полем $\Bbbk$ в само это поле[1] называется *ковектором*[2] на пространстве V. Ковекторы образуют векторное пространство, которое обозначается $V^* \stackrel{\text{def}}{=} \operatorname{Hom}_{\Bbbk}(V, \Bbbk)$ и называется *двойственным* (или *сопряжённым*) к V пространством.

Пример 7.1 (функционалы вычисления)
Пусть X — произвольное множество, и $V = \Bbbk^X$ — пространство всех функций на X со значениями в поле $\Bbbk$, как в прим. 6.7 на стр. 87. С каждой точкой $p \in X$ связан *функционал вычисления* $\mathrm{ev}_p : V \to \Bbbk$, переводящий функцию $f : X \to \Bbbk$ в её значение $f(p) \in \Bbbk$.

Упражнение 7.1. Убедитесь, что отображение ev_p линейно, и покажите, что для конечного множества X функционалы вычисления ev_p, где p пробегает X, составляют базис пространства, двойственного к пространству функций на X.

Пример 7.2 (координатные функционалы)
Каждому базису $\{e_i\}$ пространства V отвечает набор *координатных функционалов* $e_i^* \in V^*$. Функционал e_i^* сопоставляет вектору $v = \sum x_i e_i \in V$ значение i-той координаты этого вектора: $e_i^* : x_1 e_1 + x_2 e_2 + \cdots + x_n e_n \mapsto x_i$. В частности, значения функционала e_i^* на базисных векторах e_j суть

$$e_i^*(e_j) = \begin{cases} 1 & \text{при } j = i \\ 0 & \text{при } j \neq i \end{cases} \tag{7-1}$$

Упражнение 7.2. Убедитесь, что все отображения $e_i^* : V \to \Bbbk$ линейны.

Предложение 7.1
Координатные функционалы любого базиса пространства V линейно независимы в V^*. Если пространство V конечномерно, то они составляют базис пространства V^*. В частности, $\dim V = \dim V^*$.

Доказательство. Пусть в V^* имеется конечная линейная комбинация

$$\lambda_1 e_1^* + \lambda_2 e_2^* + \cdots + \lambda_N e_N^* = 0\,.$$

Вычисляя обе части на базисном векторе e_i, получаем, что $\lambda_i = 0$ для всех i. Второе утверждение вытекает из того, что каждый функционал φ на пространстве V с базисом $e_1, e_2, \ldots, e_n$ линейно выражается через функционалы e_i^* по формуле

$$\varphi = \varphi(e_1)\, e_1^* + \varphi(e_2)\, e_2^* + \cdots + \varphi(e_n)\, e_n^*\,,$$

поскольку обе части этого равенства принимают одинаковое значение $\varphi(e_i)$ на каждом базисном векторе $e_i \in V$. □

Определение 7.1
Базисы $(e_1, e_2, \ldots, e_n) \in V$ и $(e_1^*, e_2^*, \ldots, e_n^*) \in V^*$ называются *двойственными* базисами конечномерных пространств V и V^*.

[1] рассматриваемое как одномерное векторное пространство над собой
[2] а также *линейной формой* или *линейным функционалом*

7.1.1. Канонический изоморфизм $V \simeq V^{**}$. Конечномерные пространства V и V^* играют по отношению друг к другу абсолютно симметричные роли. А именно, каждый вектор $v \in V$ может рассматриваться как *функционал вычисления* на пространстве V^*, переводящий линейные формы в их значения на векторе v:

$$\mathrm{ev}_v : V^* \to \Bbbk, \quad \varphi \mapsto \varphi(v).$$

Поскольку число $\varphi(v) \in \Bbbk$ линейно зависит как от v, так и от φ, сопоставление вектору v функционала вычисления ev_v задаёт *каноническое*[1] линейное отображение

$$\mathrm{ev} : V \to V^{**}, \quad v \mapsto \mathrm{ev}_v, \tag{7-2}$$

Упражнение 7.3. Убедитесь, что отображение (7-2) переводит любой базис $e_1, e_2, \ldots, e_n$ пространства V в базис пространства V^{**}, двойственный к базису $e_1^*, e_2^*, \ldots, e_n^*$ пространства V^*.

Упражнение показывает, что отображение (7-2) является *изоморфизмом*. Это означает, что каждая линейная форма $\Phi : V^* \to \Bbbk$ на пространстве V^* является функционалом вычисления значения на некотором векторе $v \in V$, однозначно определяемым формой Φ, а любой базис $\varphi_1, \varphi_2, \ldots, \varphi_n$ пространства V^* является набором координатных форм e_i^* для единственного базиса[2] $e_1, e_2, \ldots, e_n \in V$.

Упражнение 7.4. Пусть $\dim V = n$ и наборы $v_1, v_2, \ldots, v_n \in V$ и $\varphi_1, \varphi_2, \ldots, \varphi_n \in V^*$ таковы, что $\varphi_i(v_i) = 1$ и $\varphi_i(v_j) = 0$ при $i = j$. Покажите, что

а) оба набора являются базисами

б) любой вектор v выражается через векторы v_i с коэффициентами $\varphi_i(v)$.

Пример 7.3 (формула Лагранжа)
Зафиксируем $n+1$ различных чисел $a_0, a_1, \ldots, a_n \in \Bbbk$ и рассмотрим на пространстве многочленов степени не выше n функционалы вычисления $\varphi_0, \varphi_1, \ldots, \varphi_n$, сопоставляющие многочлену f его значения $f(a_0)$, $f(a_1)$, $\ldots$, $f(a_n)$ в точках $a_0, a_1, \ldots, a_n \in \Bbbk$. Многочлен

$$f_i(x) = \prod_{\nu \neq i} (x - a_\nu)$$

имеет степень n и обращается в нуль во всех точках a_ν кроме точки a_i, где его значение отлично от нуля. Стало быть, многочлены $v_i(x) = f_i(x)/f_i(a_i)$ и формы φ_i удовлетворяют условию упр. 7.4 и являются двойственными друг другу базисами, а разложение произвольного многочлена $g(x) \in \Bbbk[x]_{\leqslant n}$ по базису $v_0, v_1, \ldots, v_n$ имеет вид

$$g(x) = \sum_{i=0}^{m} g(a_i) \cdot v_i(x) = \sum_{i=0}^{m} g(a_i) \cdot \frac{\prod\limits_{\nu \neq i} (x - a_\nu)}{\prod\limits_{\nu \neq i} (a_i - a_\nu)}. \tag{7-3}$$

Таким образом, для любого наперёд заданного набора значений $g_0, g_1, \ldots, g_n \in \Bbbk$ эта формула задаёт *единственный* многочлен $g \in \Bbbk[x]_{\leqslant n}$, принимающий значения $g(a_i) = g_i$ при всех i. Формула (7-3) называется *интерполяционной формулой Лагранжа.*

[1] т. е. не прибегающее к фиксации каких-либо дополнительных данных вроде базиса

[2] а именно, для двойственного к $\varphi_1, \varphi_2, \ldots, \varphi_n$ базиса в $V^{**} = V$

Пример 7.4 (формула Тейлора)
Пусть поле $\Bbbk$ имеет характеристику нуль[1]. Зафиксируем $a \in \Bbbk$ и рассмотрим на пространстве многочленов степени не выше n функционалы $\varphi_0, \varphi_1, \dots, \varphi_n$, сопоставляющие многочлену f его значение и значения первых n его производных в точке a:

$$f(a),\ f'(a),\ \dots\ ,\ f^{(n)}(a)\,.$$

Многочлены $v_k = (x-a)^k/k!$ и формы φ_k удовлетворяют условию упр. 7.4, а значит, являются двойственными друг другу базисами, и произвольный многочлен $g(x) \in \Bbbk[x]_{\leqslant n}$ обладает единственным разложением

$$g(x) = g(a) + g'(a)\cdot(x-a) + g''(a)\cdot\frac{(x-a)^2}{2} + \dots + g^{(n)}(a)\cdot\frac{(x-a)^n}{n!}\,, \tag{7-4}$$

которое называется *разложением Тэйлора* многочлена g в точке a.

7.1.2. Свёртка. Будем называть *свёрткой* (или *спариванием*) между векторными пространствами V и W отображение

$$V \times W \to \Bbbk\,, \quad v, w \mapsto \langle\, v\,,\, w\,\rangle\,, \tag{7-5}$$

сопоставляющее каждой паре векторов $v \in V$, $w \in W$ число $\langle\, v\,,\, w\,\rangle \in \Bbbk$, которое линейно зависит от v при фиксированном w и линейно зависит от w при фиксированном v, т. е. для любых векторов $v_1, v_2 \in V$, $w_1, w_2 \in W$ и любых чисел $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \Bbbk$ выполняется равенство

$$\begin{aligned}\big\langle\, \lambda_1 v_1 + \lambda_2 v_2\,,\, \mu_1 w_1 + \mu_2 w_2\,\big\rangle = \\ = \lambda_1\mu_1\langle\, v_1\,,\, w_1\,\rangle + \lambda_1\mu_2\langle\, v_1\,,\, w_2\,\rangle + \lambda_2\mu_1\langle\, v_2\,,\, w_1\,\rangle + \lambda_2\mu_2\langle\, v_2\,,\, w_2\,\rangle\,.\end{aligned}$$

Спаривание называется *невырожденным*, если оно удовлетворяет условиям следующей леммы:

Лемма 7.1
Следующие свойства свёртки (7-5) равносильны друг другу:

1) для каждого ненулевого $v \in V$ найдётся $w \in W$, а для каждого ненулевого $w \in W$ найдётся $v \in V$, такие что $\langle\, v\,,\, w\,\rangle \neq 0$.

2) отображение $V \to W^*$, сопоставляющее вектору v линейную форму $w \mapsto \langle\, v\,,\, w\,\rangle$ на W, является изоморфизмом

3) отображение $W \to V^*$, сопоставляющее вектору w линейную форму $v \mapsto \langle\, v\,,\, w\,\rangle$ на V, является изоморфизмом

Доказательство. В силу линейности $\langle\, v\,,\, w\,\rangle$ по v и по w, оба отображения, о которых идёт речь в (2) и (3), корректно определены и линейны. Условие (1) утверждает, что оба они инъективны. Поэтому из (1) вытекают неравенства $\dim V \leqslant \dim W^*$ и $\dim W \leqslant \dim V^*$. Так как $\dim V = \dim V^*$ и $\dim W = \dim W^*$, оба эти неравенства являются равенствами,

[1]это означает, что сумма конечного числа единиц поля $\Bbbk$ никогда не равна нулю или, эквивалентно, что наименьшее подполе в $\Bbbk$, содержащее 0 и 1, изоморфно полю $\mathbb{Q}$

а вложения (2) и (3) — изоморфизмы. Таким образом, из (1) вытекают (2) и (3). Наоборот, если выполняется одно из условий (2) или (3), то автоматически выполняется и второе[1], а значит, и условие (1). □

Пример 7.5 (свёртка векторов с ковекторами)
Свёртка между конечномерными пространствами V^* и V, задаваемая вычислением значения линейных форм на векторах $\langle\, \varphi\,,\, v\,\rangle = \varphi(v)$ невырождена. Обозначение стоящее в левой части подчёркивает симметрию между V и V^*, и мы будем им часто пользоваться в дальнейшем.

Пример 7.6 (определитель на $\Bbbk^2$)
На координатной плоскости $V = \Bbbk^2$ имеется невырожденная свёртка $V \times V \to \Bbbk$, задаваемая определителем из прим. 6.4 на стр. 85 : $\langle\, a\,,\, b\,\rangle = \det(a, b)$. В частности, любая линейная форма $\varphi : \Bbbk^2 \to \Bbbk$ имеет вид $\varphi(a) = \det(b_\varphi, a)$, где $b_\varphi \in \Bbbk^2$ — некоторый вектор, однозначно определяемый по форме φ.

7.2. **Аннуляторы**. Каждое множество ковекторов $M \subset V^*$ можно воспринимать как систему однородных линейных уравнений $\xi(x) = 0$, $\xi \in M$, на вектор $x \in V$. Множество всех решений этой системы обозначается

$$\operatorname{Ann}(M) = \{v \in V \mid \xi(v) = 0 \quad \forall\, \xi \in M\ \} \subset V\,.$$

и называется *аннулятором* множества ковекторов $M \subset V^*$. Будучи пересечением ядер линейных отображений $\xi : V \to \Bbbk$ по всем $\xi \in M$, аннулятор произвольного множества ковекторов $M \subset V^*$ всегда является векторным подпространством в V.

Двойственным образом, для любого множества векторов $N \subset V$ положим

$$\operatorname{Ann}(N) = \{\varphi \in V^* \mid \varphi(v) = 0\ \ \forall\, v \in N\ \} \subset V^*\,.$$

Алгебраически, $\operatorname{Ann}(N)$ это множество всех линейных уравнений $\xi(x) = 0$, решения которых содержат все векторы из N. Геометрически — это множество всех проходящих через N гиперплоскостей в V. Вместе с тем, как и выше, $\operatorname{Ann}(N) \subset V^*$ есть множество решений системы однородных уравнений $\operatorname{ev}_v(y) = 0$, $v \in N$, на ковектор $y \in V^*$ или, что то же самое, пересечение гиперплоскостей $\operatorname{Ann}(v) \subset V^*$ по всем $v \in N$. В частности, $\operatorname{Ann}(N)$ является векторным подпространством в V^*.

Упражнение 7.5. Убедитесь, что аннулятор любого множества совпадает с аннулятором его линейной оболочки.

Предложение 7.2
$\dim U + \dim \operatorname{Ann} U = \dim V$ для любого подпространства $U \subset V$.

Доказательство. Выберем базис $u_1, u_2, \dots, u_k \in U$ и дополним его векторами $w_1, w_2, \dots, w_m$ до базиса в V (таким образом, $\dim V = k + m$) и обозначим через

$$u_1^*, u_2^*, \dots, u_k^*,\ w_1^*, w_2^*, \dots, w_m^* \in V^*$$

[1] это переформулировка канонического отождествления $W \simeq W^{**}$: если V изоморфно W^*, то и W изоморфно $V^* = W^{**}$

двойственный базис. Тогда $w_1^*, w_2^*, \dots, w_m^* \in \operatorname{Ann} U$, поскольку для любого $v = \sum x_i u_i \in U$

$$w_\nu^*(v) = w_\nu^*\left(x_1 u_1 + x_2 u_2 + \dots + x_k u_k\right) = \sum x_i \cdot w_\nu^*(u_i) = 0\,.$$

Так как любой ковектор $\varphi = \sum y_i u_i^* + \sum z_j w_j^* \in \operatorname{Ann}(U)$ имеет $y_i = \varphi(u_i) = 0$, базисные ковекторы $w_1^*, w_2^*, \dots, w_m^*$ линейно порождают $\operatorname{Ann}(U)$, а значит, образуют там базис. Тем самым, $\dim \operatorname{Ann}(U) = m = \dim V - \dim U$. □

Следствие 7.1
$\operatorname{Ann}\operatorname{Ann}(U) = U$ для любого подпространства $U \subset V$.

Доказательство. $U \subset \operatorname{Ann}\operatorname{Ann}(U)$ и по предл. 7.2 $\dim \operatorname{Ann}\operatorname{Ann} U = \dim U$. □

Замечание 7.1. Для любого подпространства $U \subset V^*$ также выполняются равенства

$$\dim U + \dim \operatorname{Ann} U = \dim V \quad \text{и} \quad \operatorname{Ann}\operatorname{Ann}(U) = U\,.$$

Они получаются, если в предл. 7.2 и сл. 7.1 взять в них взять в качестве V двойственное пространство V^* и воспользоваться каноническим отождествлением V^{**} с V.

Замечание 7.2. На языке линейных уравнений предл. 7.2 означает, что каждое подпространство коразмерности m в V можно задать системой из m линейно независимых линейных уравнений, и наоборот, множество решений всякой системы из m линейно независимых уравнений на пространстве V представляет собою векторное подпространство коразмерности m. А сл. 7.1 утверждает, что любая линейная форма, зануляющаяся на множестве решений произвольно заданной системы линейных однородных уравнений линейно выражается через уравнения этой системы.

Упражнение 7.6. Покажите, что $\operatorname{Ann}\operatorname{Ann} N = \operatorname{span} N$ для любого подмножества $N \subset V$.

Теорема 7.1
Соответствие $U \leftrightarrow \operatorname{Ann}(U)$ задаёт биекцию между подпространствами дополнительных размерностей в двойственных пространствах V и V^*. Эта биекция оборачивает включения: $U \subset W \iff \operatorname{Ann} U \supset \operatorname{Ann} W$, и переводит суммы подпространств в пересечения, а пересечения — в суммы.

Доказательство. Обозначим через $\mathcal{S}(V)$ множество всех подпространств векторного пространства V. Равенство $\operatorname{Ann}\operatorname{Ann}(U) = U$ означает, что отображения, сопоставляющие подпространству его аннулятор в двойственном пространстве:

$$\mathcal{S}(V) \underset{\operatorname{Ann} W \leftarrow\!\shortmid W}{\overset{U \mapsto \operatorname{Ann} U}{\rightleftarrows}} \mathcal{S}(V^*)$$

обратны друг другу, и следовательно, биективны. Импликация $U \subset W \Rightarrow \operatorname{Ann} U \supset \operatorname{Ann} W$ очевидна. Если взять в ней в качестве U и W, соответственно, подпространства $\operatorname{Ann} W$ и $\operatorname{Ann} U$ и воспользоваться равенствами $\operatorname{Ann}\operatorname{Ann} W = W$ и $\operatorname{Ann}\operatorname{Ann} U = U$, получим обратную импликацию $\operatorname{Ann} U \supset \operatorname{Ann} W \Rightarrow U \subset W$. Равенство

$$\bigcap_\nu \operatorname{Ann}(U_\nu) = \operatorname{Ann}\left(\sum_\nu U_\nu\right) \tag{7-6}$$

очевидно: любая линейная форма, зануляющаяся на каждом из подпространств U_ν, зануляется и на их линейной оболочке, а форма, зануляющаяся на сумме подпространств, зануляется и на каждом из них в отдельности. Если взять в (7-6) в качестве подпространств U_ν пространства $\operatorname{Ann} U_\nu$, получаем равенство $\bigcap\limits_\nu U_\nu = \operatorname{Ann}\Big(\sum\limits_\nu \operatorname{Ann} U_\nu\Big)$. Беря в нём аннуляторы обеих частей, получаем равенство $\operatorname{Ann}\big(\bigcap\limits_\nu W_\nu\big) = \sum\limits_\nu \operatorname{Ann}(W_\nu)$. □

Следствие 7.2
Для любого подпространства $U \subset V$ имеются канонические изоморфизмы

$$(V/U)^* \simeq \operatorname{Ann}(U) \quad \text{и} \quad U^* \simeq V^*/\operatorname{Ann}(U)\,.$$

Доказательство. Если форма $\varphi \in \operatorname{Ann} U$, то для любых $u \in U$ и $v \in V$ выполняются равенства $\varphi(v+u) = \varphi(v) + \varphi(u) = \varphi(v)$. Поэтому правило $\widetilde{\varphi}([v]) = \varphi(v)$ корректно задаёт линейную форму $\widetilde{\varphi}$ на факторе V/U. Отображение

$$\operatorname{Ann}(U) \to (V/U)^*\,, \quad \varphi \mapsto \widetilde{\varphi}\,,$$

линейно и имеет нулевое ядро. Так как размерности пространств одинаковы, это изоморфизм. Для доказательства второго изоморфизма рассмотрим оператор $V^* \to U^*$, переводящий линейную форму на V в её ограничение на $U \subset V$. Поскольку ядро этого оператора это $\operatorname{Ann} U$, его образ изоморфен $V^*/\operatorname{Ann}(U) \subset U^*$. Так как размерности обоих пространств одинаковы, вложение является равенством. □

7.3. **Двойственные операторы**. С каждым линейным отображением $F : U \to W$ связано *двойственное* (или *сопряжённое*) линейное отображение $F^* : W^* \to V^*$, действующее между двойственными пространствами в противоположном к F направлении и переводящее ковектор $\xi : W \to \Bbbk$ в его композицию с F:

$$F^*(\xi) = \xi \circ F : u \mapsto \xi\big(F(u)\big)\,.$$

Упражнение 7.7. Проверьте, что $\varphi \circ F$ является линейным отображением из U в $\Bbbk$ и линейно зависит как от ξ так и от F.

Из упражнения вытекает, что сопряжение опреаторов $F \mapsto F^*$ является линейным отображением

$$\operatorname{Hom}(U,V) \to \operatorname{Hom}(W^*, U^*)\,. \tag{7-7}$$

В более симметричных обозначениях из прим. 7.5 выше действие F на векторы $u \in U$ и действие F^* на ковекторы $\xi \in W^*$ выражаются друг через друга по формуле

$$\langle\, F^*\xi\,,\, v\,\rangle = \langle\, \xi\,,\, Fv\,\rangle \quad \forall\, \xi \in W^*,\, v \in V\,, \tag{7-8}$$

которая показывает, что при отождествлении V^{**} с V оператор $F^{**} : V^{**} \to W^{**}$ отождествляется с F. Таким образом, операции сопряжения сопряжения $F \mapsto F^*$ и $F^* \mapsto F^{**} = F$ обратны друг другу, и оператор сопряжения (7-7) является изоморфизмом.

Упражнение 7.8. Докажите, что $\Big(F \circ G\Big)^* = G^* \circ F^*$.

Предложение 7.3
Имеют место равенства $\ker F^* = \operatorname{Ann}\operatorname{im} F$ и $\operatorname{im} F^* = \operatorname{Ann}\ker F$.

Доказательство. Первое равенство очевидно из формулы (7-8):

$$\xi \in \operatorname{Ann}\operatorname{im} F \iff \langle\, \xi\,,\, Fv\,\rangle = 0 \ \ \forall\, v \in V \iff \langle\, F^*\xi\,,\, v\,\rangle = 0 \ \ \forall\, v \in V \iff F^*\xi = 0\,.$$

Второе получается взятием аннуляторов от обеих частей первого равенства, написанного для оператора F^*. □

Следствие 7.3
Инъективность F равносильна сюръективности F^*. Двойственным образом, сюръективность F равносильна инъективности F^*.

7.3.1. Матрица двойственного оператора. Выберем в U и U^* двойственные базисы $\{u_j\}$ и $\{u_j^*\}$, а в W и W^* — двойственные базисы $\{w_i\}$ и $\{w_i^*\}$, и сопоставим оператору $F : U \to W$ его матрицу $F_{wu} = \left(f_{ij}\right)$ в базисах u и w. Напомним[1], что в j-том столбце матрицы F_{wu} стоят координаты f_{ij} (где $1 \leqslant i \leqslant m$) образа j-того базисного вектора u_j в базисе w, т. е. коэффициенты разложения $F(u_j) = f_{1j}w_1 + f_{2j}w_2 + \cdots + f_{mj}w_m$, или свёртки

$$f_{ij} = \left\langle\, w_i^*\,,\, Fu_j\,\right\rangle = \left\langle\, F^*w_i^*\,,\, u_j\,\right\rangle\,.$$

Эта же свёртка является одновременно j-той координатой ковектора $F^*(w_i)$ в базисе u^*, т. е. (j,i)-тым элементом f_{ji}^* матрицы $F_{u^*w^*}^* = \left(f_{ij}^*\right)$ двойственного оператора F^* в двойственных базисах. Иначе говоря, i-тая строка матрицы F_{wu} является i-тым столбцом матрицы $F_{u^*w^*}^*$, а j-тый столбец матрицы F_{wu} является i-той строкой матрицы $F_{u^*w^*}^*$.

Матрица A^t по строкам которой записаны сверху вниз прочитанные слева направо столбцы[2] матрицы A называется *транспонированной* к матрице A. На языке формул, матрица $A^t = \left(a_{ij}^t\right)$, транспонированная к матрице $A = \left(a_{ij}\right)$, имеет $a_{ij}^t = a_{ji}$.

Итак, матрицы двойственных операторов в двойственных базисах получаются друг из друга транспонированием: $F_{u^*w^*}^* = F_{wu}^t$.

Следствие 7.4 (теорема о ранге матрицы)
У любой матрицы $A \in \operatorname{Mat}_{m\times n}(\Bbbk)$ размерность линейной оболочки её строк в $\Bbbk^n$ и размерность линейной оболочки её столбцов в $\Bbbk^m$ равны друг другу. Это число называется *рангом* матрицы A и обозначается $\operatorname{rk} A$.

Доказательство. Обозначим через $F : \Bbbk^n \to \Bbbk^m$ линейный оператор, матрица которого в стандартных базисах этих двух координатных пространств равна A. Тогда размерность линейной оболочки столбцов матрицы A равна $\dim\operatorname{im} F$, а размерность линейной оболочки строк матрицы A равна $\dim\operatorname{im} F^*$, где $F^* : \Bbbk^{m*} \to \Bbbk^{n*}$ — двойственный к F оператор. По предл. 7.3 и предл. 6.1 $\dim\operatorname{im} F^* = \dim\operatorname{Ann}\ker F = n - \dim\ker F = \dim\operatorname{im} F$. □

[1] см. 6-19 на стр. 93

[2] по-другому можно сказать, что матрица A^t получается из матрицы A отражением относительно биссектрисы левого верхнего угла — прямой $i = j$

Следствие 7.5 (теорема Кронекера – Капелли)
Система (неоднородных) линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

имеет решение тогда и только тогда, когда

$$\operatorname{rk}\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \operatorname{rk}\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

Доказательство. Наличие у системы решения означает, что столбец правых частей b лежит в линейной оболочке столбцов матрицы $A = \left(a_{ij}\right)$. Это равносильно тому, что при добавлении к матрице A столбца b размерность линейной оболочки столбцов не меняется. □

Следствие 7.6
Размерность пространства решений системы однородных линейных уравнений на n переменных с матрицей коэффициентов A равна $n - \operatorname{rk} A$.

Доказательство. $\dim \ker = n - \dim \operatorname{im} A = n - \operatorname{rk} A$. □

7.4. **Метод Гаусса**. Пусть подпространство $U \subset \Bbbk^n$ задано как линейная оболочка k векторов

$$\begin{aligned} w_1 &= (w_{11},\ w_{12},\ \dots\ ,\ w_{1n}) \\ w_2 &= (w_{21},\ w_{22},\ \dots\ ,\ w_{2n}) \\ &\cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ w_k &= (w_{k1},\ w_{k2},\ \dots\ ,\ w_{kn}), \end{aligned} \tag{7-9}$$

Мы собираемся построить в U такой базис $u_1, u_2, \dots, u_r$, что матрица вида (7-9), по строкам которой записаны координаты векторов u_i, будет иметь в некоторых r столбцах с номерами $I = (i_1, i_2, \dots, i_r)$ *единичную подматрицу* размера $r \times r$

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

т. е. базис $u_1, u_2, \dots, u_r$ будет удовлетворять условию (4) из предл. 6.7 на стр. 100. Идея построения состоит в том, чтобы обнулять координаты в столбцах матрицы (7-9), последовательно заменяя подходящие пары векторов w_i, w_j их линейными комбинациями

$w'_i = aw_i + bw_j$ и $w'_j = cw_i + dw_j$ так, чтобы линейная оболочка этой пары не менялась. Таковы, например, замены следующих трёх типов:

$$\begin{array}{lll} 1) & w'_i = w_i + \lambda w_j & w'_j = w_j \quad (\text{с любым } \lambda \in \Bbbk \text{ любое}) \\ 2) & w'_i = w_j & w'_j = w_i \\ 3) & w'_i = \varrho w_i & w'_j = w_j \quad (\text{с ненулевым } \varrho \in \Bbbk) \end{array} \tag{7-10}$$

Исходные векторы линейно выражаются в них через преобразованные как

$$\begin{array}{ll} w_i = w'_i - \lambda w'_j & w_j = w'_j \\ w_i = w'_j & w_j = w'_i \\ w_i = \varrho^{-1} w'_i & w_j = w'_j\,. \end{array}$$

При заменах (7-10) матрица $\big(w_{ij}\big)$, по строкам которой стоят координаты векторов (7-9), испытывает следующие *элементарные преобразования строк*:

1. к одной из строк прибавляется другая, умноженная на любое число[1]
2. какие-нибудь две строки матрицы меняются местами
3. одна из строк умножается на ненулевое число.

Лемма 7.2 (о приведении к строгому ступенчатому виду)
Всякая матрица $A \in \mathrm{Mat}_{m\times n}(\Bbbk)$ элементарными преобразованиями строк приводится к виду, в котором самый левый ненулевой элемент каждой строки равен 1, располагается строго правее, чем в предыдущей строке, и является единственным ненулевым элементом своего столбца.

Доказательство. Удобно разбить процесс на n последовательных шагов (по количеству столбцов). Будем предполагать, что после выполнения $(k-1)$-го шага та часть матрицы, что находится слева от k-ого столбца, имеет нужный вид (при $k = 1$ это ничего не означает). Пусть в этой части имеется s ненулевых строк. По нашему предположению $0 \leqslant s \leqslant k-1$ и эти строки являются верхними. Очередной k-тый шаг вычисления состоит из следующих действий.

Выберем в k-том столбце в строках строго ниже s-той какой-нибудь ненулевой элемент a (если его нет, можно перейти к $(k+1)$-му шагу). Умножим строку, где он стоит, на a^{-1}. Потом поменяем эту строку местами с $(s+1)$-ой строкой. Это не изменит левые $(k-1)$ столбцов матрицы, а $(s+1)$-ую строку приведёт к виду

$$\underbrace{0\,0\,\ldots\,0\,0}_{k-1}\;1\;\underbrace{*\;*\;\ldots\;*\;*}_{n-k}\,.$$

Теперь для каждого $i \neq s+1$ вычтем из i-той строки $(s+1)$-ую строку, умноженную на элемент, стоящий в пересечении i-той строки и k-того столбца. Это не изменит левые $(k-1)$ столбцов матрицы и занулит все элементы k-того столбца за исключением стоящей $(s+1)$-ой строке единицы. В результате мы попадаем в исходное положение для $(k+1)$-го шага. □

[1] подчеркнём, что все остальные строки (в том числе та, что прибавлялась) остаются без изменения

7.4.1. Отыскание базисов в линейной оболочке и факторе. Поскольку линейная оболочка строк матрицы не меняется при элементарных преобразованиях, ненулевые строки $u_1, u_2, \dots, u_r$ итоговой строгой ступенчатой матрицы порождают то же самое подпространство U, что и строки $w_1, w_2, \dots, w_k$ исходной матрицы (7-9), но при этом удовлетворяют условию (4) из предл. 6.7, в котором в качестве $I = (i_1, i_2, \dots, i_r)$ следует взять номера тех столбцов, где стоят самые левые единицы строк строгой ступенчатой матрицы. По предл. 6.7 строки ступенчатой матрицы составляют базис в U, а классы базисных векторов $e_j \in \Bbbk^n$ с $j \notin I$, образуют базис в $\Bbbk^n / U$.

Пример 7.7
Найдём базис в линейной оболочке U четырёх векторов координатного пространства $\mathbb{Q}^5$, строки которых образуют матрицу:

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \tag{7-11}$$

умножим последнюю строку на -1 и поменяем местами с первой

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ 2 & -4 & -8 & 2 & -4 \end{pmatrix}$$

зануляем первый столбец под первой строкой, добавляя ко всем строкам подходящие кратности первой:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 1 & -2 \\ 0 & -4 & -4 & 4 & -2 \end{pmatrix}$$

теперь зануляем второй столбец под второй строкой, добавляя подходящие её кратности к последним двум строкам:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

делим третью строку на -2 и зануляем последний столбец вне третьей строки, добавляя к первой и четвёртой строкам подходящие кратности третьей

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{7-12}$$

Получилась строгая ступенчатая матрица. Её строки составляют базис в линейной оболочке строк исходной матрицы (7-11). Таким образом, $\dim U = 3$ и U изоморфно проектируется на трёхмерное координатное подпространство

$$E_{(1,2,5)} = \operatorname{span}(e_1, e_2, e_5)$$

вдоль дополнительного к нему двумерного координатного подпространства

$$E_{(3,4)} = \operatorname{span}(e_3,\ e_4)$$

так что строки матрицы (7-12) переходят при такой проекции в точности в стандартные базисные векторы e_1, e_2, e_3. Тем самым, подпространство U имеет нулевое пересечение с ядром этой проекции, т. е. $U \cap E_{(3,4)} = 0$. Поэтому координатное подпространство $E_{(3,4)}$ изоморфно проектируется на фактор $\mathbb{Q}^5 / U$, и классы $e_3 \pmod U$ и $e_4 \pmod U$ образуют в нём базис.

Упражнение 7.9. Покажите, что r-мерное пространство U, заданное координатами каких-нибудь $m \geqslant r$ порождающих векторов (7-9), изоморфно проектируется на координатное подпространство E_I тогда и только тогда, когда в матрице (7-9), по строкам которой написаны координаты этих векторов, в столбцах с номерами $i_1, i_2, \ldots, i_r$ находится $m \times r$ подматрица ранга r.

Пример 7.8
На двойственном языке вычисление (7-11) – (7-12) выглядит как решение системы линейных уравнений. А именно, аннулятор $\operatorname{Ann} U \subset \mathbb{Q}^{5*}$ подпространства $U \subset \mathbb{Q}^5$, порождённого строками матрицы

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \tag{7-13}$$

есть пространство решений системы однородных линейных уравнений

$$\begin{cases} 2x_1 - 4x_2 - 8x_3 + 2x_4 - 4x_5 = 0 \\ -x_1 + x_2 + 3x_3 + x_5 = 0 \\ -x_1 - x_2 + x_3 + 2x_4 - x_5 = 0 \\ -x_1 + 2x_3 + x_4 + x_5 = 0 \end{cases} \tag{7-14}$$

матрица коэффициентов которой есть матрица (7-13). Приведя её к строгому ступенчатому виду (7-12)

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

мы выбрали в пространстве уравнений U базис, состоящий из уравнений

$$\begin{cases} x_1 - 2x_3 - x_4 = 0 \\ x_2 + x_3 - x_4 = 0 \\ x_5 = 0 \end{cases}$$

которые эквивалентны исходным уравнениям (7-14), но допускают явное выражение переменных x_1, x_2, x_5 через переменные x_3 и x_4

$$\begin{cases} x_1 = 2x_3 + x_4 \\ x_2 = -x_3 + x_4 \\ x_5 = 0 \end{cases} \tag{7-15}$$

Переменные x_3 и x_4 называются в этой ситуации *свободными* (им можно придавать любые значения), а переменные x_1, x_2 и x_5 — *связанными* (они однозначно определяются из (7-15) как только заданы какие-нибудь значения свободных переменных). На геометрическом языке это означает, что двумерное пространство $\operatorname{Ann}(U) \simeq \left(\mathbb{Q}^5/U\right)^*$ изоморфно проектируется в $\mathbb{Q}^{5*}$ на координатное подпространство $E^*_{3,4} = \operatorname{span}\left(e^*_3, e^*_4\right)$ вдоль дополнительного координатного подпространства $E^*_{1,2,5} = \operatorname{span}\left(e^*_1, e^*_2, e^*_5\right)$. В частности, в пространстве $\operatorname{Ann}(U) \simeq \left(\mathbb{Q}^5/U\right)^*$ решений системы (7-14) есть базис из ковекторов вида[1] $u^\perp_1 = (*, *, 1, 0, *)$, $u^\perp_2 = (*, *, 0, 1, *)$. Отмеченные звёздочками координаты легко находятся из (7-15) и равны $(2, -1, 1, 0, 0)$ и $(1, 1, 0, 1, 0)$.

7.4.2. **Решение системы линейных уравнений**. Пространство решений произвольной системы линейных однородных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{7-16}$$

описывается аналогично. Обозначим через $U \subset \Bbbk^n$ линейную оболочку строк матрицы $A = \left(a_{ij}\right)$. Тогда пространство решений системы (7-16) представляет собой аннулятор $\operatorname{Ann}(U) \simeq \left(\Bbbk^n/U\right)^*$. Если выбрать в пространстве уравнений U базис вида

$$\begin{aligned} u_1 &= e_{i_1} + \alpha_{1j_1}e_{j_1} + \alpha_{1j_2}e_{j_2} + \cdots + \alpha_{1j_{n-r}}e_{j_{n-r}} \\ u_2 &= e_{i_2} + \alpha_{2j_1}e_{j_1} + \alpha_{2j_2}e_{j_2} + \cdots + \alpha_{2j_{n-r}}e_{j_{n-r}} \\ &\cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ u_r &= e_{i_r} + \alpha_{rj_1}e_{j_1} + \alpha_{rj_2}e_{j_2} + \cdots + \alpha_{rj_{n-r}}e_{j_{n-r}} \end{aligned} \tag{7-17}$$

удовлетворяющий условию (4) из предл. 6.7, то матрица $\left(\alpha_{ij}\right)$ соответствующей ему системы уравнений содержит единичную подматрицу размера $r \times r$ в столбцах с номерами $i_1, i_2, \ldots, i_r$.

Упражнение 7.10. Пусть $e^*_1, e^*_2, \ldots, e^*_n$ обозначают стандартный базис[2] в $\Bbbk^{n*}$. Положим

$$E^*_J = \operatorname{span}\left(e^*_{j_1}, e^*_{j_2}, \ldots, e^*_{j_{n-r}}\right) \quad \text{и} \quad E^*_I = \operatorname{span}\left(e^*_{i_1}, e^*_{i_2}, \ldots, e^*_{i_r}\right).$$

Покажите, что если подпространство $U \subset \Bbbk^n$ удовлетворяет условиям из предл. 6.7 на стр. 100, то его аннулятор $\operatorname{Ann} U \subset \Bbbk^{n*}$ обладает следующими эквивалентными друг другу свойствами: а) $\operatorname{Ann} U \cap E^*_I = 0$ б) E^*_I изоморфно отображается на $\Bbbk^{n*}/\operatorname{Ann} U$ в) проекция $c_J : \Bbbk^{n*} \twoheadrightarrow E^*_J$ вдоль E^*_I изоморфно отображает U на E^*_J г) в $\operatorname{Ann} U$ есть $(n-r)$ ковекторов вида $u^\perp_\mu = e^*_{j_\mu} + \tau_\mu$, где $\tau_\mu \in E^*_J$. При этом векторы, о которых идёт

[1] эти ковекторы являются прообразами стандартных базисных ковекторов e^*_3, e^*_4 относительно проекции $\operatorname{Ann}(U) \twoheadrightarrow E^*_{(3,4)}$ вдоль $E_{(1,2,5)}$ и образуют базис в $\left(\mathbb{Q}^5/U\right)^* \simeq \operatorname{Ann}(U)$, двойственный к обсуждавшемуся выше базису $e_3 \pmod U$, $e_4 \pmod U$ в факторе $\mathbb{Q}^5/U$

[2] двойственный к стандартному базису $e_1, e_2, \ldots, e_n$ пространства $\Bbbk^n$

речь в (г), единственны, образуют базис в $\operatorname{Ann} U$ и связаны с векторами $u_\nu = e_{i_\nu} + w_\nu \in$ $\in U$ из условия (4) в предл. 6.7 на стр. 100 формулой

$$\tau_\mu = -\left\langle e^*_{j_\mu}, w_1 \right\rangle \cdot e^*_{i_1} - \left\langle e^*_{j_\mu}, w_2 \right\rangle \cdot e^*_{i_2} - \cdots - \left\langle e^*_{j_\mu}, w_r \right\rangle \cdot e^*_{i_r}. \tag{7-18}$$

Согласно упр. 7.10 ковекторы

$$\begin{aligned} u_1^\perp &= e^*_{j_1} - \alpha_{1j_1} e^*_{i_1} - \alpha_{2j_1} e^*_{i_2} - \cdots - \alpha_{rj_1} e^*_{i_r} \\ u_2^\perp &= e^*_{j_1} - \alpha_{1j_2} e^*_{i_1} - \alpha_{2j_2} e^*_{i_2} + \cdots - \alpha_{rj_2} e^*_{i_r} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{n-r}^\perp &= e^*_{j_{n-r}} - \alpha_{1j_{n-r}} e^*_{i_1} - \alpha_{2j_{n-r}} e^*_{i_2} - \cdots - \alpha_{rj_{n-r}} e^*_{i_r} \end{aligned} \tag{7-19}$$

составляют базис пространства $\operatorname{Ann}(U) \subset \Bbbk^{n*}$ решений системы (7-16).

Упражнение 7.11. Проверьте это независимо от упр. 7.10.

Иначе можно сказать, что базисные решения $u_j^\perp$ получаются приданием одной из свободных переменных $x_{j_1}, x_{j_2}, \ldots, x_{j_{n-r}}$ значения 1, остальным свободным переменным — значения нуль, а каждой связанной переменной x_{i_ν} — того значения, которое получается из единственного содержащего x_{i_ν} уравнения.

7.4.3. Расположение подпространства относительно базиса. Покажем, что с точностью до добавления нулевых строк результат приведения к строгому ступенчатому виду матрицы координат любого набора векторов, порождающих данное подпространство $U \subset \Bbbk^n$, не зависит ни от выбора этих векторов, ни от способа приведения.

Для этого рассмотрим убывающую цепочку координатных подпространств

$$V = V^0 \supset V^1 \supset V^2 \supset \cdots \supset V^{n-1} \supset V^n = 0, \tag{7-20}$$

в которой $V^i = \operatorname{span}\left(e_{i+1}, e_{i+2}, \ldots, e_n\right)$, и обозначим через $\pi_i : V \twoheadrightarrow V/V^i$ отображение факторизации[1]. Цепочка (7-20) называется *полным флагом*. Сопоставим каждому r-мерному подпространству $U \subset V$ набор неотрицательных целых чисел $d_i = \dim \pi_i(U) = r - \dim U \cap V^i \quad (i = 0, 1, \ldots, n)$. Числа $d_0, d_1, \ldots, d_n$ образуют неубывающую последовательность, которая начинается с $d_0 = 0$, заканчивается на $d_n = r$ и прирастает не более, чем на единицу за один шаг: $d_i - d_{i-1} \leqslant 1$.

Упражнение 7.12. Докажите это.

Например, для подпространства $U \subset \mathbb{Q}^5$, порождённого строками матрицы (7-12), получаем последовательность $(d_0, d_1, \ldots, d_5) = (0, 1, 2, 2, 2, 3)$.

Набор $I = (i_1, i_2, \ldots, i_r)$ тех номеров, в которых происходят ненулевые приращения $d_{i_\nu} - d_{i_\nu - 1} = 1$, зависит только от подпространства U и флага (7-20). Мы будем называть его *комбинаторным типом* U относительно полного координатного флага (7-20). Так, подпространство $U \subset \mathbb{Q}^5$, порождённое строками матрицы (7-12) имеет комбинаторный тип $I = (1, 2, 5)$.

Упражнение 7.13. Убедитесь, что комбинаторный тип подпространства, порождённого строками строгой ступенчатой матрицы, всегда представляет собою набор номеров тех столбцов, где стоят самые левые единицы строк.

[1] ограничение π_i на координатное подпространство $E_i = \operatorname{span}(e_1, e_2, \ldots, e_i)$ задаёт изоморфизм $E_i \xrightarrow{\sim} V/V^i$, при помощи которого можно отождествить π_i с проекцией $\Bbbk^n$ на E_i вдоль V^i, т. е. с забыванием последних $(n-i)$ координат в $\Bbbk^n$

Таким образом, форма ступенчатой матрицы, однозначно определяется флагом (7-20) и подпространством U. Поскольку базис $u_{i_1}, u_{i_2}, \dots, u_{i_r} \in U$, проектирующийся в стандартные базисные векторы $e_{i_1}, e_{i_2}, \dots, e_{i_r}$ вдоль дополнительного координатного подпространства E_J тоже единственен по предл. 6.7 на стр. 100, ненулевые строки строгой ступенчатой матрицы, которая получится при применении метода Гаусса к матрице координат любой системы порождающих векторов пространства U, зависит только от самого подпространства U и зафиксированного нами с самого начала стандартного базиса в $\Bbbk^n$, в котором записываются координаты всех векторов. Мы доказали

Следствие 7.7
В каждом подпространстве $U \subset \Bbbk^n$ существует единственный базис со строгой ступенчатой матрицей координат M_U, и сопоставление подпространству U матрицы M_U устанавливает биекцию между строгими ступенчатыми матрицами с r ненулевыми строками и r-мерными подпространствами в $\Bbbk^n$. □

Упражнение 7.14. Покажите, что строгие ступенчатые матрицы комбинаторного типа $(i_1, i_2, \dots, i_r)$ образуют в $\mathrm{Mat}_{r\times n}(\Bbbk)$ аффинное подпространство размерности $r(n-r) - \sum_{\nu=1}^{r}(i_\nu - \nu + 1)$.

§8. Матрицы

8.1. Алгебры над полем. Векторное пространство A над полем $\Bbbk$ называется *алгеброй* над $\Bbbk$ (или $\Bbbk$-*алгеброй*), если на нём имеется такая операция умножения $A \times A \to A$, что при каждом $a \in \Bbbk$ операторы левого и правого умножения на a

$$\lambda_a : A \to A,\ v \mapsto av, \quad \text{и} \quad \varrho_a : A \to A,\ v \mapsto va, \tag{8-1}$$

линейны. Это включает в себя перестановочность умножения векторов на константы с умножением в алгебре: $\forall\, \lambda \in \Bbbk,\ \forall\, a, b \in A\ \ (\lambda a)b = \lambda(ab) = a(\lambda b)$ и стандартное правило раскрытия скобок: $\forall\, \lambda_1, \lambda_2, \mu_1, \mu_2 \in \Bbbk$ и $\forall\, a_1, a_2, b_1, b_2 \in A$

$$(\lambda_1 a_1 + \mu_1 b_1)(\lambda_2 a_2 + \mu_2 b_2) = \lambda_1\lambda_2 a_1 a_2 + \lambda_1\mu_2 a_1 b_2 + \mu_1\lambda_2 b_1 a_2 + \mu_1\mu_2 b_1 b_2\,.$$

Алгебра A называется *ассоциативной*, если $\forall\, a, b, c \in A\ (ab)c = a(bc)$. Алгебра A называется *коммутативной*, если $\forall\, a, b \in A\ ab = ba$. Алгебра A называется *алгеброй с единицей*, если в ней есть нейтральный элемент по отношению к умножению (или *единица*) — такое $e \in A$, что $ea = ae = a$ для всех $a \in A$.

Упражнение 8.1. Покажите, что $0 \cdot a = 0$ для всех a в любой алгебре A и что единичный элемент единственен (если существует).

Примерами *коммутативных* ассоциативных алгебр с единицами являются алгебра многочленов $\Bbbk[x_1, x_2, \ldots, x_n]$ и прочие коммутативные $\Bbbk$-алгебры в смысле n° 5.2.1 на стр. 74. Модельный пример некоммутативной ассоциативной алгебры — это линейные эндоморфизмы векторного пространства.

Пример 8.1 (алгебра $\operatorname{End} V$ линейных эндоморфизмов пространства V)
Композиция линейных отображений $G : U \to V$ и $F : V \to W$ тоже является линейным отображением, поскольку $FG(\lambda u + \mu w) = F(\lambda G(u) + \mu G(w)) = \lambda FG(u) + \mu FG(w)$. При этом отображение композиции $\operatorname{Hom}(V, W) \times \operatorname{Hom}(U, V) \to \operatorname{Hom}(U, W)$, $(F, G) \mapsto FG$, линейно по каждому из аргументов при фиксированном втором:

$$(\lambda_1 F_1 + \lambda_2 F_2)G = \lambda_1 F_1 G + \lambda_2 F_2 G \quad \text{и} \quad F(\mu_1 G_1 + \mu_2 G_2) = \mu_1 F G_1 + \mu_2 F G_2\,.$$

Таким образом, линейные эндоморфизмы $\operatorname{End} V = \operatorname{Hom}(V, V)$ любого пространства V образуют алгебру с единицей $e = \mathrm{Id}_V$.

Упражнение 8.2. Составьте таблицу умножения базисных операторов[1] $E_{ij} \in \operatorname{End}(\Bbbk^n)$ и покажите, что при $\dim V \geqslant 2$ композиция в $\operatorname{End}(\Bbbk^n)$ не коммутативна.

Поскольку композиция отображений всегда ассоциативна (когда определена):

$$F(GH) = (FG)H : u \mapsto F(G(H(u)))\,,$$

алгебра $\operatorname{End} V$ ассоциативна.

[1] напомним (см. предл. 6.2), что линейный оператор $E_{ij} : \Bbbk^n \to \Bbbk^n$ переводит e_j в e_i, а все остальные стандартные базисные векторы — в нуль

8.1.1. Обратимые элементы. Элемент a алгебры A с единицей $e \in A$ называется *обратимым*, если существует $a^{-1} \in A$, такой что $aa^{-1} = a^{-1}a = e$. В ассоциативной алгебре A это требование можно ослабить до существования левого и правого обратных к a элементов $a', a'' \in A$, таких что $a'a = aa'' = e$ — при этом они автоматически совпадут друг с другом: $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. Эта же выкладка показывает, что обратный к a элемент однозначно определяется по a.

Пример 8.2 (полная линейная группа $\mathrm{GL}\, V \subset \mathrm{End}\, V$)
Согласно предл. 1.4 обратимыми элементами алгебры $\mathrm{End}\, V$ являются линейные изоморфизмы $V \xrightarrow{\sim} V$. Они образуют группу преобразований[1] пространства V. Эта группа обозначается $\mathrm{GL}\, V$ и называется *полной линейной группой* пространства V.

8.1.2. Алгебраические и трансцендентные элементы. Любой элемент ξ любой ассоциативной $\Bbbk$-алгебры A с единицей определяет гомоморфизм вычисления

$$\mathrm{ev}_\xi : \Bbbk[t] \to A\,, \quad f(x) \mapsto f(\xi) \in A \tag{8-2}$$

который переводит многочлен $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ в результат подстановки в него[2] $x = \xi$.

Если гомоморфизм (8-2) инъективен, то элемент ξ называется *трансцендентным* над $\Bbbk$. Отметим, что в этом случае алгебра A обязательно бесконечномерна как векторное пространство над $\Bbbk$, поскольку все степени элемента ξ линейно независимы.

Если гомоморфизм (8-2) имеет ненулевое ядро, то элемент ξ называется *алгебраическим* над $\Bbbk$. В этом случае ядро $\ker \mathrm{ev}_\xi = \big(\mu_\xi\big)$ является главным идеалом[3] в $\Bbbk[x]$. Приведённый многочлен, порождающий этот идеал, называется *минимальным многочленом* элемента ξ и обозначается $\mu_\xi(x)$. Таким образом, минимальный многочлен — это многочлен наименьшей степени с единичным старшим коэффициентом, такой что $\mu_\xi(\xi) = 0$. Отметим, что все остальные многочлены, аннулирующие ξ, делятся на минимальный.

Пример 8.3 (аннулирующий многочлен линейного оператора)
Поскольку алгебра эндоморфизмов $\mathrm{End}\, V$ n-мерного векторного пространства V имеет размерность $\dim \mathrm{End}\, V = n^2$, всякий линейный оператор $F : V \to V$ алгебраичен над $\Bbbk$: n^2+1 векторов $F^k \in \mathrm{End}\, V$ с $0 \leqslant k \leqslant n^2$ линейно зависимы, и равная нулю нетривиальная линейная комбинация этих элементов представляет собой многочлен степени не выше n^2, аннулирующий оператор F. На самом деле эта степень сильно завышена: в n° 10.1.4 на стр. 148 мы покажем, что любой оператор $F : V \to V$ аннулируется многочленом степени $\dim V$ (см. также прим. 8.4 на стр. 120).

8.2. Алгебра матриц. Рассмотрим три координатных пространства $\Bbbk^n$, $\Bbbk^s$, $\Bbbk^n$ и обозначим через $u_1, u_2, \ldots, u_n \in \Bbbk^n$, $v_1, v_2, \ldots, v_s \in \Bbbk^s$, $w_1, w_2, \ldots, w_m \in \Bbbk^m$ их стандартные базисы. Пусть линейные операторы $B : \Bbbk^n \to \Bbbk^s$ и $A : \Bbbk^s \to \Bbbk^m$ имеют в этих базисах матрицы $A = \big(a_{ij}\big)$ и $B = \big(b_{ij}\big)$. Матрица $P = \big(p_{ij}\big)$ их композиции $P = AB : \Bbbk^n \to \Bbbk^m$

[1] см. n° 1.6 на стр. 14
[2] т. е. в $a_0\xi^m + a_1\xi^{m-1} + \cdots + a_{m-1}\xi + a_m\xi^0 \in A$, где $\xi^0 \stackrel{\text{def}}{=} e$ — единица алгебры A
[3] ибо $\Bbbk[x]$ — это кольцо главных идеалов

называется *произведением*[1] матриц A и B. Таким образом, для каждой упорядоченной пары матриц, в которой ширина первой матрицы совпадает с высотой второй, определена матрица-произведение, имеющая столько же строк, сколько первый сомножитель, и столько же столбцов, сколько второй. Элемент p_{ij} в пересечении i-той строки и j-того столбца произведения равен коэффициенту при w_i в разложении $AB(u_j) = A\left(\sum_k v_k b_{kj}\right) = \sum_k A(v_k) b_{kj} = \sum_i \sum_k w_i a_{ik} b_{kj}$, т. е. $p_{ij} = \sum_k a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{is}b_{sj}$. Это правило для вычисления произведения можно переговорить несколькими эквивалентными способами, каждый из которых по-своему полезен при практических вычислениях.

Во-первых, произведение матриц полностью определяется правилом умножения строки ширины s на столбец высоты s:

$$(a_1, a_2, \dots, a_s) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_s b_s ,$$

и результат умножения матрицы A из m строк ширины s на матрицу B из n столбцов высоты s представляет собою таблицу, в (i, j)-той клетке которой стоит произведение i-той строки A на j-тый столбец B:

$$p_{ij} = \begin{pmatrix} a_{i1}, & a_{i2}, & \dots, & a_{is} \end{pmatrix} \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{sj} \end{pmatrix} .$$

Упражнение 8.3. Убедитесь, что операция транспонирования матриц $A \mapsto A^t$ (см. n° 7.3.1) взаимодействует с умножением матриц по правилу $(AB)^t = B^t A^t$.

Второе описание таково: в j-том столбце произведения AB стоит линейная комбинация s столбцов матрицы A, рассматриваемых как векторы координатного пространства $\mathbb{k}^m$, с коэффициентами, стоящими в j-том столбце матрицы B. Если, к примеру, в матрице

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \tag{8-3}$$

хочется написать вместо второго столбца сумму первого и третьего, а первый и третий столбец заменить на их суммы со вторым, умноженным, соответственно, на λ и на μ, после чего добавить к полученной матрице ещё один, четвёртый столбец, равный сумме столбцов матрицы A, умноженных на их номера, то это достигается умножением A справа на матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ \lambda & 0 & \mu & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Упражнение 8.4. Проверьте это прямым вычислением по первому способу.

[1] обратите внимание, что сомножители стоят в том же порядке, что и операторы в композиции

Третье описание произведения двойственно второму и получается из во второго описания произведения транспонированных матриц $B^t A^t = (AB)^t$ заменой слова «столбец» на слово «строка». А именно, в i-той строке матрицы AB стоит линейная комбинация s строк матрицы B, рассматриваемых как векторы координатного пространства $\mathbb{k}^n$, с коэффициентами, стоящими в i-той строке матрицы A. Например, если в той же матрице (8-3) хочется поставить вторую строку на место первой, а вместо второй написать её сумму с первой строкой, умноженной на λ, то это достигается умножением слева на матрицу

$$\begin{pmatrix} 0 & 1 \\ \lambda & 1 \end{pmatrix}$$

Упражнение 8.5. Проверьте это прямым вычислением по первому способу.

Поскольку композиция операторов ассоциативна и линейна по каждому сомножителю, произведение матриц также ассоциативно и линейно по каждому сомножителю, т. е.

$$(FG)H = H(FG) \quad \forall\, F \in \mathrm{Mat}_{m\times k}\,,\ G \in \mathrm{Mat}_{k\times \ell}\,,\ H \in \mathrm{Mat}_{\ell\times n}$$
$$(\lambda_1 F_1 + \mu_1 G_1)(\lambda_2 F_2 + \mu_2 G_2) = \lambda_1\lambda_2 F_1F_2 + \lambda_1\mu_2 F_1G_2 + \mu_1\lambda_2 G_1F_2 + \mu_1\mu_2 G_1G_2$$

Таким образом, пространство $\mathrm{Mat}_n(\mathbb{k}) \stackrel{\text{def}}{=} \mathrm{Mat}_{n\times n}(\mathbb{k}) \simeq \mathrm{End}(\mathbb{k}^n)$ квадратных матриц размера $n \times n$ является ассоциативной $\mathbb{k}$-алгеброй с единицей

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

(по диагонали стоят единицы, в остальных местах — нули). При $n \geqslant 2$ алгебра $\mathrm{Mat}_n(\mathbb{k})$ некоммутативна. Например:

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 12 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}$$

Пример 8.4 (аннулирующий многочлен 2×2-матрицы)
Поскольку $\dim \mathrm{Mat}_n(\mathbb{k}) = n^2 < \infty$, все матрицы алгебраичны над $\mathbb{k}$. Покажем, что каждая 2×2-матрица $F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ удовлетворяет квадратному уравнению. В самом деле,

$$F^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix} = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix}.$$

Поэтому

$$F^2 - (a + d) \cdot F = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix} - \begin{pmatrix} a(a + d) & b(a + d) \\ c(a + d) & d(a + d) \end{pmatrix} =$$
$$= \begin{pmatrix} (bc - ad) & 0 \\ 0 & (bc - ad) \end{pmatrix} = (bc - ad) \cdot E$$

и F удовлетворяет квадратному уравнению $F^2 - (a+b)F + (ad-bc)E = 0$. Числа

$$\det F \stackrel{\text{def}}{=} ad - bc \quad \text{и} \quad \operatorname{tr} F \stackrel{\text{def}}{=} a + b$$

называются, соответственно, *определителем* и *следом* матрицы F. В этих обозначениях квадратное уравнение на матрицу F имеет вид

$$F^2 - \operatorname{tr}(F) \cdot F + \det(F) \cdot E = 0\,. \tag{8-4}$$

8.3. Обратимые матрицы. Обратимые элементы алгебры $\mathrm{Mat}_n(\Bbbk)$ называются *обратимыми матрицами*. Это в точности матрицы линейных изоморфизмов координатного пространства $\Bbbk^n$, записанные в стандартном базисе. Группа обратимых матриц обозначается $\mathrm{GL}_n(\Bbbk) \subset \mathrm{Mat}_n(\Bbbk)$.

Пример 8.5 (обратимые 2×2-матрицы)
Формулу (8-4) можно переписать в виде $\det(F) \cdot E = \operatorname{tr}(F) \cdot F - F^2 = F \cdot \big(\operatorname{tr}(F)\,E - F\big)$. Если матрица $F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ обратима, то, умножая обе части слева на F^{-1}, получаем

$$\det(F) \cdot F^{-1} = \operatorname{tr}(F) \cdot E - F = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{8-5}$$

При $\det F = 0$ в левой части стоит нулевая матрица, откуда $a = b = c = d = 0$, и т. к. нулевая матрица не обратима, мы заключаем, что матрицы F с $\det F = 0$ необратимы. Наоборот, при $\det F \neq 0$ формула (8-5) явно вычисляет F^{-1}:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad-bc)^{-1} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \tag{8-6}$$

Упражнение 8.6. Проверьте прямым вычислением, что эта матрица обратна к F.

8.3.1. Обращение матриц методом Гаусса. Выяснить, обратима ли данная матрица $A \in \mathrm{Mat}_n(\Bbbk)$, и если да, то явно вычислить A^{-1}, можно умножая матрицу A слева на *заведомо обратимые* матрицы с таким расчётом, чтобы в результате линейных преобразований строк, которые матрица A при этом будет испытывать, в конце концов получилась либо единичная матрица, либо матрица с нулевой строкой.

Упражнение 8.7. Покажите, что матрица с линейно зависимыми строками или столбцами (в частности, матрица, содержащая нулевую строку или нулевой столбец) необратима.

Если после k последовательных умножений слева на обратимые матрицы $S_1, S_2, \dots, S_k$ получится заведомо необратимая матрица $N = S_k S_{k-1} \cdots S_2 S_1 A$, то матрица A тоже не обратима, ибо существование A^{-1} влечёт существование $N^{-1} = A^{-1} S_1^{-1} S_2^{-1} \dots S_k^{-1}$. Если же получится единичная матрица $S_k S_{k-1} \cdots S_2 S_1 A = E$, то умножая это равенство слева на $S_1^{-1} S_2^{-1} \dots S_k^{-1}$, мы приходим к соотношению $A = S_1^{-1} S_2^{-1} \dots S_k^{-1}$, из которого вытекает, что A обратима, и обратная к A матрица $A^{-1} = S_k S_{k-1} \cdots S_2 S_1 E$ получается применением к единичной матрице E ровно той же цепочки преобразований, которая позволила получить из матрицы A матрицу E.

Вычисление удобно организовать следующим образом. Припишем к матрице A справа единичную матрицу, чтобы получилась матрица $\boxed{A\,|\,E}$ размера $n \times 2n$. Если в результате обратимых линейных преобразований строк этой большой матрицы мы придём к матрице вида $\boxed{E\,|\,B}$, то $A^{-1} = B$. Если же мы придём к матрице вида $\boxed{N\,|\,C}$, в которой N необратима, то матрица A тоже необратима. Коль скоро мы знаем все обратимые 2×2-матрицы, проще всего на каждом шагу изменять только какие-нибудь две строки матрицы $M = \boxed{A\,|\,E}$, а все остальные строки оставлять без изменения. Умножение пары строк ϱ_1 и ϱ_2 слева на обратимую матрицу $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ приведёт к замене этих строк[1] на их линейные комбинации

$$\begin{pmatrix} \varrho_1 \\ \varrho_2 \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \varrho_1 \\ \varrho_2 \end{pmatrix} = \begin{pmatrix} a\varrho_1 + b\varrho_2 \\ c\varrho_1 + d\varrho_2 \end{pmatrix} .$$

Подчеркнём, что $ad - bc$ должно быть отлично от нуля, т. е. коэффициенты используемых двух линейных комбинаций не должны быть пропорциональны. Классический метод Гаусса из n° 7.4 на стр. 110 ограничивался тремя специальными типами таких преобразований, отвечающих умножению на обратимые 2×2 матрицы S вида:

1) $S = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$ или $S = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}$

2) $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ с $S^{-1} = S$

3) $S = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \mu^{-1} \end{pmatrix}$, где $\lambda, \mu \in \Bbbk$ отличны от нуля.

Следствие 8.1
Приведение матрицы $\boxed{A\,|\,E}$ к строгому ступенчатому виду методом Гаусса позволяет за конечное число шагов либо найти A^{-1}, либо убедиться, что A необратима. □

Пример 8.6
Выясним обратима ли матрица

$$A = \begin{pmatrix} 6 & 3 & -2 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 3 & -1 \\ -1 & 0 & -2 & 1 \end{pmatrix}$$

Для этого припишем к ней справа единичную матрицу и применим метод Гаусса

$$\left(\begin{array}{cccc|cccc} 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & -2 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

[1] соответственно, чтобы проделать такое преобразование с i-той и j-той строками $n \times 2n$-матрицы $\boxed{A\,|\,E}$, мы должны умножить эту матрицу слева на $n \times n$-матрицу S', содержащую 2×2-подматрицу S в пересечениях i-той и j-той строк с i-тым и j-тым столбцами и имеющую $s'_{kk} = 1$ при $k \neq i, j$ и нули в остальных местах

меняем знак нижней строки, потом меняем её местами с верхней

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \end{array}\right)$$

зануляем первый столбец под первой строкой, отнимая из всех строк надлежащие кратности первой строки

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 4 & -1 & 2 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 3 & -14 & 7 & 1 & 0 & 0 & 6 \end{array}\right)$$

меняем вторую и третью строки местами и зануляем нижние два элемента второго столбца

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & -5 & 2 & 0 & 1 & -4 & -3 \\ 0 & 0 & -17 & 7 & 1 & 0 & -3 & 3 \end{array}\right) \tag{8-7}$$

Теперь, чтобы избежать вычислений с дробями, отклонимся от классического метода Гаусса и умножим нижние две строки на матрицу[1]

$$\begin{pmatrix} -5 & 2 \\ -17 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & -2 \\ 17 & -5 \end{pmatrix}$$

Получим

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array}\right)$$

Остаётся вычесть из 2-й строки 3-ю, а из 1-й — 4-ю и удвоенную 3-ю

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & -3 & 9 & 11 \\ 0 & 1 & 0 & 0 & -2 & 7 & -21 & -26 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array}\right)$$

Итак, A обратима и

$$A^{-1} = \begin{pmatrix} 1 & -3 & 9 & 11 \\ -2 & 7 & -21 & -26 \\ 2 & -7 & 22 & 27 \\ 5 & -17 & 53 & 66 \end{pmatrix}$$

[1] что соответствует умножению всей матрицы слева на $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 17 & -5 \end{pmatrix}$

Пример 8.7 (решение системы линейных уравнений)
Система из n (неоднородных) линейных уравнений с n неизвестными

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

в матричных обозначениях сворачивается до одного линейного уравнения $Ax = b$, где $A = \left(a_{ij}\right)$ есть матрицы коэффициентов, а x и b суть матрицы-столбцы размеров $n \times 1$, представляющие собою столбец переменных и столбец правых частей. Если матрица A обратима, то решение задаётся формулой $x = A^{-1}b$, причём вместо поиска $A^{-1} = S_k S_{k-1} \cdots S_2 S_1$ методом Гаусса, можно искать решение конкретной системы: поскольку $A^{-1}b = S_k S_{k-1} \cdots S_2 S_1 b$ получается применением к столбцу b той же цепочки преобразований, что приводит от A к E, преобразовав по Гауссу $n \times (n+1)$-матрицу $\boxed{A\,|\,b}$ к виду $\boxed{E\,|\,s}$, мы получаем в правом столбце решение s. Однако, если требуется искать решения многих уравнений с одной и той же матрицей A и меняющимися правыми частями, то может оказаться выгоднее всё-таки вычислить A^{-1}, а потом находить решения умножая правые части на A^{-1}.

8.4. Матрицы перехода. Пусть некий вектор v линейно выражается через какие-то ещё векторы w_i

$$v = \sum_{i=1}^{m} x_i w_i = w_1 x_1 + w_2 x_2 + \cdots + w_m x_m\,. \tag{8-8}$$

Организуем коэффициенты $x_i \in \Bbbk$ в матрицу-столбец размера $m \times 1$

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \tag{8-9}$$

а векторы w_i — в матрицу-строку $w = (w_1, w_2, \ldots, w_m)$ размера $1 \times n$ с элементами $w_i \in V$. Тогда формула (8-8) свернётся в матричное равенство $v = wx$, в котором v рассматривается как матрица размера 1×1 с элементом из V. Такая матричная запись позволяет упростить многие вычисления, связанные с линейным выражением одних векторов через другие.

Пусть, например, даны два набора векторов $u = (u_1, u_2, \ldots, u_n)$, $w = (w_1, w_2, \ldots, w_m)$ и пусть каждый из векторов u_j линейно выражен через векторы w_i

$$u_j = \sum_{\nu=1}^{m} c_{\nu j} w_\nu = w_1 \cdot c_{1j} + w_2 \cdot c_{2j} + \cdots + w_m \cdot c_{mj}\,.$$

Эти n равенств сокращённо записывается одной матричной формулой $u = w \cdot C_{wu}$, в

которой $u = (u_1, u_2, \dots, u_n)$, $w = (w_1, w_2, \dots, w_m)$, а матрица

$$C_{wu} = (c_{ij}) = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{pmatrix} \tag{8-10}$$

получается подстановкой в матрицу u вместо каждого из векторов u_j столбца коэффициентов его линейного выражения через векторы w_i.

Матрица (8-10) называется *матрицей перехода* от векторов u к векторам w. Отметим, что столбец (8-9) коэффициентов линейного выражения вектора v через векторы u_j является частным случаем матрицы перехода: $x = C_{uv}$. Название «матрица перехода» вызвано тем, что C_{uw} позволяет переходить от линейных выражений векторов $v \in V$ через векторы u_j к их линейным выражениям через векторы w_i: $v = uC_{uv} \Rightarrow v = wC_{wu}C_{uv}$, т. е. произведение матрицы перехода от векторов u к векторам w и матрицы перехода от векторов v к векторам u является матрицей перехода от векторов v к векторам w:

$$C_{wu}C_{uv} = C_{wv}\,. \tag{8-11}$$

Замечание 8.1. Если набор векторов $w = (w_1, w_2, \dots, w_m)$ линейно зависим, то каждый вектор v из их линейной оболочки допускает много *различных* линейных выражений[1] через векторы w_j. Поэтому обозначение C_{wv} не корректно в том смысле, что элементы матрицы C_{wv} определяются по векторам w и v не однозначно. Тем не менее, равенство (8-11) содержательно и означает, что имея какие-нибудь линейные выражения C_{wu} и C_{uv} векторов u через v и векторов v через w, мы можем предъявить явное линейное выражение C_{wv} векторов u через w *перемножив матрицы* C_{wu} и C_{uv}.

Если набор векторов $e = (e_1, e_2, \dots, e_n)$ является базисом, то матрица перехода C_{ew}, выражающая произвольный набор векторов $w = (w_1, w_2, \dots, w_m)$ через базис e, однозначно определяется по e и w, и два набора векторов u и w совпадают тогда и только тогда, когда совпадают матрицы перехода $C_{eu} = C_{ew}$ от них к базису e.

Лемма 8.1
Пусть набор векторов $v = (v_1, v_2, \dots, v_n)$ образует базис пространства V. Для того, чтобы набор векторов $u = vC_{vu}$ тоже составлял базис, необходимо и достаточно, чтобы матрица C_{vu} была обратима, и в этом случае $C_{vu}^{-1} = C_{uv}$.

Доказательство. Если u базис, то векторы e линейно выражается через u и по (8-11) выполнены равенства $C_{ee} = C_{eu}C_{ue}$ и $C_{uu} = C_{ue}C_{eu}$. Так как каждый набор векторов (в том числе, и базис) имеет единственное выражение через базис, $C_{ee} = C_{uu} = E$, откуда $C_{ue}C_{eu} = C_{ue}C_{eu} = E$. Наоборот, если u не базис, то это линейно зависимая система векторов, и $u\lambda = 0$ для некоторого *ненулевого* столбца коэффициентов λ. Тогда $eC_{eu}\lambda = 0$, откуда $C_{eu}\lambda = 0$. Такое равенство невозможно с обратимым C_{eu} и ненулевым λ, поскольку умножение обеих частей слева на C_{eu}^{-1} даёт $\lambda = 0$. □

[1] как мы видели в n° 7.4 эти выражения представляют собою смежный класс подпространства линейных зависимостей $U \subset \mathbb{k}^m$ между векторами w_j

Пример 8.8 (замена координат при смене базиса)
Пусть набор векторов $w = (w_1, w_2, \dots, w_m)$ выражается через базис $e = (e_1, e_2, \dots, e_n)$ как $w = eC_{ew}$. Если $v = eC_{ev}$ — другой базис, то в выражении $w = vC_{vw}$ векторов w через базис v матрица $C_{vw} = C_{ve}C_{ew} = C_{ev}^{-1}C_{vw}$. В частности столбец координат произвольного вектора w в базисе v получаются из столбца его координат в базисе e умножением слева на матрицу C_{ev}^{-1}, обратную к матрице координат векторов базиса v в базисе e.

Пример 8.9 (замена матрицы оператора при смене базиса)
Для произвольных линейного оператора $F : U \to W$ и строки векторов $v = (v_1, v_2, \dots, v_r)$ будем обозначать через $F(v)$ строку значений оператора F на этих векторах

$$F(v) \stackrel{\text{def}}{=} \big(F(v_1),\, F(v_2),\, \dots\,,\, F(v_r)\big)\,.$$

В силу линейности оператора F для любой числовой матрицы $M \in \mathrm{Mat}_{r\times s}(\Bbbk)$ выполняется равенство $F(vM) = F(v)M$.

Упражнение 8.8. Убедитесь в этом.

В таких обозначениях матрица F_{wu} оператора F, записанная в базисах u и w пространств U и W, однозначно определяется равенством[1] $F(u) = wF_{wu}$. При переходе к другим базисам $\widetilde{u} = uC_{u\widetilde{u}}$ и $\widetilde{w} = wC_{w\widetilde{w}}$ она меняется по правилу

$$F_{\widetilde{w}\widetilde{u}} = C_{w\widetilde{w}}^{-1} F_{wu} C_{u\widetilde{u}}\,. \tag{8-12}$$

ибо $F(\widetilde{u}) = F(uC_{u\widetilde{u}}) = F(u)\,C_{u\widetilde{u}} = w\,F_{wu}C_{u\widetilde{u}} = \widetilde{w}\,C_{\widetilde{w}w}F_{wu}C_{u\widetilde{u}} = \widetilde{w}\,C_{\widetilde{w}w}^{-1}F_{wu}C_{u\widetilde{u}}$.

В частности, если линейный эндоморфизм $F : V \to V$ задаётся матрицей $F_e = F_{ee}$, j-тый столбец которой есть столбец координат $F(e_j)$ в *том же самом* базисе e, то при замене базиса e на базис $u = eC_{eu}$ матрица оператора F в новом базисе будет равна

$$F_u = C_{eu}^{-1} F_e C_{eu}\,. \tag{8-13}$$

8.5. Некоммутативные кольца. Абелева группа R с операцией умножения $R \times R \to R$ называется *кольцом*, если умножение ассоциативно, т. е. $\forall\ f, g, h \in R\ \ f(gh) = (fg)h$ и двусторонне дистрибутивно, т. е. $\forall\, f, g, h \in R\ \ f(g+h) = fg + fh$ и $(f+g)h = fh + gh$. Если в кольце R существует элемент e, такой что $ef = fe = f$ для всех $f \in R$, этот элемент называется *единицей* и кольцо называется *кольцом с единицей*.

Упражнение 8.9. Покажите, что $0 \cdot f = 0$ для всех f в любом кольце R и что единичный элемент единственен (если существует).

Всякая (некоммутативная) алгебра является одновременно (некоммутативным) кольцом, так что рассмотренные выше алгебра эндоморфизмов векторного пространства и алгебра матриц с элементами из поля доставляют примеры некоммутативных колец. Последний из них можно обобщить.

[1] напомним (см. формулу (6-19) на стр. 93), что j-тый столбец матрицы F_{wu} есть столбец координат вектора $F(u_j)$ по базису w

8.5.1. Матрицы над некоммутативным кольцом. Квадратные $n \times n$-матрицы с элементами из произвольного кольца R образуют кольцо $\mathrm{Mat}_n(R)$, сложение и умножение в котором задаются теми же правилами, что и сложение и умножение матриц с элементами из поля: сумма $S = F + G$ и произведение $P = FG$ матриц $F = \left(f_{ij}\right)$ и $G = \left(g_{ij}\right)$ имеют в качестве матричных элементов

$$s_{ij} = f_{ij} + g_{ij} \quad \text{и} \quad p_{ij} = \sum_{\nu} f_{i\nu} g_{\nu j}$$

Упражнение 8.10. Проверьте выполнение свойств ассоциативности и дистрибутивности для умножения матриц с элементами из произвольного кольца.

Замечание 8.2. Вычисления с матрицами, элементы которых лежат в некоммутативном кольце отличаются от вычислений с матрицами, элементы которых лежат в поле, двумя существенными особенностями: сомножители в произведениях нельзя переставлять друг с другом (последствие некоммутативности) и не на все ненулевые элементы можно делить (последствие того, что не все элементы кольца обратимы).

Например, формула (8-4) перестаёт быть верной над некоммутативным кольцом, поскольку при её выводе мы переставили сомножители, когда выделили на побочной диагонали матрицы F^2 общий множитель $(a + d)$ — над некоммутативным кольцом этот множитель, вообще говоря, не выносится.

Аналогично, критерий обратимости матрицы размера 2×2 и формула (8-6) для обратной матрицы над некоммутативным кольцом, вообще говоря, неверны, а над коммутативным кольцом, не являющимся полем, нуждаются в уточнении: 2×2-матрица над коммутативным кольцом обратима тогда и только тогда, когда её определитель $\det F$ обратим, и если это так, то имеет место формула (8-6) для обратной матрицы.

Упражнение 8.11. Докажите последнее утверждение.

8.5.2. Примеры обратимых матриц 2×2. Матрица вида

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

с элементами из произвольного (некоммутативного) кольца R обратима тогда и только тогда, когда обратимы её диагональные элементы. В самом деле, из равенства

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ dz & dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

вытекает, что $dw = 1$ и $dz = 0$, откуда d обратим, а $w = d^{-1}$ и $z = 0$. Поэтому $ax = 1$, откуда a обратим, а $x = a^{-1}$. Тогда в правом верхнем углу получаем соотношение $ay + bd^{-1} = 0$, из которого $y = -a^{-1}bd^{-1}$. Таким образом,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}bd^{-1} \\ 0 & d^{-1} \end{pmatrix}$$

Аналогичные рассуждения показывают, что обратимость матрицы вида

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

равносильна обратимости диагональных элементов a, d, и в этом случае

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -d^{-1}ca^{-1} & d^{-1} \end{pmatrix}$$

Упражнение 8.12. Покажите, что матрицы $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ обратимы тогда и только тогда, когда обратимы оба элемента c и b, и в этом случае

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}ac^{-1} \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -c^{-1}db^{-1} & c^{-1} \\ b^{-1} & 0 \end{pmatrix}$$

Из проделанных вычислений вытекает, что гауссовы элементарные преобразования строк задаются умножениями на обратимые матрицы и, стало быть, могут применяться для обращения матриц методом Гаусса над произвольным некоммутативным кольцом с единицей.

8.5.3. Обратимость унитреугольных матриц Диагонали

$$\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} & & * \\ & * & \\ * & & \end{pmatrix}$$

квадратной матрицы называются, соответственно, *главной* и *побочной*. Квадратная матрица называется *верхней* (соотв. *нижней*) *треугольной*, если у неё обращаются в нуль все элементы, стоящие под (соотв. над) *главной* диагональю.

Упражнение 8.13. Проверьте, что над любым (в том числе некоммутативным) кольцом R верхние и нижние треугольные матрицы составляют подкольца в $\mathrm{Mat}_n(R)$.

Если в кольце R есть единица, то треугольные матрицы с единицами на главной диагонали называются *унитреугольными*.

Лемма 8.2
Любая верхняя унитреугольная матрица $A = (a_{ij})$ над произвольным (в том числе, некоммутативным) кольцом с единицей обратима, причём $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами

$$b_{ij} = \sum_{s=0}^{j-i-1} (-1)^{s+1} \sum_{i<\nu_1<\cdots<\nu_s<j} a_{i\nu_1}a_{\nu_1\nu_2}a_{\nu_2\nu_3}\ \dots\ a_{\nu_{s-1}\nu_s}a_{\nu_s j} =$$
$$= -a_{ij} + \sum_{i<k<j} a_{ik}a_{kj} - \sum_{i<k<\ell<j} a_{ik}a_{k\ell}a_{\ell j} + \sum_{i<k<\ell<m<j} a_{ik}a_{k\ell}a_{\ell m}a_{mj} - \cdots . \quad (8\text{-}14)$$

Доказательство. Прямое вычисление методом Гаусса. Для матрицы 4×4

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} \\ 0 & 1 & a_{23} & a_{24} \\ 0 & 0 & 1 & a_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

оно выглядит так: приписываем справа единичную матрицу

$$\left(\begin{array}{cccc|cccc} 1 & a_{12} & a_{13} & a_{14} & 1 & 0 & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

зануляем 1-й столбец над главной диагональю используя 2-ю строку

$$\left(\begin{array}{cccc|cccc} 1 & 0 & a_{13}-a_{12}a_{23} & a_{14}-a_{12}a_{24} & 1 & -a_{12} & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

зануляем 2-й столбец над главной диагональю используя 3-ю строку

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & a_{14}-a_{12}a_{24}-a_{13}a_{34}+a_{12}a_{23}a_{34} & 1 & -a_{12} & -a_{13}+a_{12}a_{23} & 0 \\ 0 & 1 & 0 & a_{24}-a_{23}a_{34} & 0 & 1 & -a_{23} & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

наконец, зануляем последний столбец, используя 4-ю строку, получая справа

$$A^{-1}=\begin{pmatrix} 1 & -a_{12} & -a_{13}+a_{12}a_{23} & -a_{14}+a_{12}a_{24}+a_{13}a_{34}-a_{12}a_{23}a_{34} \\ 0 & 1 & -a_{23} & -a_{24}+a_{23}a_{34} \\ 0 & 0 & 1 & -a_{23} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

В общем случае удобно нарисовать n различных точек $1, 2, \dots, n$ и воспринимать матричный элемент a_{ij} как стрелку, ведущую из j в i, а левое умножение на a_{ij} — как проход из j в i по этой стрелке. Тогда формула (8-14) гласит, что b_{ij} равен сумме всех маршрутов, ведущих из j в i, в которую все маршруты, состоящие из $s+1$ стрелок, входят со знаком $(-1)^{s+1}$. По индукции, умножая $n\times(2n)$-матрицу $\boxed{A\,|\,E}$ слева на матрицу

$$S=\begin{pmatrix} 1 & b_{12} & b_{13} & \dots & b_{1\,(n-1)} & 0 \\ 0 & 1 & b_{23} & \dots & b_{2\,(n-1)} & 0 \\ & & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & b_{(n-2)\,(n-1)} & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}$$

в левом верхнем углу которой стоит матрица размера $(n-1)\times(n-1)$, обратная к верхней левой угловой подматрице в A, образованной первыми $(n-1)$ строками и столбцами, мы получим в последнем n-том столбце левой половины матрицы

$$S\cdot\boxed{A\,|\,E}$$

в позиции (i,n) сумму $a_{in}+b_{i2}a_{2n}+b_{i3}a_{3n}+\dots+b_{i\,(n-1)}a_{(n-1)\,n}$ всех маршрутов, ведущих из n в i, в которую каждый маршрут длины $s+1$ входит со знаком $(-1)^s$. Обнуляя этот столбец методом Гаусса, получаем в n-м столбце правой половины матрицы требуемые значения b_{in}. □

§9. Определители

9.1. Объём и полилинейные косые формы. Интуитивным геометрическим критерием линейной зависимости набора векторов $v_1, v_2, \dots, v_n$ в n-мерном векторном пространстве V является обращение в нуль *объёма* параллелепипеда, для которого эти векторы составляют множество рёбер, исходящих из одной вершины (см. рис. 9⋄1). Не ставя себе задачу определить объём сколь-нибудь общей фигуры, отметим, что объём параллелепипеда, как бы он ни определялся, должен обладать следующими двумя геометрическими свойствами: во-первых, он не должен меняться при сохраняющем высоту «параллельном перекосе» параллелепипеда вдоль любой из сторон в плоскости любой примыкающей к этой стороне двумерной грани[1], как на рис. 9⋄2.

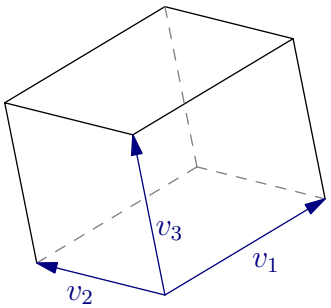


Рис. 9⋄1. Параллелепипед.

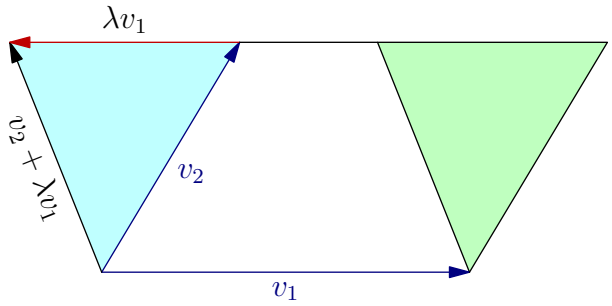


Рис. 9⋄2. Параллельный перекос.

во-вторых при растяжении одной из сторон параллелепипеда в λ раз объём должен умножаться[2] на λ. Оказывается, что эти свойства *определяют* объём параллелепипеда однозначно с точностью до постоянного множителя (см. сл. 9.3 ниже).

Определение 9.1
Функция $\omega : V_1 \times V_2 \times \dots \times V_n \to \Bbbk$, сопоставляющая каждому упорядоченному набору векторов $(v_1, v_2, \dots, v_n)$ n-мерного векторного пространства V над полем $\Bbbk$ число $\omega(v_1, v_2, \dots, v_n) \in \Bbbk$, называется *формой n-мерного объёма* (или *ориентированным n-мерным объёмом*) на пространстве V, если она удовлетворяет следующим двум свойствам:

1) объём не меняется при добавлений к одному из аргументов произвольной кратности любого другого: $\omega\left(\dots, v_i + \lambda v_j, \dots, v_j, \dots\right) = \omega\left(\dots, v_i, \dots, v_j, \dots\right)$

2) при умножении одного из аргументов на число объём умножается на это число: $\omega(\dots, \lambda v_i, \dots) = \lambda\, \omega(\dots, v_i, \dots)$

(в обеих формулах все отмеченные многоточием аргументы в левой и в правой части равенства остаются без изменений).

[1] на рис. 9⋄2 изображена параллельная проекция происходящего на плоскость той грани, в которой совершается «перекос», вдоль дополнительного к этой грани $(n-2)$-мерного подпространства, натянутого на все остальные рёбра; видно, что «отрезаемая» слева призма параллельно переносится вправо и «прикладывается» к параллелепипеду с другой стороны

[2] например, при удвоении любой стороны объём удваивается

Лемма 9.1
На любом векторном пространстве размерности n над произвольным полем $\Bbbk$ всякая форма n-мерного объёма обращается в нуль, если аргументы линейно зависимы (в частности, когда среди аргументов есть совпадающие и/или нулевые), линейна каждому из своих аргументов при фиксированных остальных:

$$\omega(\dots, \lambda v + \mu w, \dots) = \lambda\,\omega(\dots, v, \dots) + \mu\,\omega(\dots, w, \dots) \tag{9-1}$$

и меняет знак при перестановке любых двух аргументов местами:

$$\omega(\dots, v, \dots, w, \dots) = -\omega(\dots, w, \dots, v, \dots)\,. \tag{9-2}$$

Доказательство. Если векторы $v_1, v_2, \dots, v_n$ линейно зависимы, то один из них выражается через остальные. Пусть, например, $v_1 = \lambda_2 v_2 + \dots + \lambda_n v_n$. Тогда

$$\omega(v_1, v_2, \dots, v_n) = \omega(v_1 - \lambda_2 v_2 - \dots - \lambda_n v_n,\, v_2,\, \dots,\, v_n) = \\ = \omega(0, v_2, \dots, v_n) = \omega(0 \cdot 0, v_2, \dots, v_n) = 0 \cdot \omega(0, v_2, \dots, v_n) = 0\,.$$

Для доказательства линейности заметим, что если оба набора аргументов в правой части (9-1) линейно зависимы, то набор аргументов в левой части тоже линейно зависим, и стало быть, обе части равенства нулевые. Поэтому мы можем без ограничения общности считать, что аргументы первого слагаемого правой части образуют базис пространства V. Разложение w по этому базису имеет вид $w = \varrho v + u$, где u является линейной комбинацией остальных $(n-1)$ аргументов. По первому свойству объёма левая часть (9-1) равна $\omega(\dots, \lambda v + \mu w, \dots) = \omega(\dots, (\lambda + \mu\varrho)v + \mu u, \dots) = \omega(\dots, (\lambda + \mu\varrho)v, \dots)$, а второе слагаемое правой части (9-1) равно $\mu\omega(\dots, w, \dots) = \mu\omega(\dots, \varrho v + u, \dots) = \mu\omega(\dots, \varrho v, \dots)$. Тем самым, вся правая часть $\lambda\omega(\dots, v, \dots) + \mu\omega(\dots, \varrho v, \dots) = (\lambda + \mu\varrho)\,\omega(\dots, v, \dots)$ совпадает с левой. Равенство (9-2) вытекает из линейности объёма и его обращения в нуль при совпадении любых двух аргументов: $0 = \omega(\dots, v + w, \dots, v + w, \dots) = \omega(\dots, v, \dots, v, \dots) + \\ + \omega(\dots, v, \dots, w, \dots) + \omega(\dots, w, \dots, v, \dots) + \omega(\dots, w, \dots, w, \dots) = \omega(\dots, v, \dots, w, \dots) + \\ + \omega(\dots, w, \dots, v, \dots)$. □

Определение 9.2
Пусть K — произвольное коммутативное кольцо, и V — любой K-модуль. Отображение $\omega : V \times V \times \dots \times V \to K$ называется *полилинейной*[1] *косой формой*, если оно линейно по каждому аргументу при фиксированных остальных и обращается в нуль всякий раз, когда какие-нибудь из два из аргументов совпадают друг с другом.

Пример 9.1 (форма объёма)
Согласно лем. 9.1 всякая форма объёма на n-мерном векторном пространстве V является n-линейной косой формой. Обратное тоже верно: любая полилинейная косая форма от n аргументов является формой объёма, т. е. удовлетворяет двум условиям из опр. 9.1 на стр. 130. Действительно, второе свойство составляет часть линейности, а первое вытекает из линейности и кососимметричности:

$$\omega\left(\dots, v_i + \lambda v_j, \dots, v_j, \dots\right) = \\ = \omega\left(\dots, v_i, \dots, v_j, \dots\right) + \lambda\,\omega\left(\dots, v_j, \dots, v_j, \dots\right) = \\ = \omega\left(\dots, v_i, \dots, v_j, \dots\right).$$

[1] *или, точнее, m-линейной, когда число аргументов у ω равно m*

9.2. Знак перестановки. В доказательстве лем. 9.1 мы видели, что из полилинейности и кососимметричности вытекает *знакопеременность*: каждая полилинейная косая форма «меняет знак» при перестановке двух аргументов местами:

$$\omega(\dots, v, \dots, w, \dots) = -\omega(\dots, w, \dots, v, \dots).$$

Если $1+1$ не делит нуль в K, то и наоборот, из знакопеременности полилинейной формы вытекает её кососимметричность: $\omega(\dots, v, \dots, v, \dots) = 0$.

Следуя прим. 1.6 на стр. 14, будем воспринимать каждую перестановку

$$g = (g_1, g_2, \dots, g_n) \in S_n$$

элементов набора $(1,\ 2,\ \dots\ ,\ n)$ как биективное отображение из множества $\{1,\ 2,\ \dots\ ,\ n\}$ в себя, переводящее элемент i в элемент g_i. Например, перестановка $(2, 4, 3, 5, 1)$ пяти чисел $1, 2, 3, 4, 5$ соответствует отображению $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 5$, $5 \mapsto 1$. Композиция fg перестановок $f, g \in S_n$ действует по правилу $fg : i \mapsto f\big(g(i)\big)$: например, в группе S_5 перестановки $f = (2, 4, 3, 5, 1)$ и $g = (3, 2, 1, 5, 4)$ имеют композиции $fg = (3, 4, 2, 1, 5)$ и $gf = (2, 5, 1, 4, 3)$.

Перестановка, которая меняет между собою местами какие-нибудь два элемента i и j, а все остальные элементы $k \neq i, j$ оставляет на месте, называется *транспозицией* элементов i и j и обозначается σ_{ij}.

Упражнение 9.1. Убедитесь, что каждая перестановка является композицией транспозиций.

Перестановки, представимые в виде композиции чётного числа транспозиций, называются *чётными*, а перестановки, раскладывающиеся в композицию нечётного числа транспозиций — *нечётными*.

Разложение перестановки в композицию транспозиций *не единственно*: например, $\sigma_{13} = (3, 2, 1) \in S_3$ можно получить и как $\sigma_{12}\sigma_{23}\sigma_{12}$, и как $\sigma_{23}\sigma_{12}\sigma_{23}$. Однако, не смотря на эту неоднозначность, чётность перестановки корректно определена в том смысле, что одну и ту же перестановку нельзя представить в виде композиции как чётного, так и нечётного числа транспозиций. Это открывает возможность существования ненулевых косых форм: если бы имелась перестановка, одновременно являющаяся как чётной, так и нечётной, то любая знакопеременная форма обязана была бы обращаться в нуль на любом наборе векторов.

Чтобы убедиться в том, что чётность перестановки не зависит от выбора её разложения в композицию транспозиций, мы укажем другой способ определения чётности, не использующий такового разложения. Назовём упорядоченную пару чисел (i, j), в которой $1 \leqslant i < j \leqslant n$, *инверсной парой* перестановки $g \in S_n$, если $g(i) > g(j)$. Таким образом, каждая перестановка $g \in S_n$ разбивает множество всех $n(n-1)/2$ пар (i, j) с $1 \leqslant i < j \leqslant n$ на два непересекающихся подмножества — инверсные пары и неинверсные пары.

Лемма 9.2
Чётность числа инверсных пар каждой перестановки совпадает с чётностью количества транспозиций, на которые её можно разложить.

Доказательство. Для любой перестановки g и любой транспозиции σ_{ij} чётность числа инверсных пар у перестановок g и $g\sigma_{ij}$ различна. В самом деле, перестановки

$$\begin{aligned} g &= \bigl(g_1, \dots, g_{i-1}, \boldsymbol{g_i}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_j}, g_{j+1}, \dots, g_n\bigr) \\ g\sigma_{ij} &= \bigl(g_1, \dots, g_{i-1}, \boldsymbol{g_j}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_i}, g_{j+1}, \dots, g_n\bigr) \end{aligned} \tag{9-3}$$

отличаются друг от друга транспозицией элементов $g_i = g(i)$ и $g_j = g(j)$, стоящих на i-том и j-том местах, и наше утверждение вытекает из следующего упражнения:

Упражнение 9.2. Проверьте, что у двух перестановок (9-3) пара (i, j), а также $2(j-i-1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ имеют противоположную инверсность[1], а инверсность всех остальных пар одинакова.

Таким образом, если перестановка g разложена в композицию транспозиций, то чётность числа инверсных пар в ней отличается от чётности числа инверсных пар в тождественной перестановке в точности на чётность числа транспозиций, на которые разложена g. □

Следствие 9.1 (знак перестановки)
Существует единственное отображение $\operatorname{sgn} : S_n \twoheadrightarrow \{+1, -1\}$ со свойствами: $\operatorname{sgn}(\mathrm{Id}) = 1$, $\operatorname{sgn}(\sigma_{ij}) = -1$ для всех транспозиций σ_{ij} и $\operatorname{sgn}(fg) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g)$ для всех $f, g \in S_n$. Это отображение корректно определяется формулой

$$\operatorname{sgn}(g_1, g_2, \dots, g_n) = \begin{cases} +1 & \text{если перестановка } (g_1, g_2, \dots, g_n) \text{ чётна} \\ -1 & \text{если перестановка } (g_1, g_2, \dots, g_n) \text{ нечётна}. \end{cases} \tag{9-4}$$

Пример 9.2 (правило ниточек)
Интерпретация чётности перестановки как чётности числа инверсных пар даёт практический способ отыскания чётности перестановки — возможно, не самый быстрый[2], но всё же полезный в некоторых ситуациях, с которыми мы далее столкнёмся. Напишем исходные числа и их перестановку друг под другом, как на рис. 9⋄3, и соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала за пределы прямоугольника, образованного четырьмя угловыми числами, и чтобы все точки пересечения нитей были простыми двойными[3]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

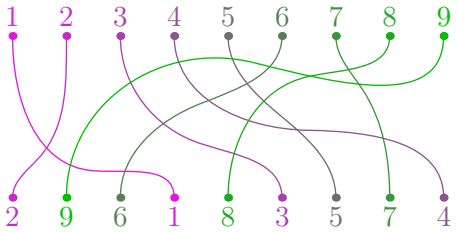


Рис. 9⋄3. $\operatorname{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (всего 18 пересечений).

[1] т. е. если такая пара инверсна в g, то она не инверсна в $\sigma_{ij}g$ и наоборот

[2] обычно быстрее бывает разложить перестановку в композицию непересекающихся циклов и воспользоваться тем, что циклы чётной длины нечётны, а циклы нечётной длины чётны

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

Упражнение 9.3. 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 $(i_1, i_2, \dots, i_k)$ и $(j_1, j_2, \dots, j_m)$ не пересекаются, и каждый из них строго возрастает слева направо.

Теорема 9.1
Для любого коммутативного кольца K с единицей на координатном модуле K^n существует единственная с точностью до пропорциональности ненулевая косая форма от n аргументов. Её значение на произвольном наборе векторов $v = e \cdot C_{ev}$, где матрица $C_{ev} = \left(c_{ij}\right) \in \mathrm{Mat}_n(K)$ имеет в j-том столбце координаты вектора v_j в стандартном базисе e координатного модуля K^n, вычисляется по формуле:

$$\begin{gathered}\omega(v_1, v_2, \dots, v_n) = \omega(e_1, e_2, \dots, e_n) \cdot \det\left(c_{ij}\right), \quad \text{где} \\ \det\left(c_{ij}\right) = \sum_g \operatorname{sgn}(g_1, g_2, \dots, g_n) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n}\end{gathered} \tag{9-5}$$

и суммирование происходит по всем перестановкам $g = (g_1, g_2, \dots, g_n) \in S_n$.

Доказательство. Подставим в $\omega(v_1, v_2, \dots, v_m)$ разложения $v_j = \sum\limits_{i=1}^{n} e_i \cdot c_{ij}$ и воспользуемся полилинейностью:

$$\omega(v_1, v_2, \dots, v_n) = \omega\Big(\sum_{i_1} e_{i_1} c_{i_1 1}, \sum_{i_2} e_{i_2} c_{i_2 2}, \ \dots\ , \sum_{i_n} e_{i_n} c_{i_n n} \Big) =$$

$$= \omega\left(e_{i_1}, e_{i_2}, \dots, e_{i_n}\right) \cdot \sum_{i_1 i_2 \dots i_n} c_{i_1 1} \cdot c_{i_2 2} \cdot \ \cdots\ \cdot c_{i_n n}\,.$$

Так как при совпадении двух аргументов ω обращается в нуль, ненулевой вклад в последнюю сумму вносят только наборы $(i_1, i_2, \dots, i_n)$, в которых каждое из чисел $1,\ 2,\ \dots\ , n$ встречается ровно один раз, причём

$$\omega(e_{i_1}, e_{i_2}, \dots, e_{i_n}) = \begin{cases} +\omega(e_1, e_2, \dots, e_n) & \text{если перестановка } (i_1, i_2, \dots, i_n) \text{ чётна} \\ -\omega(e_1, e_2, \dots, e_n) & \text{если перестановка } (i_1, i_2, \dots, i_n) \text{ нечётна} \end{cases}$$

что и даёт формулу (9-5). Из неё следует, что существует самое большее одна n-линейная косая форма ω_1 на K^n, принимающая на стандартном базисе e значение 1, а на произвольном наборе векторов $v = eC_{ev}$ — значение

$$\omega(v_1, v_2, \dots, v_n) = \det(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \det C_{ev}\,, \tag{9-6}$$

где C_{ev} — квадратная матрица размера $n \times n$, в j-том столбце которой записаны координаты вектора v_j в базисе e. При этом для любой n-линейной косой формы ω на K^n и любого набора векторов $(v_1, v_2, \dots, v_n)$ выполняется равенство:

$$\omega(v_1, v_2, \dots, v_n) = \omega_1(v_1, v_2, \dots, v_n) \cdot \omega(e_1, e_2, \dots, e_n),$$

означающее, что форма $\omega = \lambda \cdot \omega_1$ пропорциональна форме ω_1 с коэффициентом $\lambda = \omega(e_1, e_2, \dots, e_n) \in K$. Для завершения доказательства остаётся проверить, что формула (9-6) действительно задаёт полилинейную косую форму на K^n, т. е. что функция

$$\det : \mathrm{Mat}_n(K) \to K$$

является полилинейной косой формой от столбцов матрицы. Мы сделаем это в предл. 9.1 ниже. □

9.3. Определитель. Стоящее в правой части равенства (9-5) выражение

$$\det C = \det(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \sum_{g \in S_n} \operatorname{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n} \tag{9-7}$$

называется *определителем* квадратной матрицы $C = \left(c_{ij}\right) \in \operatorname{Mat}_n(K)$ или набора векторов $v_1, v_2, \dots, v_n \in K^n$, образующих столбцы матрицы C. Для вычисления определителя следует всеми возможными способами выбирать из матрицы n-ки элементов так, чтобы в каждой строке и в каждом столбце выбиралось ровно по одному элементу. Выбранные n элементов перемножаются и полученные таким образом $n!$ произведений складываются с надлежащими знаками, которые определяются так: множество клеток, где стоят выбранные элементы, представляет собою график биективного отображения $j \mapsto g_j$ из множества номеров столбцов в множество номеров строк, и произведению приписывается знак этой перестановки.

Например, определители матриц размера 2×2 и 3×3 имеют вид

$$\det \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{12}c_{21} \tag{9-8}$$

$$\begin{aligned} \det \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = {} & c_{11}c_{22}c_{33} + c_{13}c_{21}c_{32} + c_{12}c_{23}c_{31} - \\ & - c_{11}c_{23}c_{32} - c_{13}c_{22}c_{31} - c_{12}c_{21}c_{33} \end{aligned} \tag{9-9}$$

(во втором равенстве сначала выписаны тождественная и две циклических перестановки, потом — три транспозиции).

Предложение 9.1
Определитель $\det C = \det(v_1, v_2, \dots, v_n)$ линеен по каждому столбцу матрицы C, кососимметричен, и $\det C^t = \det C$ где $C^t = \left(c^t_{ij}\right)$ — матрица, транспонированная[1] к $C = \left(c_{ij}\right)$.

Доказательство. Каждое из складываемых в формуле (9-7) произведений содержит ровно по одному сомножителю из каждого столбца и, стало быть, линейно по каждому столбцу. Поэтому линейна и их сумма. Это доказывает первое утверждение. Если i-тый столбец матрицы C совпадает с j-тым, то составляющие сумму (9-7) произведения разбиваются на отвечающие перестановкам g и $g\sigma_{ij}$ пары вида[2]

$$\operatorname{sgn}(g) \cdot c_{g_1 1} \cdots c_{g_i i} \cdots c_{g_j j} \cdots c_{g_n n} \quad \text{и} \quad \operatorname{sgn}(g\sigma_{ij}) \cdot c_{g_1 1} \cdots c_{g_j i} \cdots c_{g_i j} \cdots c_{g_n n},$$

различающиеся только знаком, поскольку $c_{g_i i} = c_{g_i j}$ и $c_{g_j j} = c_{g_j i}$. Стало быть, сумма получится нулевой. Наконец, равенство $\det C^t = \det C$ вытекает из того, что набор произведений n-ок матричных элементов в разложениях $\det C$ и $\det C^t$ одинаков, а знаки, с которыми каждое произведение входит в $\det C$ и $\det C^t$, суть знаки обратных друг другу перестановок.

Упражнение 9.4. Покажите, что обратные друг другу перестановки имеют одинаковую чётность.

[1] так что $c^t_{ij} = c_{ji}$

[2] ср. с форм. (9-3) на стр. 133

Таким образом, разложения (9-7) для $\det C$ и $\det C^t$ состоят из одних и тех же слагаемых с одними и теми же знаками. □

Следствие 9.2
Определитель матрицы является полилинейной кососимметричной формой от её строк.

Следствие 9.3
На любом конечномерном векторном пространстве над любым полем существует единственная с точностью до пропорциональности ненулевая форма объёма ω. Если

$$\omega(e_1, e_2, \dots, e_n) = 1$$

и набор векторов $v = (v_1, v_2, \dots, v_n)$ выражаются через набор векторов $e = (e_1, e_2, \dots, e_n)$ по формуле $v = eC_{ev}$, то $\omega(v_1, v_2, \dots, v_n) = \det C_{ev}$.

Предложение 9.2 (мультипликативность определителя)
$\det(AB) = \det(A) \cdot \det(B)$ для любых матриц $A, B \in \mathrm{Mat}_n(K)$ над любым кольцом K.

Доказательство. Разность $\det(AB) - \det(A) \cdot \det(B)$ представляет собой многочлен с целыми коэффициентами от $2n^2$ переменных a_{ij} и b_{ij}. Достаточно проверить, что этот многочлен нулевой: тогда подставляя в него произвольные элементы произвольного кольца мы получим нуль. Для проверки того, что многочлен $f \in \mathbb{Z}[x_1, x_2, \dots, x_m]$ нулевой, достаточно установить, что его значение в каждой точке $p \in \mathbb{Q}^m$ нулевое.

Упражнение 9.5. Убедитесь, что над бесконечным полем $\Bbbk$ только нулевой многочлен от m переменных принимает нулевое значение во всех точках пространства $\Bbbk^m$ и покажите, что над конечным полем $\mathbb{F}_q$ это не так.

Таким образом, достаточно доказать предложение для $K = \mathbb{Q}$, что мы и сделаем.

Если столбцы $v_1, v_2, \dots, v_n \in \mathbb{Q}^n$ матрицы A линейно зависимы, то размерность их линейной оболочки меньше n. Поскольку столбцы матрицы AB лежат в линейной оболочке столбцов матрицы A, размерность их линейной оболочки тоже меньше n, и значит, они тоже линейно зависимы. Таким образом, в этом случае $\det A = 0$ и $\det AB = 0$, и равенство $\det A \det B = \det AB$ тривиально выполняется.

Если векторы v_i линейно независимы, то они образуют в $\mathbb{Q}^n$ базис. Зададим на пространстве $\mathbb{Q}^n$ две формы объёма: ω_e, такую что $\omega_e(e_1, e_2, \dots, e_n) = 1$ на элементах стандартного базиса e пространства $\mathbb{Q}^n$, и ω_v, такую что $\omega_v(v_1, v_2, \dots, v_n) = 1$. По сл. 9.3 эти две формы пропорциональны друг другу, и так как $\omega_1(v_1, v_2, \dots, v_n) = \det A$, коэффициент пропорциональности равен $\det A$:

$$\omega_1 = \det(A) \cdot \omega_v\,. \tag{9-10}$$

Обозначим через $w_1, w_2, \dots, w_n \in \mathbb{Q}^n$ векторы, координаты которых в базисе $v_1, v_2, \dots, v_n$ являются столбцами матрицы B, т. е.

$$(w_1, w_2, \dots, w_n) = (v_1, v_2, \dots, v_n) \cdot B = (e_1, e_2, \dots, e_n) \cdot AB\,.$$

Тогда по сл. 9.3 $\omega_v(w_1, w_2, \dots, w_n) = \det(B)$, а $\omega_e(w_1, w_2, \dots, w_n) = \det(AB)$, и из (9-10) вытекает требуемое равенство $\det AB = \det A \det B$. □

Следствие 9.4
$\forall\, A, B \in \mathrm{Mat}_n(K)\ \ \det(AB) = \det(BA)$.

9.3.1. Определитель линейного оператора. Зафиксируем на конечномерном векторном пространстве V форму объёма ω. Для любого линейного оператора $F : V \to V$ форма

$$\omega_F(v_1, v_2, \dots, v_n) \stackrel{\text{def}}{=} \omega\left(Fv_1,\ Fv_2,\ \dots\ , Fv_n\right)$$

полилинейна и кососимметрична. Поэтому она пропорциональна форме ω. Коэффициент пропорциональности равен отношению значений этих двух форм на элементах любого базиса $e = (e_1, e_2, \dots, e_n)$ пространства V и не зависит от выбора базиса e. Поскольку $\left(Fe_1,\ Fe_2,\ \dots\ , Fe_n\right) = (e_1, e_2, \dots, e_n) \cdot F_e$, где F_e — матрица оператора F в базисе e, коэффициент пропорциональности равен определителю матрицы оператора:

$$\frac{\omega_F}{\omega} = \frac{\omega\left(Fe_1,\ Fe_2,\ \dots\ , Fe_n\right)}{\omega(e_1, e_2, \dots, e_n)} = \frac{\omega(e_1, e_2, \dots, e_n) \cdot \det F_e}{\omega(e_1, e_2, \dots, e_n)} = \det F_e$$

Таким образом, $\det F_e$ не зависит от e, и при применении F к любому набору векторов объём натянутого на них параллелепипеда умножается на $\det F_e$. Определитель $\det F_e$ называется *определителем линейного оператора* $F : V \to V$ и обозначается $\det F$.

Из предл. 9.2 вытекает, что определитель мультипликативен по отношению к композиции: $\det FG = \det F \det G$. Поэтому операторы определителя один образуют в полной линейной группе $\mathrm{GL}(V)$ подгруппу. Она обозначается $\mathrm{SL}(V)$ и называется *специальной линейной группой* пространства V. Геометрически, специальная линейная группа состоит из всех операторов, сохраняющих некоторую (а значит, и любую) ненулевую форму объёма.

Специальная линейная группа координатного пространства $\Bbbk^n$ состоит из матриц определителя 1 и обозначается $\mathrm{SL}_n(\Bbbk) \subset \mathrm{GL}_n(\Bbbk)$.

9.4. Грассмановы многочлены. Полезным алгебраическим инструментом для работы с определителями являются *грассмановы многочлены*. Алгебра *грассмановых многочленов* $K\langle\xi_1, \xi_2, \dots, \xi_n\rangle$ от переменных $\xi_1, \xi_2, \dots, \xi_n$ с коэффициентами в коммутативном кольце K определяется точно также, как алгебра обычных многочленов, с той только разницей, что грассмановы переменные ξ_i, в отличие от обычных, не коммутируют, а *антикоммутируют* друг с другом, т. е. подчиняются соотношениям[1]

$$\forall\, i, j \quad \xi_i \wedge \xi_j = -\xi_j \wedge \xi_i \quad \text{и} \quad \forall\, i \quad \xi_i \wedge \xi_i = 0\,. \tag{9-11}$$

Символ « $\wedge$ » здесь и далее используется для обозначения грассманова (антикоммутативного) умножения, чтобы отличать его от обычного (коммутативного). Для каждой строго возрастающей слева направо последовательности номеров $I = (i_1, i_2, \dots, i_m)$, положим

$$\xi_I \stackrel{\text{def}}{=} \xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}\,, \quad i_1 < i_2 < \dots < i_m\,. \tag{9-12}$$

Перестановка переменных $g \in S_m$ меняет знак этого монома по правилу

$$\xi_{i_{g(1)}} \wedge \xi_{i_{g(2)}} \wedge \dots \wedge \xi_{i_{g(m)}} = \mathrm{sgn}(g) \cdot \xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}\,. \tag{9-13}$$

[1]если $1 + 1$ не делит нуль в K, то соотношения $\xi_i \wedge \xi_i = 0$ могут быть опущены, поскольку они вытекают из соотношений $\xi_i \wedge \xi_j = -\xi_j \wedge \xi_i$, если положить в них $i = j$; если же $-1 = 1$, то условия антикоммутирования $\xi_i \wedge \xi_j = -\xi_j \wedge \xi_i$ и коммутирования $\xi_i \wedge \xi_j = \xi_j \wedge \xi_i$ совпадают друг с другом, и именно соотношение $\xi_i \wedge \xi_i = 0$ отличает грассмановы переменные от обычных

Поскольку квадраты грассмановых переменных равны нулю, мономы (9-13) исчерпывают всё множество грассмановых мономов. Иначе говоря, $\binom{n}{m}$ мономов (9-12) по-определению образуют базис в модуле Λ^m грассмановых многочленов степени m, а вся грассманова алгебра как модуль над K является конечной прямой суммой

$$K\langle\xi_1,\xi_2,\dots,\xi_n\rangle = \Lambda^0 \oplus \Lambda^1 \oplus \Lambda^2 \oplus \dots \oplus \Lambda^n .$$

Умножение базисных мономов (9-12) задаётся правилом

$$\xi_I \wedge \xi_J = \begin{cases} \operatorname{sgn}(i_1,i_2,\dots,i_m,j_1,j_2,\dots,j_k)\cdot\xi_{I\sqcup J} & \text{если } I\cap J=\varnothing \\ 0 & \text{если } I\cap J\neq\varnothing \end{cases} \tag{9-14}$$

(перестановка $(i_1,i_2,\dots,i_m,j_1,j_2,\dots,j_k)\in S_{k+m}$ обратна к тасующей перестановке, расставляющей набор номеров $i_1,i_2,\dots,i_m,j_1,j_2,\dots,j_k$ в порядке их возрастания).

Отметим, что базис в Λ^0 состоит из единственного монома нулевой степени $\xi_\varnothing \stackrel{\text{def}}{=} 1$, отвечающего пустому набору $I=\varnothing$ и являющегося единицей грассмановой алгебры, а базис в Λ^n состоит из единственного монома старшей степени

$$\xi_{\text{top}} = \xi_1\wedge\xi_2\wedge\dots\wedge\xi_n ,$$

который аннулируется умножением на любой грассманов многочлен с нулевым свободным членом.

Два грассмановых монома степеней m и k коммутируют друг с другом по правилу

$$\left(\xi_{i_1}\wedge\xi_{i_2}\wedge\dots\wedge\xi_{i_m}\right)\wedge\left(\xi_{j_1}\wedge\xi_{j_2}\wedge\dots\wedge\xi_{j_k}\right) = \\ = (-1)^{km}\left(\xi_{j_1}\wedge\xi_{j_2}\wedge\dots\wedge\xi_{j_k}\right)\wedge\left(\xi_{i_1}\wedge\xi_{i_2}\wedge\dots\wedge\xi_{i_m}\right)$$

(для перенесения каждой из k переменных ξ_j через m переменных ξ_i требуется m транспозиций). Поэтому для любых двух однородных грассмановых многочленов f и g выполняется *Кошулево правило знаков*

$$f\wedge g = (-1)^{\deg f\deg g} g\wedge f . \tag{9-15}$$

В частности, однородные многочлены чётной степени коммутируют со всеми грассмановыми многочленами.

Упражнение 9.6. Опишите *центр* грассмановой алгебры (т. е. грассмановы многочлены, перестановочные со всеми элементами грассмановой алгебры).

9.4.1. Линейная замена переменных и миноры. Рассмотрим набор однородных грассмановых линейных форм $(\eta_1,\eta_2,\dots,\eta_k)=(\xi_1,\xi_2,\dots,\xi_n)\cdot C$, где $C\in\operatorname{Mat}_{n\times k}(K)$. Составленные из этих форм мономы m-той степени $\eta_J=\eta_{j_1}\wedge\eta_{j_2}\wedge\dots\wedge\eta_{j_m}$ линейно выражаются через базисные мономы $\xi_I=\xi_{i_1}\wedge\xi_{i_2}\wedge\dots\wedge\xi_{i_m}$ следующим образом:

$$\eta_J=\eta_{j_1}\wedge\eta_{j_2}\wedge\dots\wedge\eta_{j_m}=\left(\sum_{i_1}\xi_{i_1}c_{i_1j_1}\right)\wedge\left(\sum_{i_2}\xi_{i_2}c_{i_2j_2}\right)\wedge\dots\wedge\left(\sum_{i_m}\xi_{i_m}c_{i_mj_m}\right)= \\ = \sum_{1\leqslant i_1<i_2<\dots<i_m\leqslant n}\xi_{i_1}\wedge\xi_{i_2}\wedge\dots\wedge\xi_{i_m}\cdot\sum_{g\in S_m}\operatorname{sgn}(g)\,c_{i_{g(1)}j_1}c_{i_{g(2)}j_2}\dots c_{i_{g(m)}j_m}=\sum_I\xi_I\cdot c_{IJ} ,$$

где $c_{IJ} = \det C_{IJ}$ обозначает определитель $m \times m$-подматрицы $C_{IJ} \subset C$, сосредоточенной в пересечениях столбцов с номерами из J и строк с номерами из I, где $I = (i_1, i_2, \dots, i_m)$ пробегает все наборы из m возрастающих номеров $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k$. Определитель $c_{IJ} \stackrel{\text{def}}{=} \det C_{IJ}$ этой подматрицы называется IJ-тым *минором* m-того порядка в матрице C.

Таким образом, IJ-тый элемент матрицы, выражающей грассманов моном η_J через грассмановы мономы ξ_I равен IJ-тому минору m-того порядка в матрицы выражающей переменные η через переменные ξ.

9.5. Соотношения Лапласа. Для каждого набора возрастающих индексов

$$J = (j_1, j_2, \dots, j_m) \subset \{1, 2, \dots, n\}$$

положим $\deg J \stackrel{\text{def}}{=} m$, $|J| \stackrel{\text{def}}{=} j_1 + j_2 + \cdots + j_m$ и условимся обозначать через

$$\bar{J} = \left(\bar{j}_1, \bar{j}_2, \dots, \bar{j}_{n-m}\right) = \{1, 2, \dots, n\} \smallsetminus J$$

дополнительный к J набор возрастающих индексов длины $\deg \bar{J} = n - m$.

Рассмотрим произвольную квадратную матрицу $A \in \mathrm{Mat}_n(K)$ и грассмановы линейные формы $\alpha_1, \alpha_2, \dots, \alpha_n$ от переменных $\xi_1, \xi_2, \dots, \xi_n$, заданные равенствами

$$\alpha_j = \xi_1 \cdot a_{1j} + \xi_2 \cdot a_{2j} + \cdots + \xi_n \cdot a_{nj}. \tag{9-16}$$

Для любых двух наборов I, J одинаковой длины $\deg I = \deg J = m$ произведения

$$\alpha_J = \alpha_{j_1} \wedge \alpha_{j_2} \wedge \cdots \wedge \alpha_{j_m} \quad \text{и} \quad \alpha_{\bar{I}} = \alpha_{\bar{i}_1} \wedge \alpha_{\bar{i}_2} \wedge \cdots \wedge \alpha_{\bar{i}_m}$$

имеют дополнительные степени m и $n - m$. Перемножая их по формуле (9-14), получим

$$\alpha_J \wedge \alpha_{\bar{I}} = \begin{cases} (-1)^{|J| + \frac{m(m+1)}{2}} \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{9-17}$$

(знак соответствующей тасующей перестановки был вычислен в упр. 9.3). Подставляя в равенство (9-17) разложения (9-16), в левой части будем иметь

$$\left(\sum_M \xi_M a_{MJ}\right) \wedge \left(\sum_L \xi_L a_{L\bar{I}}\right) = (-1)^{\frac{m(m+1)}{2}} \xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n \sum_M (-1)^{|M|} a_{MJ} a_{\overline{MI}},$$

где M пробегает все индексы длины $\deg M = m$. В правой же части получим 0 при $I \neq J$ и

$$(-1)^{\frac{m(m+1)}{2} + |J|} \det A \cdot \xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n$$

при $I = J$. Таким образом, для каждых двух наборов J, I по m строк произвольной квадратной матрицы A выполняются *соотношения Лапласа*

$$\sum_M (-1)^{|M| + |J|} a_{MJ} a_{\overline{MI}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{9-18}$$

где суммирование идёт по всем наборам M из m строк матрицы A.

При $I = J$ соотношение (9-18) даёт формулу для вычисления определителя $\det A$ через всевозможные миноры a_{MJ} порядка m, сосредоточенные в m фиксированных столбцах матрицы A с номерами J, и *дополнительные* к ним миноры $a_{\overline{JM}}$ порядка $n-m$, равные определителям матриц, получающихся из A вычёркиванием всех строк и столбцов, содержащих минор a_{MJ}:

$$\det A = \sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MJ}} \tag{9-19}$$

Произведение $(-1)^{|M|+|J|} a_{\overline{MJ}}$ называется *алгебраическим дополнением* к минору a_{MJ} и обозначается $\overline{a}_{MJ}$. При $I \neq J$ соотношение (9-18) имеет с точностью до знака вид

$$\sum_M (-1)^{|M|+|I|} a_{MJ} a_{\overline{MI}} = 0 \tag{9-20}$$

и называется *теоремой об умножении на чужие алгебраические дополнения*, поскольку левая часть в (9-20) отличается от (9-19) тем, что миноры a_{MJ} умножаются не на свои алгебраические дополнения $a_{\overline{MJ}}$, а дополнения $a_{\overline{MI}}$ к минорам a_{MI}, сосредоточенным в другом наборе столбцов $I \neq J$.

Упражнение 9.7. Установите транспонированный вариант соотношений Лапласа

$$\sum_M (-1)^{|I|+|M|} a_{JM} a_{\overline{IM}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{9-21}$$

Если согласованно занумеровать все m-элементные подмножества и все $(n-m)$-элементные подмножества в множестве $\{1, 2, \ldots, n\}$ так, чтобы дополнительные подмножества J и $\bar{J}$ имели одинаковые номера, и обозначить через $\mathcal{A}_m$ и $\mathcal{A}_m^\vee$ квадратные матрицы размера $\binom{n}{m} \times \binom{n}{m}$, у которых в позиции IJ стоят, соответственно, $\bar{I}\bar{J}$-тый минор a_{IJ} и алгебраическое дополнение $(-1)^{|J|+|I|} a_{\overline{JI}}$ к $\bar{J}\bar{I}$-тому[1] минору матрицы A, то все соотношения Лапласа (9-18) можно записать одним матричным равенством

$$\mathcal{A}_m^\vee \cdot \mathcal{A}_m = \det A \cdot \mathcal{E}, \tag{9-22}$$

где через $\mathcal{E}$ — единичная матрица размера $\binom{n}{m} \times \binom{n}{m}$, а их транспонированные версии (9-21) — равенством

$$\mathcal{A}_m \cdot \mathcal{A}_m^\vee = \det A \cdot \mathcal{E}. \tag{9-23}$$

Тем самым, матрицы $\mathcal{A}_m$ и $\mathcal{A}_m^\vee$ коммутируют и «почти обратны» друг другу.

Пример 9.3 (определитель пучка матриц)
Рассмотрим квадратные матрицы $A, B \in \mathrm{Mat}_n(K)$ и пару коммутирующих переменных x, y. Матрица $x \cdot A + y \cdot B$ имеет элементы в $K[x, y]$, и её определитель $\det(x \cdot A + y \cdot B) \in K[x, y]$ является однородным многочленом степени n от x и y. Покажем, что его коэффициент при $x^m y^{n-m}$ равен

$$\sum_{IJ} (-1)^{|I|+|J|} a_{IJ} b_{\overline{IJ}}, \tag{9-24}$$

где суммирование идёт по всем m-элементным подмножествам $I, J \subset \{1, 2, \ldots, n\}$. Для вывода формулы (9-24) рассмотрим два набора грассмановых линейных однородных форм

[1] обратите внимание, что буквы I и J переставились

$(\alpha_1, \alpha_2, \dots, \alpha_n) = (\xi_1, \xi_2, \dots, \xi_n) \cdot A$ и $(\beta_1, \beta_2, \dots, \beta_n) = (\xi_1, \xi_2, \dots, \xi_n) \cdot B$ от переменных $\xi_1, \xi_2, \dots, \xi_n$ и равенство

$$(x\alpha_1 + y\beta_1) \wedge (x\alpha_2 + y\beta_2) \wedge \dots \wedge (x\alpha_n + y\beta_n) = \det(xA + yB) \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n .$$

В левой части слагаемые, содержащие $x^m y^{n-m}$, возникают при выборе из каких-нибудь m перемножаемых скобок первого слагаемого, а из всех остальных скобок — второго. Если первое слагаемое выбирается в скобках с номерами $i_1, i_2, \dots, i_m$, то коэффициент при $x^m y^{n-m}$ получается равным

$$\begin{aligned}
&\operatorname{sgn}(i_1, i_2, \dots, i_m, \bar{i}_1, \bar{i}_2, \dots, \bar{i}_{n-m}) \cdot \alpha_{i_1} \wedge \alpha_{i_2} \wedge \dots \wedge \alpha_{i_k} \wedge \beta_{\bar{i}_1} \wedge \beta_{\bar{i}_2} \wedge \dots \wedge \beta_{\bar{i}_{n-m}} = \\
&\qquad = (-1)^{\frac{m(m+1)}{2}+|I|} \alpha_I \wedge \beta_{\bar{I}} = (-1)^{\frac{m(m+1)}{2}+|I|} \Big(\sum_J \xi_J a_{JI}\Big) \wedge \Big(\sum_M \xi_M b_{M\bar{I}}\Big) = \\
&\qquad = (-1)^{\frac{m(m+1)}{2}+|I|} \sum_{JM} a_{JI} \cdot b_{M\bar{I}} \cdot \xi_J \wedge \xi_M = \Big(\sum_J (-1)^{|I|+|J|} a_{JI} \cdot b_{\overline{JI}}\Big) \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n
\end{aligned}$$

Коэффициент при $a^m b^{n-m}$ в $\det(xA + yB)$ получается суммированием этих подобных слагаемых по всем наборам I из m возрастающих номеров, что и даёт формулу (9-24).

Пример 9.4 (главные миноры)
Полагая в формуле (9-24) $x = 1$, $y = t$ и $B = E$, получаем разложение

$$\begin{aligned}
\det(tE + A) &= t^n + \sum_{m=1}^{n} t^{n-m} \cdot \sum_{\#I=m} a_{II} = \\
&= t^n + t^{n-1} \cdot \sum_i a_{ii} + t^{n-1} \cdot \sum_{i<j} (a_{ii}a_{jj} - a_{ij}a_{ji}) + \dots + t \cdot \sum_i a_{\bar{i}\bar{i}} + \det A ,
\end{aligned}$$

в котором коэффициент при t^{n-m} равен сумме определителей всех $m \times m$ подматриц матрицы A, главная диагональ[1] которых содержится в главной диагонали матрицы A. Они называются *главными минорами* m-того порядка. Коэффициент при t^{n-1}, равный сумме элементов, стоящих на главной диагонали матрицы A, называется *следом* матрицы A и обозначается

$$\operatorname{tr}(A) \stackrel{\text{def}}{=} \sum_{i=1}^{n} a_{ii} . \tag{9-25}$$

Упражнение 9.8. Покажите, что $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$ и $\operatorname{tr}(AB) = \sum_{ij} a_{ij} b_{ji} = \operatorname{tr}(BA)$.

Упражнение 9.9. Убедитесь, что в обозначениях из формулы (9-22) соотношение (9-24) означает равенство $\det(xA + yB) = \sum_m \operatorname{tr}\left(\mathcal{A}_m \cdot \mathcal{B}^{\vee}{}_m\right) \cdot x^m y^{n-m}$.

[1] напомню, что *главной* называется диагональ, идущая из левого верхнего угла в правый нижний и состоящая из элементов a_{ii}

9.6. Присоединённая матрица. При $m = 1$ в соотношениях Лапласа (9-22) наборы $I = (i)$ и $J = (j)$ содержат по одному индексу и миноры $a_{IJ} = a_{ij}$ превращаются в матричные элементы, а матрица $\mathcal{A}_1$ — в матрицу A. Матрица $\mathcal{A}_1^\vee$, транспонированная к матрице из алгебраических дополнений до элементов матрицы A, состоит из элементов

$$a_{ij}^\vee \stackrel{\text{def}}{=} (-1)^{i+j} a_{\overline{ji}}\,. \tag{9-26}$$

Она называется *присоединённой* к A матрицей и обозначается $A^\vee$. Минор $a_{\overline{ji}}$ равен определителю матрицы, которая получается из A вычёркиванием j-й строки и i-го столбца. Его часто обозначают A_{ji}. Матричные соотношения (9-22) и (9-23) при $m = 1$ имеют вид

$$A \cdot A^\vee = A^\vee \cdot A = \det(A) \cdot E = \begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix}.$$

Если $\det A \in K$ обратим, мы получаем явную формулу для обратной матрицы:

$$A^{-1} = \frac{1}{\det A} A^\vee\,.$$

Например, для 2×2-матрицы определителя 1

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

а для 3×3-матрицы определителя 1

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}^{-1} = \begin{pmatrix} (a_{22}a_{33} - a_{23}a_{32}) & -(a_{12}a_{33} - a_{13}a_{31}) & (a_{12}a_{23} - a_{13}a_{22}) \\ -(a_{21}a_{33} - a_{23}a_{31}) & (a_{11}a_{33} - a_{13}a_{31}) & -(a_{11}a_{23} - a_{13}a_{21}) \\ (a_{21}a_{32} - a_{22}a_{31}) & -(a_{11}a_{32} - a_{12}a_{32}) & (a_{11}a_{22} - a_{12}a_{21}) \end{pmatrix}$$

(в общем случае все элементы матриц в правых частях надо поделить на $\det A$).

Предложение 9.3 (критерий обратимости матрицы)
Над произвольным коммутативным кольцом K с единицей матрица $A \in \mathrm{Mat}_n(K)$ обратима тогда и только тогда, когда обратим её определитель $\det A \in K$, и в этом случае $A^{-1} = A^\vee / \det A$.

Доказательство. Если A обратима, то $AA^{-1} = E$, откуда $\det(A)\det(A^{-1}) = 1$. Наоборот, если $\det A$ обратим, то по предыдущему $AA^\vee / \det A = E$. □

Предложение 9.4
Пусть модуль V над произвольным коммутативным кольцом K линейно порождается векторами $(w_1, w_2, \dots, w_m)$ и линейный оператор $F : V \to V$ действует на них по правилу $\left(Fw_1, Fw_2, \dots, Fw_n\right) = (w_1, w_2, \dots, w_m) \cdot C$, где $C \in \mathrm{Mat}_m(K)$. Тогда образ оператора умножения на $\det C : v \mapsto v \cdot \det C$ содержится в образе оператора F.

Доказательство. Оператор умножения на $\det C$ действует на порождающие по правилу

$$(w_1, w_2, \dots, w_m) \mapsto (w_1, w_2, \dots, w_m) \cdot \det C \cdot E = (w_1, w_2, \dots, w_m) \cdot C \cdot C^\vee\,,$$

где E — единичная матрица, а $C^\vee$ — матрица, присоединённая к C. Столбцы матрицы $C \cdot C^\vee$ являются линейными комбинациями столбцов матрицы C и, тем самым, лежат в образе F. □

Предложение 9.5 (правило Крамера 1)
Над произвольным коммутативным кольцом K с единицей набор векторов $(v_1, v_2, \dots, v_n)$ координатного модуля K^n тогда и только тогда образует базис в K^n, когда определитель $\det(v_1, v_2, \dots, v_n) = \det C_{ev}$ матрицы их координат в стандартном базисе e обратим в K, и в этом случае коэффициенты разложения $w = x_1v_1 + x_2v_2 + \cdots + x_nv_n$ произвольного вектора $w \in K^n$ по базису $(v_1, v_2, \dots, v_n)$ вычисляются по *правилу Крамера*:

$$x_i = \frac{\det\left(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n\right)}{\det(v_1, v_2, \dots, v_n)}. \tag{9-27}$$

Доказательство. Если векторы $v_1, v_2, \dots, v_n$ образуют базис, то $e = vC_{ve}$ для некоторой матрицы $C_{ve} \in \mathrm{Mat}_n(K)$. Тогда $C_{ev}C_{ve} = E$ и $\det C_{ev} \det C_{ve} = 1$, так что $\det C_{ev}$ обратим.

Наоборот, если $\det C_{ev}$ обратим, то векторы v линейно независимы, а матрица C_{ev} обратима по предл. 9.3. Умножая соотношение $v = e \cdot C_{ev}$ справа на C_{ev}^{-1}, получаем линейное выражение стандартного базиса через векторы v: $e = v \cdot C_{ev}^{-1}$. Поэтому набор v линейно порождает K^n и, значит, является базисом[1]. Если $w = x_1v_1 + x_2v_2 + \cdots + x_nv_n$, то

$$\det\left(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n\right) = \det\Big(v_1, \dots, v_{i-1}, \sum_\nu x_\nu v_\nu, v_{i+1}, \dots, v_n\Big) =$$
$$= \sum_\nu x_\nu \cdot \det\left(v_1, \dots, v_{i-1}, v_\nu, v_{i+1}, \dots, v_n\right) = x_i \cdot \det\left(v_1, \dots, v_{i-1}, v_i, v_{i+1}, \dots, v_n\right),$$

что влечёт за собой правило Крамера. □

Пример 9.5 (разложения определителя по строке и столбцу)
При $m = 1$ первое из соотношений Лапласа (9-19) имеет вид

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} a_{\overline{ij}} = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} A_{ij} \tag{9-28}$$

и называется *разложением определителя по j-тому столбцу*, а его транспонированный вариант (9-21) имеет вид

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} a_{\overline{ij}} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij} \tag{9-29}$$

называется *разложением определителя по i-той строке*. Например, разложение определителя 3×3 по первому столбцу таково:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}\left(a_{22}a_{33} - a_{23}a_{32}\right) - a_{21}\left(a_{12}a_{33} - a_{13}a_{32}\right) + a_{31}\left(a_{12}a_{23} - a_{13}a_{22}\right)$$

[1] см. зам. 6.3. на стр. 89

Пример 9.6 (правило Крамера 2)
Рассмотрим систему из n линейных уравнений на $n+1$ неизвестных

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{20}x_0 + a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{n0}x_1 + a_{n1}x_1 + \cdots + a_{nn}x_n = 0 \end{cases} \tag{9-30}$$

и построим по матрице $A = \left(a_{ij}\right)$ её коэффициентов вектор $\alpha = (A_0, A_1, \ldots, A_n) \in K^{n+1}$, i-тая координата которого равна умноженному на $(-1)^i$ определителю $n \times n$-матрицы, которая получается из $n \times (n+1)$-матрицы A выкидыванием i-того столбца:

$$A_i = (-1)^i \det \begin{pmatrix} a_{1,0} & \cdots & a_{1,i-1} & a_{1,i+1} & \cdots & a_{1,n} \\ a_{2,0} & \cdots & a_{2,i-1} & a_{2,i+1} & \cdots & a_{2,n} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ a_{n,0} & \cdots & a_{n,i-1} & a_{n,i+1} & \cdots & a_{n,n} \end{pmatrix} \tag{9-31}$$

Из формулы для разложения определителя по строке вытекает, что $x = \alpha$ является решением системы (9-30). В самом деле, дописывая к матрице A сверху ещё один экземпляр её i-той строки, мы получим квадратную матрицу размера $(n+1) \times (n+1)$ с нулевым определителем. Раскладывая последний по верхней строке, приходим к равенству

$$a_{i0}A_0 + a_{i1}A_1 + \cdots + a_{in}A_n = 0\,.$$

Упражнение 9.10. Проверьте, что если $K = \Bbbk$ — поле, то уравнения (9-30) линейно независимы тогда и только тогда, когда $\alpha \neq 0$, и в этом случае решения системы (9-30) образуют в $\Bbbk^{n+1}$ одномерное векторное подпространство, порождённое вектором α.

Например, в $\Bbbk^3$ пересечение двух не совпадающих плоскостей

$$\begin{cases} a_1x + a_2y + a_3z = 0 \\ b_1x + b_2y + b_3z = 0 \end{cases}$$

является прямой с направляющим вектором $\left(a_2b_3 - a_3b_2\,,\ -a_1b_3 + a_3b_1\,,\ a_1b_2 - a_2b_1\right)$.

§10. Конечно порождённые модули над кольцами главных идеалов

10.1. Модули над коммутативными кольцами. Напомним, что абелева группа M называется *унитальным модулем* над коммутативным кольцом K с единицей, если задана операция $K \times M \to M$, обладающая всеми свойствами умножения векторов на числа, перечисленными в опр. 6.1 на стр. 83. Всюду далее, если специально не оговаривается противное, мы рассматриваем именно такие модули.

Абелева подгруппа $N \subset M$ в K-модуле M называется K-подмодулем, если она выдерживают умножение на элементы кольца, т. е. для всех $a \in N$ и $\lambda \in K$ $\lambda a \in N$. Подмодуль называется *собственным*, если он отличен от нуля и от всего модуля.

Фактор модуль M/N по подмодулю $N \subset M$ определяется как множество смежных классов $[m]_N = m \,(\mathrm{mod}\, N) = m + N = \{m' \in M \mid m' - m \in N\}$, которые являются классами эквивалентности по отношению $m \underset{N}{\sim} m'$, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами:

$$[m_1] + [m_2] = [m_1 + m_2] \quad \text{и} \quad \lambda[m] = [\lambda m].$$

Упражнение 10.1. Проверьте, что эти операции корректно определены и удовлетворяют аксиомам модуля.

Гомоморфизм, или *K-линейное отображение* между K-модулями M и M' это гомоморфизм абелевых групп $M \to M'$, перестановочный с умножением на элементы кольца:

$$\varphi(\lambda v) = \lambda\varphi(v) \qquad \forall\, \lambda \in K \ ,\ \forall\, v, w \in M\,.$$

Таким образом, гомоморфизм модулей обладает всеми свойствами гомоморфизма абелевых групп. Например, $\varphi(0) = 0$, $\varphi(v - w) = \varphi(v) - \varphi(w)$ и т. п.. Инъективность K-линейного отображения φ равносильна тому, что φ имеет нулевое *ядро* $\ker(\varphi) = \{\, a \in M_1 \mid \varphi(a) = 0 \,\}$.

Упражнение 10.2. Убедитесь, что ядро и образ произвольного гомоморфизма K-модулей $\varphi : M_1 \to M_2$ являются K-подмодулями в M_1 и M_2 соответственно, и постройте канонический изоморфизм $M_1/\ker(\varphi) \xrightarrow{\sim} \mathrm{im}(\varphi)$.

K-линейные отображения $M \to N$ образуют K-модуль, который обозначается $\mathrm{Hom}(M, N)$ или $\mathrm{Hom}_K(M, N)$, если важно указать, над каким именно кольцом K рассматриваются модули.

10.1.1. Образующие и соотношения. Понятия линейной зависимости, линейной оболочки и линейных порождающих сохраняют смысл в любом модуле M. Набор векторов $\{e_\nu\}$ называется *базисом* модуля M, если каждый вектор $w \in M$ допускает единственное представление в виде конечной линейной комбинации $w = \sum \lambda_i e_{\nu_i}$.

Упражнение 10.3. Докажите, что набор векторов тогда и только тогда является базисом, когда он линейно независим и линейно порождает модуль.

Модуль, обладающий базисом, называется *свободным*. Примером свободного модуля является координатный модуль K^n. Число элементов в базисе свободного модуля M называется *рангом* этого модуля и обозначается $\mathrm{rk}\, M$. В теор. 10.2 на стр. 151 ниже мы покажем, что ранг свободного модуля не зависит от выбора базиса.

С каждым набором векторов $w_1, w_2, \dots, w_m$, линейно порождающих M, связан сюръективный гомоморфизм координатного модуля ранга m на модуль M, переводящий стандартный базисный вектор $e_i \in K^m$ в образующую w_i:

$$\pi_w : K^m \twoheadrightarrow M, \quad e_i \mapsto w_i, \tag{10-1}$$

Ядро $R_w \stackrel{\text{def}}{=} \ker \pi_w$ этого эпиморфизма называется *модулем соотношений* между образующими w_i, поскольку векторы $(\lambda_1, \lambda_2, \dots, \lambda_m) \in R_w$ суть коэффициенты всевозможных линейных зависимостей между векторами w_i:

$$\sum \lambda_i w_i = 0 \iff (\lambda_1, \lambda_2, \dots, \lambda_m) \in R_w .$$

Таким образом, любой конечно-порождённый K-модуль M представляется в виде

$$M = K^m / R . \tag{10-2}$$

Это представление называется *заданием M образующими и соотношениями*. Если кольцо K не является полем, наиболее интересные K-модули, как правило, *не свободны*, и любая их система образующих оказывается связанной линейными соотношениями с необратимыми коэффициентами.

Пример 10.1 (идеалы)
Каждое кольцо K является модулем над самим собой. Его подмодули $I \subset K$ — это в точности идеалы кольца K. Если идеал не является главным, то любое множество его образующих содержит хотя бы два элемента и, тем самым, линейно зависимо, поскольку любые два элемента $a, b \in K$ линейно зависимы над K: $a \cdot b - b \cdot a = 0$. Например, идеал $I = (x, y) \subset \mathbb{Q}[x, y]$, рассматриваемый как модуль над кольцом $K = \mathbb{Q}[x, y]$, порождается двумя векторами x и y. Эпиморфизм (10-1) имеет вид

$$\pi_{(x,y)} : K^2 \twoheadrightarrow I, \quad (f, g) \mapsto xf + yg .$$

Его ядро $R_{(x,y)} = \ker \pi_{(x,y)}$ представляет собою свободный модуль ранга 1 с базисным вектором $(y, -x)$. В самом деле, из факториальности кольца $\mathbb{Q}[x, y]$ вытекает, что равенство $xf = -yg$ возможно только при $f = yh$, $g = -xh$ для некоторого $h \in \mathbb{Q}[x, y]$. Тем самым, любое K-линейное соотношение между x и y пропорционально соотношению с коэффициентами $(y, -x)$.

Пример 10.2 (абелевы группы)
Всякая абелева группа A имеет каноническую структуру модуля над кольцом целых чисел $\mathbb{Z}$, заданную правилом $n \cdot a \stackrel{\text{def}}{=} \operatorname{sgn}(n) \cdot (\underbrace{a + a + \dots + a}_{|n| \text{ слагаемых}})$, где $\operatorname{sgn}(n) = n/|n| = \pm 1$.

Упражнение 10.4. Проверьте выполнение аксиом $\mathbb{Z}$-модуля.

Например, аддитивная группа вычетов $M = \mathbb{Z}/(k)$ может рассматриваться как $\mathbb{Z}$-модуль с операцией $n \cdot [m]_k \stackrel{\text{def}}{=} [nm]_k$, где мы обозначаем через $[m]_k = m \pmod k$ класс числа m по модулю k. Модуль M порождается одним элементом $[1]_k$, который удовлетворяет соотношению $k \cdot [1]_k = 0$, т. е. линейно зависим и, в частности, не является базисом. Обратите внимание, что запись $M = \mathbb{Z}/(k)$ есть ни что иное как представление (10-2) модуля M одной образующей и модулем соотношений $R = (k) \subset \mathbb{Z}$, который является

свободным $\mathbb{Z}$-модулем с базисным элементом k. Отметим, что соотношение $k \cdot [1]_k = 0$ влечёт за собой отсутствие ненулевых гомоморфизмов $\mathbb{Z}/(k) \to \mathbb{Z}$. В самом деле, для такого гомоморфизма φ в кольце $\mathbb{Z}$ выполняется равенство $k \cdot \varphi([1]_k) = \varphi(k \cdot [1]_k) = \varphi(0) = 0$, откуда $\varphi([1]_k) = 0$, поскольку в $\mathbb{Z}$ нет делителей нуля. Но тогда для всех m

$$\varphi\left([m]_k\right) = \varphi\left(m \cdot [1]_k\right) = m \cdot \varphi\left([1]_k\right) = 0\,.$$

Упражнение 10.5. Покажите, что класс $[n]_k$ порождает $\mathbb{Z}$-модуль $\mathbb{Z}/(k)$ тогда и только тогда, когда n взаимно просто с k.

10.1.2. Продолжение по линейности. Пусть K-модуль M линейно порождается векторами $w_1, w_2, \ldots, w_m$. Тогда любой K-линейный гомоморфизм $F : M \to N$ однозначно определяется своими значениями $u_i = \varphi(w_i)$ на этих образующих: образ произвольного вектора $v = \sum x_i w_i \in M$ будет равен

$$Fv = F\Big(\sum x_i w_i\Big) = \sum x_i u_i\,. \tag{10-3}$$

Однако, если мы захотим *определить* гомоморфизм $F : M \to N$ произвольным образом указав в модуле N элементы $u_i = F(w_i)$ и по линейности продолжив F на все остальные векторы $v \in M$ формулой (10-3), то такое определение может оказаться некорректным из-за того, что линейное выражение $v = \sum x_i w_i$ через образующие *не единственно*.

Лемма 10.1
Для того, чтобы правило $w_i \mapsto u_i$ корректно продолжалось формулой (10-3) до гомоморфизма модулей $M \to N$, необходимо и достаточно, чтобы каждое линейное соотношение $\lambda \in R_w$ между образующими w_i в модуле M выполнялось также и между векторами u_i в модуле N: $\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_m w_m = 0 \;\Rightarrow\; \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_m u_m = 0$. Иначе говоря, если $M = K^m/R$, то $\operatorname{Hom}(M, N) \simeq \{f : K^m \to N \mid f(R) = 0\}$.

Доказательство. Необходимость: если $\sum \lambda_i w_i = 0$, то $\sum \lambda_i u_i = F\big(\sum \lambda_i w_i\big) = F(0) = 0$. Наоборот, пусть каждое линейное соотношение между w_i выполняются и между u_i. Наличие двух разложений $v = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n = y_1 w_1 + y_2 w_2 + \cdots + y_n w_n$ влечёт соотношение $\sum (x_i - y_i) \cdot w_i = 0$, а значит, и соотношение $\sum (x_i - y_i) \cdot u_i = 0$. Тогда $x_1 u_1 + x_2 u_2 + \cdots + x_n u_n = y_1 u_1 + y_2 u_2 + \cdots + y_n u_n$ в N, т. е. Fv не зависит от выбора разложения вектора v по образующим w_i. □

Лемма 10.2
Набор векторов $\mathcal{E} = \{e_i\} \subset M$ тогда и только тогда является базисом K-модуля M, когда любое отображение множеств $\varphi : \mathcal{E} \to N$ в произвольный K-модуль N единственным способом продолжается до K-линейного гомоморфизма модулей $F_\varphi : M \to N$.

Доказательство. Необходимость следует из предыдущей леммы. Для доказательства достаточности образуем множество $\mathcal{E}' \simeq \mathcal{E}$, состоящее из формальных символов e_i', взаимно однозначно соответствующих векторам $e_i \in \mathcal{E}$, и рассмотрим свободный K-модуль N с базисом $\mathcal{E}'$. Пусть отображение множеств $\mathcal{E} \to N$, переводящее e_i в e_i', однозначно продолжается до гомоморфизма модулей $F : M \to N$. По предыдущей лемме отображение множеств $\mathcal{E}' \to M$, переводящее e_i' в e_i, также однозначно продолжается до гомоморфизма модулей $G : N \to M$. Поскольку и композиция $GF : M \to M$, и тождественный

гомоморфизм $\mathrm{Id}_M : M \to M$ продолжают тавтологическое вложение $\mathcal{E} \subset M$ до K-линейного гомоморфизма $M \to M$, выполняется равенство $\psi\varphi = \mathrm{Id}_M$. По той же самой причине $FG = \mathrm{Id}_N$. Тем самым, F и G суть обратные друг другу изоморфизмы. □

Упражнение 10.6. Убедитесь, что $\mathrm{Hom}(K^m, N) \simeq N^{\oplus m}$ (прямая сумма m копий N).

10.1.3. Матрицы гомоморфизмов. Если векторы $w_1, w_2, \dots, w_m$ порождают K-модуль M, а векторы $u_1, u_2, \dots, u_n$ порождают K-модуль N, то каждому K-линейному гомоморфизму $F : M \to N$ можно сопоставить матрицу $F_{uw} \in \mathrm{Mat}_{n\times m}(K)$, в j-том столбце которой стоят коэффициенты какого-нибудь линейного выражения вектора Fw_j через образующие u_i, так что $\big(Fw_1, Fw_2, \dots, Fw_m\big) = (u_1, u_2, \dots, u_n) \cdot F_{uw}$. Если образующие u_i линейно зависимы, такое матричное представление не единственно, а если линейно зависимы образующие w_j, то не всякая матрица является матрицей гомоморфизма $F : M \to N$. Тем не менее, если гомоморфизм $F : M \to N$ корректно определён тем или иным способом, то для любого его матричного представления F_{uw} и любого линейного выражения $v = \sum w_j x_j$ произвольного вектора $v \in M$ через образующие w_j произведение $F_{uw}x$ матрицы F_{uw} на столбец коэффициентов x даст столбец коэффициентов одного из разложений вектора Fv по образующим u_i.

10.1.4. Тождество Гамильтона – Кэли. Пусть K — произвольное кольцо с единицей, $A \in \mathrm{Mat}_n(K)$ — любая квадратная матрица, и $f(t) = f_0 + f_1 t + \cdots + f_m t^m$ — любой многочлен с коэффициентами из K. Обозначим через $f(A) \in \mathrm{Mat}_n(K)$ результат *вычисления*[1] многочлена f на элементе A в алгебре $\mathrm{Mat}_n(K)$:

$$f(A) \stackrel{\text{def}}{=} f_0 E + f_1 A + f_2 A^2 + \cdots + f_m A^m \in \mathrm{Mat}_n(K)\,.$$

Наделим координатный K-модуль K^n, векторы которого будем записывать в виде столбцов, структурой модуля над кольцом $K[t]$, полагая $f(t)\cdot v$ равным произведению столбца v на матрицу $f(A)$:

$$f(t)\cdot v \stackrel{\text{def}}{=} f(A)\,v = f_0 v + f_1 Av + f_2 A^2 v + \cdots + f_m A^m v\,. \tag{10-4}$$

Упражнение 10.7. Проверьте выполнения аксиом $K[t]$-модуля для K^n.

Векторы $e_1, e_2, \dots, e_n$ стандартного базиса модуля K^n над K линейно порождают K^n над $K[t]$, однако над $K[t]$ они линейно зависимы. Поэтому $K[t]$-линейное отображение умножения на t: $v \mapsto tv$ имеет в этой системе порождающих два различных матричных представления: $t\cdot E$ и A, а нулевой гомоморфизм, отображающий все векторы в нуль, можно задать ненулевой матрицей $tE - A$. По предл. 9.4 умножение на $\det(tE - A)$ отображает любой вектор K^n в нуль. В силу определения (10-4) оператор умножения на $\det(tE - A)$, рассматриваемый как K-линейный оператор $K^n \to K^n$, задаётся в стандартном базисе матрицей $\chi_A(A)$ — результатом подстановки матрицы A вместо переменной t в *характеристический многочлен*

$$\chi_A(t) \stackrel{\text{def}}{=} \det(tE - A) \in K[t]\,.$$

Поскольку K^n свободен над K, K-линейные эндоморфизмы $K^n \to K^n$ однозначно представляются своими матрицами в стандартном базисе. Поэтому матрица $\chi_A(A) \in \mathrm{Mat}_n(K)$ это нулевая матрица. Нами установлена

[1] см. n° 8.1.2 на стр. 118

Теорема 10.1 (тождество Гамильтона – Кэли)
Над любым коммутативным кольцом K с единицей при подстановке матрицы $A \in \mathrm{Mat}_n(K)$ вместо переменной t в характеристический многочлен $\chi_A(t) = \det(tE - A) \in K[t]$ получается нулевая матрица $\chi_A(t) = \det(tE - A) \in \mathrm{Mat}_n(K)$. □

Пример 10.3
Всякая 2×2 матрица A удовлетворяет квадратному уравнению[1] $t^2 - \mathrm{tr}(A) \cdot t + \det(A) = 0$, а всякая 3×3 матрица — кубическому уравнению $t^3 - \mathrm{tr}(A) \cdot t^2 + \sigma_2(A) \cdot t - \det(A) = 0$, где

$$\sigma_2 \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \left(a_{11}a_{22} - a_{12}a_{21}\right) + \left(a_{11}a_{33} - a_{13}a_{31}\right) + \left(a_{22}a_{33} - a_{23}a_{32}\right) .$$

10.1.5. Кручение. Пусть в кольце K нет делителей нуля. Элемент m из K-модуля M называется *элементом кручения*, если $\lambda m = 0$ для некоторого ненулевого $\lambda \in K$.

Упражнение 10.8. Убедитесь, что элементы кручения образуют в M подмодуль.

Этот подмодуль называется *подмодулем кручения* и обозначается

$$\mathrm{Tors}\, M \stackrel{\text{def}}{=} \{ m \in M \mid \exists\, \lambda \neq 0 \,:\, \lambda m = 0 \} .$$

Если $\mathrm{Tors}\, M = 0$, то говорят, что M *без кручения*. Например, любой идеал кольца K и любой свободный K-модуль не имеют кручения.

Упражнение 10.9. Покажите, что любой гомоморфизм $\varphi : M \to N$ в свободный от кручения модуль N переводит $\mathrm{Tors}(M)$ в нуль.

Если $\mathrm{Tors}\, M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K-модулем кручения.

10.1.6. Факторизация модуля по идеалу кольца. Для любого идеала $I \subset K$ и произвольного K-модуля M обозначим через $IM \subset M$ подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I:

$$IM = \{ x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in I\,,\ a_i \in M \} .$$

Упражнение 10.10. Проверьте, что IM действительно является K-подмодулем в M.

Фактор модуль M/IM обладает канонической структурой модуля над фактор кольцом K/I, которая корректно задаётся правилом $[\lambda]_I \cdot [w]_{[IM]} = [\lambda w]_{[IM]}$, где $[\lambda]_I = \lambda \,(\mathrm{mod}\ I)$ и $[a]_{[IM]} = a \,(\mathrm{mod}\ [IM])$обозначают классы эквивалентности элементов $\lambda \in K$ и $w \in M$.

Упражнение 10.11. Убедитесь, что это определение корректно.

10.1.7. Прямые разложения. Прямые суммы и прямые произведения модулей определяются как прямые суммы и прямые произведения соответствующих абелевых групп и наделяются покомпонентной модульной структурой дословно также, как и векторные пространства (см. n° 6.4.4 на стр. 96).

Упражнение 10.12. Покажите, что прямая сумма свободных модулей с базисами $\mathcal{E}_1$ и $\mathcal{E}_2$ ($\mathcal{E}_1$ и $\mathcal{E}_2$ обозначают множества базисных векторов) является свободным модулем с базисом $\mathcal{E}_1 \sqcup \mathcal{E}_2$.

[1] ср. с форм. (8-4) на стр. 121

Если набор подмодулей $N_1, N_2, \dots, N_s \subset M$ таков, что гомоморфизм сложения

$$N_1 \oplus N_2 \oplus \cdots \oplus N_s \to M\,, \quad (u_1, u_2, \dots, u_s) \mapsto u_1 + u_2 + \cdots + u_s\,, \tag{10-5}$$

является изоморфизмом, то говорят, что модуль M является *прямой суммой* этих подмодулей и пишут $M = \bigoplus\limits_i N_i$. Биективность гомоморфизма (10-5) означает, что каждый вектор $w \in M$ имеет единственное разложение $w = u_1 + u_2 + \cdots + u_s$, в котором $u_i \in N_i$. Например, свободный K-модуль с базисом $e_1, e_2, \dots, e_n$ является прямой суммой свободных подмодулей ранга 1, порождённых базисными векторами: $K^n = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_n$.

Лемма 10.3
Для того чтобы модуль M распадался в прямую сумму собственных подмодулей $L, N \subset M$ необходимо и достаточно, чтобы L и N линейно порождали M и $L \cap N = 0$.

Доказательство. Сюръективность гомоморфизма сложения $\sigma : L \oplus N \to M$, $(a, b) \mapsto a + b$, равносильна тому, что L и N порождают M, а тривиальность его ядра — условию $L \cap N = 0$, ибо $(a, b) \in \ker \sigma \Rightarrow a = -b \in L \cap N$, и наоборот, $a \in L \cap N \Rightarrow (a, -a) \in \ker \sigma$. □

Упражнение 10.13. Пусть модуль M является прямой суммой $M = L \oplus N$ подмодулей $L, N \subset M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

10.1.8. Разложимость и полупростота. Модули, не представимые в виде прямой суммы двух своих собственных подмодулей называются *неразложимыми*.

Например, $\mathbb{Z}$-модуль $\mathbb{Z}$ неразложим, т. к. всякий собственный подмодуль $I \subset \mathbb{Z}$ — это главный идеал $I = (d)$, и из наличия разложения $\mathbb{Z} = (d) \oplus N$ вытекает, что в $\mathbb{Z}$ есть подмодуль N, изоморфный по упр. 10.13 модулю $\mathbb{Z}/(d)$. Но это невозможно, поскольку в $\mathbb{Z}$ нет кручения.

Этот пример показывает, что над кольцом K, содержащим необратимые элементы, у подмодуля $N \subset M$ может не оказаться *дополнительного подмодуля* $L \subset M$, такого что $M = L \oplus N$, как это имело место для векторных пространств над полем.

Упражнение 10.14. Пусть $M = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ и $N \subset M$ — подмодуль, порождённый векторами $(2, 1)$ и $(1, 2)$. Покажите, что $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, и не существует подмодуля $L \subset M$, такого что $M = L \oplus N$.

Модуль M называется *полупростым*, если любой его собственный подмодуль $N \subset M$ отщепляется прямым слагаемым, т. е. обладает дополнительным подмодулем $L \subset M$, таким что $M = L \oplus N$. Например, $\mathbb{Z}$-модуль $M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) \oplus \cdots \oplus \mathbb{Z}/(p) = \mathbb{Z}^n/p\mathbb{Z}^n$, где $p \in \mathbb{N}$ — простое, полупрост, поскольку одновременно является векторным пространством над полем $\mathbb{F}_p = \mathbb{Z}/(p)$, а всякий $\mathbb{Z}$-подмодуль $N \subset M$ одновременно является векторным подпространством, и дополнительное к нему векторное подпространство является также и дополнительным $\mathbb{Z}$-подмодулем.

Упражнение 10.15. Убедитесь, что для любого разложения $M = M_1 \oplus M_2 \oplus \cdots \oplus M_m$ и любого идеала $I \subset K$ выполняются равенства $IM = IM_1 \oplus IM_2 \oplus \cdots \oplus IM_m$ и

$$M/IM = (M_1/IM_1) \oplus (M_2/IM_2) \oplus \cdots \oplus (M_m/IM_m)\,.$$

В частности, результатом факторизации свободного K-модуля $M = K^n$ по идеалу $I \subset K$ является свободный K/I-модуль $M/IM = (K/I)^n$ того же ранга.

Теорема 10.2 (о ранге свободного модуля)
Все базисы свободного модуля M над произвольным коммутативным кольцом K с единицей равномощны.

Доказательство. Выберем произвольный максимальный идеал $\mathfrak{m} \subset K$. Фактор $M/\mathfrak{m}M$ представляет собою векторное пространство над полем $\Bbbk = K/\mathfrak{m}$. Если $e_1, e_2, \dots, e_m$ образуют базис K-модуля M, то $M = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_m$ и $\mathfrak{m}M = \mathfrak{m}e_1 \oplus \mathfrak{m}e_2 \oplus \cdots \oplus \mathfrak{m}e_m$, а $M/\mathfrak{m}M = \Bbbk e_1 \oplus \Bbbk e_2 \oplus \cdots \oplus \Bbbk e_m \simeq \Bbbk^m$. Таким образом, $m = \dim_{\Bbbk}(M/\mathfrak{m}M)$ не зависит от выбора базиса[1]. □

Замечание 10.1. Согласно зам. 6.4. на стр. 91, доказанная выше теор. 10.2 верна и для свободных модулей бесконечного ранга.

10.2. Теорема об инвариантных множителях. Начиная с этого места и до конца параграфа мы обозначаем через K произвольное кольцо главных идеалов и по умолчанию предполагаем, что все рассматриваемые нами K-модули конечно порождены. Договоримся также понимать под свободным модулем ранга 0 нулевой модуль.

Лемма 10.4
Всякий подмодуль N конечно любого порождённого модуля M над произвольным кольцом главных идеалов K тоже свободен и $\operatorname{rk} N \leqslant \operatorname{rk} M$.

Доказательство. Индукция по $m = \operatorname{rk} M$. При $m = 1$ $M \simeq K$ и подмодуль $N \subset K$ это некий главный идеал $(d) \subset K$. Если $d = 0$, то $N = 0$ свободен ранга 0. Если $d \neq 0$, то (d) свободен с базисом d, поскольку $xd = yd \Rightarrow (x-y)d = 0 \Rightarrow x = y$, т. к. в K нет делителей нуля.

Пусть теперь $m > 1$. Зафиксируем в M базис $e_1, e_2, \dots, e_m$ и будем записывать векторы $w \in M$ строчками их координат. Первые координаты $x_1(v)$ всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m-1$ с базисом $e_2, \dots, e_m$ и по индукции свободен, и $\operatorname{rk} N \leqslant (m-1)$. Если $d \neq 0$, обозначим через $v_1 \in N$ какой-нибудь вектор с первой координатой d. Тогда $N = K \cdot v_1 \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Действительно, $(K \cdot v_1) \cap N' = 0$, и любой вектор $v \in N$ представляется в виде $\lambda v_1 + w$, где $\lambda = x_1(v)/d$ и $w = v - \lambda v_1 \in N'$. Модуль Kv_1, порождённый вектором v_1, свободен ранга 1, поскольку в объемлющем свободном модуле M нет кручения. Модуль N' содержится в свободном модуле ранга $m-1$ с базисом $e_2, \dots, e_m$. По индукции N' свободен и $\operatorname{rk} M \leqslant (m-1)$. Поэтому $N = K \cdot v_1 \oplus N'$ свободен и $\operatorname{rk} N \leqslant m$. □

Теорема 10.3 (об инвариантных множителях)
Для любого подмодуля N свободного модуля M конечного ранга над кольцом главных идеалов K в модуле M существует базис $(e_1, e_2, \dots, e_m)$, такой что некоторые кратности $\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n$ первых $n \leqslant m$ базисных векторов составляют базис в N и каждый из множителей λ_i делится на все предыдущие множители λ_j с $j < i$. Набор множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ с точностью до умножения на обратимые элементы кольца не зависит от выбора такого базиса.

[1] а также от выбора максимального идеала $\mathfrak{m} \subset K$

Определение 10.1
Множители $\lambda_1, \lambda_2, \dots, \lambda_n$, о которых идёт речь в теор. 10.3, называются *инвариантными множителями* подмодуля $N \subset M$, а базисы $e_1, e_2, \dots, e_m$ в M и $\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n$ в N — *взаимными базисами* модуля M и подмодуля $N \subset M$.

Доказательство теор. 10.3 разбивается на несколько шагов, которым посвящены n° 10.2.1 – n° 10.2.4 ниже. Мы начнём с переформулировки теоремы об инвариантных множителях на языке матриц.

Предложение 10.1
Для любой матрицы $C \in \mathrm{Mat}_{m\times k}(K)$ с элементами из кольца главных идеалов K существуют такие обратимые матрицы $F \in \mathrm{GL}_m(K)$ и $G \in \mathrm{GL}_k(K)$, что матрица

$$D = FCG = \begin{pmatrix} \lambda_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & \lambda_n & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} \tag{10-6}$$

имеет $d_{ij} = 0$ при $i \neq j$, а каждый её диагональный элемент $d_{ii} = \lambda_i$ делится на все предшествующие диагональные элементы $d_{jj} = \lambda_j$ с $j < i$. При этом матрица D зависит только от матрицы C, и не зависит от выбора матриц F и G.

10.2.1. Вывод теор. 10.3 из предл. 10.1. Зафиксируем в модуле M какой-нибудь базис $w = (w_1, w_2, \dots, w_m)$, а в подмодуле $N \subset M$ — любой порождающий набор векторов $u = (u_1, u_2, \dots, u_k) = w \cdot C_{wu}$, где матрица перехода $C_{wu} \in \mathrm{Mat}_{k\times m}$ имеет в j-том столбце координаты вектора u_j в базисе w. Применим предл. 10.1 к матрице $C = C_{wu}$: пусть матрицы $F \in \mathrm{GL}_m(K)$ и $G \in \mathrm{GL}_k(K)$ таковы, что матрица $D = FC_{wu}G$ имеет диагональный вид (10-6). Так как матрица F обратима, набор векторов $e = wF^{-1}$ является базисом в M. Набор векторов $\varepsilon = uG$ выражается через этот базис как $\varepsilon = uG = wC_{wu}G = eFC_{wu}G = eD$, т. е. в наборе ε отличны от нуля в точности первые n векторов $\varepsilon_i = \lambda_i e_i$. Будучи пропорциональны базисным векторам модуля M, они линейно независимы. Исходный набор векторов u, порождающий N, линейно выражается через набор ε по формуле $u = \varepsilon G^{-1}$. Поэтому ненулевые векторы ε_i, $1 \leqslant i \leqslant n$, линейно порождают N и образуют базис. Это устанавливает существование взаимных базисов.

Если имеются два таких базиса $e' = (e'_1, e'_2, \dots, e'_m)$ и $e'' = (e''_1, e''_2, \dots, e''_m)$ модуля M, что некоторые кратности $\varepsilon'_i = \lambda'_i e'_i$ и $\varepsilon''_i = \lambda''_i e''_i$ их начальных n векторов составляют базисы подмодуля $N \subset M$ и удовлетворяют условиям делимости из предл. 10.1, то обе диагональные матрицы перехода $C_{\varepsilon''e''} = C_{\varepsilon''\varepsilon'}C_{\varepsilon'e'}C_{e'e''}$ и $C_{\varepsilon'e'} = E_n C_{\varepsilon'e'} E_m$, где E_n и E_m — единичные $n\times n$ и $m\times m$ матрицы, удовлетворяют условиям предл. 10.1 для одной и той же $n\times m$ матрицы $C = C_{\varepsilon'e'}$ и, стало быть, совпадают. Это устанавливает независимость инвариантных множителей от выбора взаимных базисов.

10.2.2. Единственность диагональной формы D в предл. 10.1. Обозначим наибольший общий делитель[1] всех $k \times k$-миноров прямоугольной матрицы C через $\Delta_k(C)$. Для

[1] напомним, что он определён с точностью до умножения на обратимые элементы кольца K

диагональной матрицы

$$D = \begin{pmatrix} \lambda_1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & \lambda_n & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix},$$

каждый диагональный элемент λ_i которой делится на все предыдущие λ_j с $j < i$,

$$\Delta_k(D) = \lambda_1\lambda_2 \dots \lambda_k,$$

откуда $\lambda_k = \Delta_k(D)/\Delta_{k-1}(D)$. Поэтому независимость диагональной матрицы D от выбора диагонализующих матриц F и G вытекает из следующего простого утверждения.

Лемма 10.5
При умножении матрицы C слева или справа на обратимую квадратную матрицу числа $\Delta_k(C)$ не меняются[1].

Доказательство. Поскольку $\Delta_k(C) = \Delta_k(C^t)$ достаточно рассмотреть только левое умножение. Пусть $F = AC$, где A обратима. Тогда каждый $k \times k$ минор матрицы F является линейной комбинацией $k \times k$ миноров матрицы C.

Упражнение 10.16. Убедитесь в этом.

Поэтому $\Delta_k(F)$ делится на $\Delta_k(C)$. Аналогично, из равенства $C = A^{-1}F$ вытекает, что $\Delta_k(C)$ делится на $\Delta_k(F)$. Тем самым, $\Delta_k(C)$ и $\Delta_k(F)$ отличаются обратимым множителем. □

10.2.3. Обобщённые элементарные преобразования. Матрицы F и G, приводящие заданную матрицу к диагональному виду, удовлетворяющему условиям предл. 10.1, мы будем строить как композиции $F = F_rF_{r-1} \dots F_1$ и $G = G_1G_2 \dots G_s$ последовательных умножений $A \mapsto F_iA$ (соотв. $A \mapsto AG_i$) на обратимые матрицы F_i (соотв. G_i), которые заменяют какие-либо две строки (соотв. столбца) a_i, a_j матрицы A их линейными комбинациями $a_i' = \alpha a_i + \beta a_j$ и $a_j' = \gamma a_i + \delta a_j$, а все остальные строки (соотв. столбцы) оставляют на месте. Для обратимости матрицы F_i (соотв. G_i), осуществляющей такое преобразование, достаточно чтобы её определитель $\alpha\delta - \beta\gamma$ был равен 1. Мы будем называть такие преобразования строк (соотв. столбцов) *обобщёнными элементарными преобразованиями.*

Лемма 10.6
Любую пару стоящих в одной строке (соотв. в одном столбце) матрицы A элементов (a_i, a_j), таких что $a_i \nmid a_j$ и $a_j \nmid a_i$, можно подходящим обобщённым элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \text{нод}(a_i, a_j)$.

Доказательство. Запишем $d = \text{нод}(a_i, a_j)$ как $d = a_ix + a_jy$, и пусть $a_i = ad$, $a_j = bd$. Тогда $-a_ib + a_jb = 0$. Поэтому $(a_i, a_j) \cdot \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = (d, 0)$ и $\begin{pmatrix} x & y \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a_i \\ a_j \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$, причём

$$\det \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = \det \begin{pmatrix} x & y \\ -b & a \end{pmatrix} = ax + by = 1$$

в силу того, что $d = xa_i + ya_j = xad + ybd = (ax + by) \cdot d$. □

[1] с точностью до умножения на обратимые элементы кольца K

10.2.4. Метод Гаусса над кольцом главных идеалов. Доказательство предл. 10.1, а с ним и теоремы об инвариантных множителях, завершает

Предложение 10.2
Любая прямоугольная матрица C над кольцом главных идеалов обобщёнными элементарными преобразованиями строк и столбцов приводится к диагональному виду (10-6), в котором каждый диагональный элемент делится на все предыдущие.

Доказательство. Сначала перестановками строк и столбцов добьёмся того, чтобы $c_{11} \neq 0$. Пусть в матрице C есть элемент a, не делящийся на c_{11}, и пусть $d = \text{нод}\,(a, c_{11})$. Тогда $(c_{11}) \subsetneq (d)$, и если мы перейдём от матрицы C к матрице C' с $c'_{11} = d$, то идеал, порождаемый левым верхним угловым элементом, строго увеличится. Покажем, что это можно сделать обобщёнными элементарными преобразованиями.

Если не делящийся на c_{11} элемент a имеется в первой строке или первом столбце, достаточно заменить пару (c_{11}, a) на $(d, 0)$ согласно лем. 10.6. Если все элементы первой строки и первого столбца делятся на c_{11}, а не делящийся на c_{11} элемент a стоит строго ниже и строго левее c_{11}, то мы сначала занулим все элементы первой строки и первого столбца за исключением самого c_{11}, добавляя ко всем столбцам подходящие кратные первого столбца, а ко всем строкам — подходящие кратные первой строки. К элементу a при этом будут добавляться числа, кратные c_{11}, и он останется не делящимся на c_{11}. Далее, прибавим ту строку, где стоит a, к первой строке — получим в ней копию элемента a. Наконец, заменим пару (c_{11}, a) на $(d, 0)$ по лем. 10.6.

Так как кольцо K нётерово, идеал (c_{11}) не может увеличиваться бесконечно долго, и после конечного числа таких переходов мы получим матрицу C, все элементы которой делятся на c_{11}. У этой матрицы мы обычными гауссовыми преобразованиями занулим все элементы первой строки и первого столбца кроме c_{11}. Все элементы подматрицы, стоящей в остальных строках и столбцах, при этом останутся делящимися на c_{11}. По индукции, эту подматрицу можно диагонализовать элементарными преобразованиями строк и столбцов. При этом первая строка и первый столбец не поменяются. □

Упражнение 10.17. Припишем к матрице $C \in \mathrm{Mat}_{m\times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ И $n \times n$ соответственно, так что получится Г-образная таблица вида $\begin{array}{|c|c|}\hline C & E \\ \hline E \\ \cline{1-1}\end{array}$, и приведём матрицу C к диагональному виду D, делая элементарные преобразования строк и столбцов сразу во всей Г-образной таблице. Покажите, что в получившейся в результате таблице $\begin{array}{|c|c|}\hline D & F \\ \hline G \\ \cline{1-1}\end{array}$ матрицы F и G таковы, что $FCG = D$.

10.2.5. Пример: абелевы подгруппы в $\mathbb{Z}^m$. По теореме об инвариантных множителях для любой абелевой подгруппы $L \subset \mathbb{Z}^m$ существует такой базис $u_1, u_2, \ldots, u_m$ в $\mathbb{Z}^m$, что некоторые кратности m_1u_1, m_2u_2, … , $m_\ell u_\ell$ первых ℓ его базисных векторов составляют базис в L. Тем самым, L тоже является свободным $\mathbb{Z}$-модулем, а фактор модуль

$$\mathbb{Z}^m / L \simeq \frac{\mathbb{Z}}{(m_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(m_\ell)} \oplus \mathbb{Z}^{m-\ell}. \tag{10-7}$$

Выясним, к примеру, как устроена подгруппа $L \subset \mathbb{Z}^3$, порождённая столбцами матрицы

$$C = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix} \tag{10-8}$$

Для этого перейдём к взаимным базисам. Заметим, что нод всех элементов матрицы (10-8) равен 3, и мы можем получить -3 в позиции $(1,4)$, прибавляя к 1-й строке учетверённую 2-ю:

$$\begin{pmatrix} 6 & -9 & 0 & -3 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}.$$

Умножаем 1-ю строку на -1 и меняем местами первый и последний столбцы

$$\begin{pmatrix} 3 & 9 & 0 & -6 \\ 9 & 15 & 18 & 30 \\ 18 & 30 & 36 & 60 \end{pmatrix}.$$

Теперь мы можем занулить левый столбец и верхнюю строку вне левого углового элемента, отнимая из 2-й и 3-й строк подходящие кратности 1-й строки, а затем из 2-го и 4-го столбцов подходящие кратности 1-го столбца

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -12 & 18 & 48 \\ 0 & -24 & 36 & 96 \end{pmatrix}$$

Зануляем 3-ю строку, отнимая из неё удвоенную 2-ю, и видим, что нод элементов второй строки можно получить, прибавляя ко 2-му столбцу 3-й

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 18 & 48 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Остаётся переставить третий столбец на место второго и занулить 3-й и 4-й столбцы, добавляя к ним подходящие кратности второго

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Таким образом, $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$.

Согласно n° 8.2, проделанные нами элементарные преобразования строк заключались в последовательном умножении слева на

$$\begin{pmatrix} 1 & -4 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -6 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix},$$

а преобразования столбцов — в последовательном умножении справа на

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & -8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & -8 \\ 0 & 1 & -2 & -8 \\ 1 & -3 & 9 & 26 \end{pmatrix}.$$

Упражнение 10.18. Проверьте эти формулы проделав предыдущие преобразования строк и столбцов с Г-образной матрицей $\begin{array}{|c|c|}\hline C & E \\ \hline E \\ \cline{1-1}\end{array}$, как в упр. 10.17.

Таким образом базис в решётке L составляют векторы $3\,u_1 = c_4$ и $6\,u_2 = c_2 + c_3 - 3\,c_4$, где c_2, c_3, c_4 суть последние три столбца исходной матрицы C, а u_1, u_2 — первые два вектора взаимного с L базиса объемлющей решётки $\mathbb{Z}^3$, образованного столбцами матрицы

$$U = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 4 & 0 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix}$$

Упражнение 10.19. Убедитесь, что следующие условия на подрешётку $L \subset \mathbb{Z}^m \subset \mathbb{Q}^m$, порождённую столбцами матрицы $C \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, эквивалентны друг другу:
а) $\mathrm{rk}\, L = m$ б) абелева группа $\mathbb{Z}^m/L$ конечна
в) $\mathbb{Q}$-линейная оболочка L в $\mathbb{Q}^m$ равна всему пространству $\mathbb{Q}^m$
г) ранг матрицы C (рассматриваемой как матрица над полем $\mathbb{Q}$) равен m

Абелевы подгруппы $L \subset \mathbb{Z}^m$, удовлетворяющие условиям упр. 10.19 называются *соизмеримыми* с $\mathbb{Z}^m$. Отметим, что для доказательства соизмеримости с $\mathbb{Z}^m$ подгруппы L, заданной как $\mathbb{Z}$-линейная оболочка столбцов некоторой целочисленной матрицы C, достаточно указать в этой матрице ненулевой минор порядка m. Для отыскания ранга L достаточно гауссовыми элементарными преобразованиями строк над полем $\mathbb{Q}$ привести матрицу C или C^t (смотря по тому, в какой из матриц меньше строк) к ступенчатому виду с рациональными элементами.

Предложение 10.3
Столбцы матрицы $C \in \mathrm{Mat}_n(\mathbb{Z})$ порождают абелеву подгруппу $L \subset \mathbb{Z}^n$, соизмеримую с $\mathbb{Z}^n$, если и только если $\det C \neq 0$. В этом случае $|\mathbb{Z}^n/L| = |\det C|$, т. е. число элементов в факторе по соизмеримой подрешётке равно объёму параллелепипеда, натянутого на любой её базис.

Доказательство. Рассмотрим в $\mathbb{Z}^m$ базис $u_1, u_2, \ldots, u_m$, некоторые кратности первых ℓ векторов которого m_1u_1, m_2u_2, … , $m_\ell u_\ell$ составляют базис в L. Как мы видели в n° 10.2.1, переход к таким базисам от стандартного базиса e модуля $\mathbb{Z}^m$ и произвольного набора u из m векторов, порождающих L, описывается матричным равенством $FCG = D$, где D — диагональная, а F и G — обратимые целочисленные $m\times m$ матрицы. Обратимость матриц F и G над кольцом $\mathbb{Z}$ равносильна равенствам $\det F = \pm 1$ и $\det G = \pm 1$. Поэтому $|\det C| = \det D$ нулевой, если $\ell < n$, и равен $m_1m_2 \ldots m_n$, если $\ell = n$. Во втором случае $\mathbb{Z}^n/L = \bigoplus\limits_i \mathbb{Z}/(m_i)$, откуда $|\det C| = |\mathbb{Z}^n/L|$. □

10.3. Теорема об элементарных делителях. Вместо упорядоченного набора инвариантных множителей $\lambda_1, \lambda_2, \ldots, \lambda_n$ иногда бывает удобнее иметь дело с неупорядоченным дизъюнктным объединением всех степеней p^μ неприводимых элементов $p \in K$, входящих в разложения чисел $\lambda_1, \lambda_2, \ldots, \lambda_n$ на неприводимые множители. Точнее, рассмотрим для каждого $i = 1, \ldots, n$ разложение $\lambda_i = p_{i1}^{m_{i1}} p_{i2}^{m_{i2}} \cdots p_{ik_i}^{m_{ik_i}}$, в котором все p_{ij} неприводимы и различны: $p_{ij} \neq p_{ik}$ при $j \neq k$. Неупорядоченное дизъюнктное[1] объединение

[1] *дизъюнктность* означает, что степень p^m, входящая в разложение ровно k инвариантных множителей λ_i, присутствует в итоговом неупорядоченном наборе в точности k раз

всех степеней $p_{ij}^{m_{ij}}$, входящих в эти разложения при $i = 1, 2, \dots, n$, называется набором *элементарных делителей* набора инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$.

Лемма 10.7
Описанная выше процедура устанавливает биекцию между упорядоченными наборами чисел[1] $\lambda_1, \lambda_2, \dots, \lambda_n \in K$, в которых $\lambda_i | \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами натуральных степеней p^μ неприводимых чисел из K, в которых разрешаются повторяющиеся элементы[2].

Доказательство. Набор инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ однозначно восстанавливается по набору элементарных делителей следующим образом. Занумеруем простые числа p, представленные в наборе элементарных делителей, в порядке (нестрогого) убывания количества имеющихся в нём степеней p^m с основанием p и разместим элементарные делители в клетки диаграммы Юнга, записав в k-тую строку все степени p_k^μ k-го числа p_k в порядке (нестрогого) убывания их показателей μ. Поскольку наибольший инвариантный множитель λ_n делится на все остальные, его разложение на простые множители содержит *все* простые элементы p_i, причём с максимальными показателями. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы образуют прочитанную справа налево последовательность инвариантных множителей. □

Пример 10.4
Набор элементарных делителей

$$\begin{array}{lllll} 3^2 & 3^2 & 3 & 3 & 3 \\ 2^3 & 2^3 & 2^2 & 2 & \\ 5 & 5 & & & \\ 7 & & & & \end{array}$$

возникает из такого набора инвариантных множителей:

$$\lambda_1 = 3\,,\ \lambda_2 = 3 \cdot 2\,,\ \lambda_3 = 3 \cdot 2^2\,,\ \lambda_4 = 3^2 \cdot 2^3 \cdot 5\,,\ \lambda_5 = 3^2 \cdot 2^3 \cdot 5 \cdot 7\,.$$

Теорема 10.4 (об элементарных делителях)
Всякий конечно порождённый модуль M над произвольным кольцом главных идеалов K изоморфен модулю вида

$$M = K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \tag{10-9}$$

где элементы $p_\nu \in K$ просты и $m_\nu \in \mathbb{N}$ (и p_ν и m_ν могут повторяться). Два модуля

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{\left(q_1^{m_1}\right)} \oplus \dots \oplus \frac{K}{\left(q_\beta^{m_\beta}\right)}$$

[1] рассматриваемых с точностью до умножения на обратимые элементы кольца K

[2] два таких набора считаются одинаковыми, если их можно привести в биективное соответствие друг с другом так, что у соответственных элементов p^μ и q^ν числа p и q отличаются обратимым множителем, а показатели степеней совпадают

изоморфны тогда и только тогда, когда $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно перенумеровать так, что $n_\nu = m_\nu$, а $p_\nu = s_\nu q_\nu$ с обратимыми $s_\nu \in K$. □

Определение 10.2
Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в правых слагаемых разложения (10-9), называется *набором элементарных делителей* модуля M.

Доказательство теор. 10.4 проводится в n° 10.3.1 – n° 10.3.4 ниже.

10.3.1. Существование разложения (10-9). Пусть $w_1, w_2, \dots, w_m$ порождают M. Тогда $M = K^m/R$, где R — ядро эпиморфизма $K^m \twoheadrightarrow M$, переводящего стандартные базисные векторы $e_i \in K^m$ в образующие $w_i \in M$, как в n° 7.4. По теор. 10.3 в K^m существует такой базис $u_1, u_2, \dots, u_m$, что некоторые кратности $\lambda_1 u_1$, $\lambda_2 u_2$, $\dots$, $\lambda_k u_k$ первых k базисных векторов составляют базис в R. Таким образом,

$$M = K^m/R = \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_k)} \oplus K^{m-k}\,.$$

Разложим каждый инвариантный множитель $\lambda = \lambda_i$ в произведение степеней различных простых: $\lambda = p_1^{m_1} p_2^{m_1} \cdots p_s^{m_s}$. По китайской теореме об остатках

$$K/(\lambda) = K/\left(p_1^{m_1}\right) \oplus K/\left(p_2^{m_2}\right) \oplus \dots \oplus K/\left(p_s^{m_s}\right)\,,$$

что и даёт разложение (10-9). Чтобы установить его единственность, мы дадим инвариантное описание всех слагаемых во внутренних терминах модуля M.

10.3.2. Отщепление кручения. Сумма $K/\left(p_1^{n_1}\right) \oplus \dots \oplus K/\left(p_\alpha^{n_\alpha}\right)$ в разложении (10-9) совпадает с подмодулем кручения $\operatorname{Tors} M = \{w \in M \mid \exists \lambda \neq 0 : \lambda w = 0\}$, а число n_0 в разложении (10-9) равно рангу свободного модуля $M/\operatorname{Tors} M$ и не зависит от выбора разложения. Из существования разложения (10-9) вытекает

Следствие 10.1
Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения (в частности, любой модуль без кручения автоматически свободен). □

10.3.3. Отщепление p-кручения. Для каждого неприводимого $p \in K$ назовём *p-кручением* в M подмодуль, образованный всеми векторами, которые аннулируются умножением на какую-нибудь степень числа p:

$$\operatorname{Tors}_p M \stackrel{\text{def}}{=} \{w \in M \mid \exists k > 0 : p^k w = 0\}\,.$$

Если простое $q \in K$ не ассоциировано с p, то класс p^k обратим в $K/\left(q^m\right)$, и гомоморфизм умножения на p^k : $K/\left(q^m\right) \to K/\left(q^m\right)$, $x \mapsto p^k x$, является изоморфизмом, в частности — не имеет ядра. Напротив, каждый модуль $K/\left(p^\ell\right)$ полностью аннулируется умножением на достаточно большую степень p. Поэтому прямая сумма всех слагаемых вида $K/\left(p^m\right)$ в разложении (10-9) совпадает с подмодулем p-кручения $\operatorname{Tors}_p M \subset M$ и тоже не зависит от выбора разложения, а из наличия разложения (10-9) вытекает

Следствие 10.2
Всякий конечно порождённый модуль кручения над кольцом главных идеалов является прямой суммой подмодулей p-кручения по всем простым $p \in K$, для которых p-кручение ненулевое. □

Упражнение 10.20. Обозначим через $\varphi_n : K/(p^m) \to K/(p^m)$ гомоморфизм умножения на $p^n : x \mapsto p^n x$. Покажите, что $\varphi_n = 0$ при $n \geqslant m$, и $\ker \varphi_n = \operatorname{im} \varphi_{m-n} \simeq K/(p^n)$ при $0 < n < m$, причём $\ker \varphi_n \supset \ker \varphi_{n-1}$ и фактор $\ker \varphi_n / \ker \varphi_{n-1}$ нулевой при $n > m$ и изорфен $K/(p)$ при $1 \leqslant n \leqslant m$.

10.3.4. Инвариантность показателей p-кручения. Для завершения доказательства теор. 10.4 остаётся проверить, что (нестрого) убывающий набор $\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_k$ показателей степеней простого числа $p \in K$ в разложении

$$M = \frac{K}{(p^{\nu_1})} \oplus \cdots \oplus \frac{K}{(p^{\nu_k})}$$

однозначно определяется модулем M. Рассмотрим диаграмму Юнга ν со строками длины $\nu_1, \nu_2, \ldots, \nu_k$ и обозначим через $\varphi_i : M \to M$ гомоморфизм умножения на $p^i : v \mapsto p^i v$. Согласно упр. 10.20 для каждого $i = 1, 2, \ldots$ фактор модуль $\ker \varphi_i / \ker \varphi_{i-1}$ является прямой суммой одинаковых слагаемых $K/(p)$ в количестве, равном числу тех строк диаграммы ν, длина которых не меньше i, т. е. высоте i-того столбца диаграммы ν.

Упражнение 10.21. Убедитесь, что на фактор модуле $\ker \varphi_i / \ker \varphi_{i-1}$ имеется корректно определённая структура $K/(p)$-модуля.

Поскольку $K/(p)$ — поле, фактор $\ker \varphi_i / \ker \varphi_{i-1}$ является векторным пространством над ним, и высота i-того столбца диаграммы[1] ν равна размерности этого пространства

$$\nu_i^t = \dim_{K/(p)} \ker \varphi_i / \ker \varphi_{i-1}\,.$$

Таким образом, диаграмма ν показателей p-кручения однозначно определяется модулем M. Теорема об элементарных делителях полностью доказана.

10.4. Строение конечно порождённых абелевых групп. Над кольцом $K = \mathbb{Z}$ теорема об элементарных делителях доставляет полную классификацию конечно порождённых абелевых групп.

Теорема 10.5
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{\left(p_1^{n_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(p_\alpha^{n_\alpha}\right)} \tag{10-10}$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две аддитивных группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{\left(p_1^{n_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(p_\alpha^{n_\alpha}\right)} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{\left(q_1^{m_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(q_\beta^{m_\beta}\right)}$$

изоморфны тогда и только тогда, когда $r = s$, $\alpha = \beta$ и после надлежащей перестановки слагаемых $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν. □

[1] высота i-того столбца диаграммы ν, это то же самое, что длина i-той строки диаграммы ν^t, транспонированной к ν.

Определение 10.3
Единственное представление заданной конечно порождённой абелевой группы A в виде прямой суммы аддитивных групп (10-10) называется её *каноническим представлением.*

Пример 10.5 (группы, заданные образующими и соотношениями)
На практике конечно порождённые абелевы группы часто задаются описанием вроде: абелева группа A, порождённая элементами $a_1, a_2, \dots, a_n$, связанными соотношениями

$$\begin{cases} \mu_{11}a_1 + \mu_{12}a_2 + \dots + \mu_{1n}a_n = 0 \\ \mu_{21}a_1 + \mu_{22}a_2 + \dots + \mu_{2n}a_n = 0 \\ \mu_{31}a_1 + \mu_{32}a_2 + \dots + \mu_{3n}a_n = 0 \\ \qquad \dots\ \dots\ \dots\ \dots\ \dots \\ \mu_{\mu 1}a_1 + \mu_{\mu 2}a_2 + \dots + \mu_{mn}a_n = 0\,, \end{cases} \tag{10-11}$$

где $\mu_{ij} \in \mathbb{Z}$. По определению, это означает, что $A = \mathbb{Z}^n / R$, где $R \subset \mathbb{Z}^n$ — подмодуль, порождённый строками $\mu_1, \mu_2, \dots, \mu_m$ матрицы $\left(\mu_{ij}\right)$. В каноническом разложении (10-10) группы A ранг r свободного слагаемого равен $n - \operatorname{rk}\left(\mu_{ij}\right)$, а степени $p_i^{n_i}$ суть элементарные делители подмодуля $R \subset \mathbb{Z}^n$.

Про конкретный элемент $w = x_1a_1 + x_2a_2 + \dots + x_na_n$ часто бывает нужно знать, отличен он от нуля в A или нет, и если нет, то каков его порядок[1] $\operatorname{ord}(w)$. Выяснить это можно посредством вычислений в векторном пространстве $\mathbb{Q}^n \supset \mathbb{Z}^n$ над полем $\mathbb{Q}$: если w не лежит в $\mathbb{Q}$-линейной оболочке строк матрицы $\left(\mu_{ij}\right)$, то никакое его целое кратное mw не лежит в M, т. е. $w \neq 0$ в A и $\operatorname{ord} w = \infty$; если же $w = x_1\mu_1 + x_2\mu_2 + \dots + x_m\mu_m$, где $x_i = p_i / q_i \in \mathbb{Q}$ — несократимые дроби, то $\operatorname{ord}(w) = \text{нок}(q_1, q_2, \dots, q_m)$; в частности, если все $q_i = 1$ (т. е. все $x_i \in \mathbb{Z}$), то $w = 0$ в $A = \mathbb{Z}^n / R$.

[1] напомним, что *порядком* $\operatorname{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, или же $\operatorname{ord}(w) = \infty$, если такого n нет (см. n° 3.5.1 на стр. 46)

§11. Пространство с оператором

11.1. Классификация пространств с оператором. Пусть $\Bbbk$ — произвольное поле, V — конечномерное векторное пространство над $\Bbbk$, а $F : V \to V$ — $\Bbbk$-линейный эндоморфизм пространства V. Мы будем называть пару (F, V) *пространством с оператором* или просто *оператором* над $\Bbbk$. Линейное отображение $C : U_1 \to U_2$ между пространствами с операторами (F_1, U_1) и (F_2, U_2) называется *гомоморфизмом*, если $F_2 \circ C = C \circ F_1$. В этом случае говорят, что диаграмма

$$\begin{array}{ccc} U_1 & \xrightarrow{C} & U_2 \\ {\scriptstyle F_1}\uparrow & & \uparrow{\scriptstyle F_2} \\ U_1 & \xrightarrow[C]{} & U_2 \end{array}$$

коммутативна[1]. Если C — изоморфизм векторных пространств, операторы $F_1 : U_1 \to U_1$ и $F_2 : U_2 \to U_2$ называются *изоморфными* или *подобными*. В этой ситуации $F_2 = CF_1C^{-1}$, и говорят, что G получается из F *сопряжением* посредством C.

Подпространство $U \subset V$ называется *F-инвариантным*, если $F(U) \subset U$. В этом случае $(F|_U, U)$ тоже является пространством с оператором и вложение $U \hookrightarrow V$ является гомоморфизмом пространств с операторами. Оператор, не имеющий инвариантных подпространств, отличных от нуля и всего пространства, называется *неприводимым* или *простым*.

Упражнение 11.1. Покажите что оператор умножения на t в фактор кольце $\mathbb{R}[t]/(t^2+1)$ неприводим над $\mathbb{R}$.

Оператор $F : V \to V$ называется *разложимым*, если пространство V можно разложить в прямую сумму двух ненулевых F-инвариантных подпространств, и *неразложимым* — в противном случае. Все простые операторы неразложимы.

Упражнение 11.2. Покажите, что оператор умножения на t в фактор кольце $\Bbbk[t]/(t^n)$ неразложим (поле $\Bbbk$ произвольно) и приводим при $n > 1$.

Таким образом, над любым полем $\Bbbk$ имеются неразложимые пространства с оператором любой размерности. Очевидно, что всякое пространство с оператором является прямой суммой неразложимых.

Упражнение 11.3. Покажите, что двойственные операторы $F : V \to V$ и $F^* : V^* \to V^*$ либо оба разложимы, либо оба неразложимы.

11.1.1. Пространство с оператором как $\Bbbk[t]$-модуль. Задание линейного оператора $F : V \to V$ эквивалентно заданию на пространстве V структуры модуля над кольцом многочленов $\Bbbk[t]$. В самом деле, структура $\Bbbk[t]$-модуля включает в себя операцию умножения векторов на $t : v \mapsto tv$, которая является линейным отображением $V \to V$. Если обозначить его буквой F, то оператор умножения векторов на фиксированный многочлен $f(t) : v \mapsto f(t) \cdot v$ имеет вид $f(F) : V \to V$, т. е. представляет собой результат вычисления многочлена f на элементе F в $\Bbbk$-алгебре $\mathrm{End}(V)$. Наоборот, каждый линейный оператор $F : V \to V$ задаёт на V структуру $\Bbbk[t]$-модуля по формуле $f(t) \cdot v \stackrel{\text{def}}{=} f(F)v$. Мы будем обозначать этот модуль через V_F.

[1] произвольная диаграмма отображений называется *коммутативной*, если композиции отображений вдоль любых двух путей с общим началом и концом одинаковы

Гомоморфизм $\Bbbk[t]$-модулей $C : V_F \to W_G$, построенных по операторам $F : V \to V$ и $G : W \to W$ — это линейное отображение $C : V \to W$, перестановочное с умножением векторов на t, т. е. такое что $C \circ F = F \circ C$. Поэтому операторы F и G изоморфны тогда и только тогда, когда изоморфны $\Bbbk[t]$-модули V_F и W_G.

Векторное подпространство $U \subset V$ является $\Bbbk[t]$-подмодулем в модуле V_F, если и только если оператор умножения на t переводит U в себя, т. е. тогда и только тогда, когда это подпространство F-инвариантно. Аналогично, разложимость V в прямую сумму инвариантных подпространств означает разложимость $\Bbbk[t]$-модуля V_F в прямую сумму $\Bbbk[t]$-подмодулей.

Если векторное пространство V конечномерно над $\Bbbk$, то $\Bbbk[t]$-модуль V_F является конечно порождённым модулем кручения. В самом деле, любой базис V над $\Bbbk$ порождает V_F как модуль над $\Bbbk[t]$, и в каноническом разложении V_F в прямую сумму свободного модуля и модуля кручения[1] свободное слагаемое отсутствует, т. к. иначе V было бы бесконечномерно над $\Bbbk$. Из теоремы об элементарных делителях[2] вытекает

Теорема 11.1
Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{\left(p_i^{m_1}(t)\right)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\left(p_k^{m_k}(t)\right)}, \tag{11-1}$$

где все многочлены $p_\nu(t) \in \Bbbk[t]$ приведены и неприводимы. Каждое прямое слагаемое в этой сумме неразложимо. Операторы умножения на t, действующие в суммах

$$\frac{\Bbbk[t]}{\left(p_i^{m_1}(t)\right)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\left(p_k^{m_k}(t)\right)} \quad \text{и} \quad \frac{\Bbbk[t]}{\left(q_i^{n_1}(t)\right)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\left(q_\ell^{n_\ell}(t)\right)}$$

изоморфны тогда и только тогда, когда $k = \ell$, и прямые слагаемые можно переставить так, чтобы $p_\nu = q_\nu$ и $m_\nu = n_\nu$ при всех ν. □

Определение 11.1 (элементарные делители линейного оператора)
Дизъюнктное объединение[3] всех многочленов $p_\nu^{m_\nu}$, стоящих в правой части разложения (11-1), называется *набором элементарных делителей* оператора $F : V \to V$ и обозначается через $\mathcal{El}(F)$.

Следствие 11.1
Линейные операторы F и G подобны тогда и только тогда, когда $\mathcal{El}(F) = \mathcal{El}(G)$. □

Следствие 11.2
Линейный оператор неразложим тогда и только тогда, когда он подобен оператору умножения на t в фактор кольце $\Bbbk[t]/\left(p^m\right)$, где $p \in \Bbbk[t]$ неприводим и приведён. Неразложимый оператор неприводим, если и только если $m = 1$. □

[1] см. сл. 10.1 на стр. 158

[2] см. теор. 10.4 на стр. 157

[3] напомню, что каждый элементарный делитель p^m входит в него ровно столько раз, сколько прямых слагаемых вида $\Bbbk[t]/(p^m)$ входит в разложение V

Следствие 11.3
Многочлен $f \in \Bbbk[t]$ тогда и только тогда аннулирует оператор $F : V \to V$, когда он делится на все элементарные делители оператора F. □

11.1.2. Нильпотентные операторы. Линейный оператор $F : V \to V$ называется *нильпотентным*, если $F^m = 0$ для некоторого $m \in \mathbb{N}$. Поскольку нильпотентный оператор аннулируется многочленом t^m, все его элементарные делители являются степенями t. Поэтому, согласно теор. 11.1, нильпотентный оператор изоморфен оператору умножения на t в прямой сумме фактор колец вида

$$\frac{\Bbbk[t]}{(t^{\nu_1})} \oplus \cdots \oplus \frac{\Bbbk[t]}{(t^{\nu_k})} \tag{11-2}$$

и два таких оператора изоморфны друг другу тогда и только тогда, когда выстроенные в порядке (нестрогого) убывания наборы показателей $\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_k$ у них одинаковы. Таким образом, нильпотентные операторы над произвольным полем $\Bbbk$ взаимно однозначно соответствуют диаграммам Юнга ν. Диаграмма $\nu(F)$, характеризующая нильпотентный оператор F, называется его *цикловым типом*.

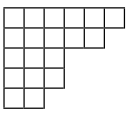
Действие умножения на t на базис пространства $\Bbbk[t] / \left(t^m\right)$, состоящий из классов $e_1 = [t^{m-1}]$, $e_2 = [t^{m-2}]$, … , $e_m = [1]$ по модулю t^m, происходит по правилу

$$0 \leftarrow\!\shortmid e_1 \leftarrow\!\shortmid e_2 \leftarrow\!\shortmid e_3 \leftarrow\!\shortmid \cdots \leftarrow\!\shortmid e_{m-1} \leftarrow\!\shortmid e_m$$

и задаётся матрицей, именуемой *нильпотентной жордановой клеткой* размера m:

$$J_m(0) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Тем самым, для нильпотентного оператора F циклового типа $\nu(F)$ в пространстве V имеется базис, векторы которого размещаются по клеткам диаграммы $\nu(F)$ так, что F переводит каждый из них в левый соседний, а векторы самого левого столбца — в нуль:



(11-3)

Базис такого вида называется *циклическим* (или *жордановым*) базисом, а наборы базисных векторов, стоящие по строкам диаграммы, называются *жордановыми цепочками*. Так как сумма длин первых m столбцов диаграммы $\nu(F)$ равна $\dim \ker F^m$, длина m-того столбца диаграммы $\nu(F)$ равна

$$\nu^t_m(F) = \dim \ker F^m - \dim \ker F^{m-1}. \tag{11-4}$$

11.1.3. Полупростые операторы. Прямая сумма простых или, в другой терминологии, неприводимых пространств с операторами называется *полупростым* или *вполне приводимым* пространством с оператором. Полупростота в каком-то смысле «противоположна» нильпотентности и допускает несколько переформулировок.

Предложение 11.1
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) пространство V является прямой суммой неприводимых F-инвариантных подпространств

2) пространство V линейно порождается неприводимыми F-инвариантными подпространствами

3) для любого ненулевого F-инвариантного подпространства $U \subsetneq V$ найдётся такое F-инвариантное подпространство $W \subset V$, что $V = U \oplus W$

4) оператор F подобен умножению на t в прямой сумме фактор колец

$$\Bbbk[t]/(p_1) \oplus \Bbbk[t]/(p_2) \oplus \cdots \oplus \Bbbk[t]/(p_r)\,,$$

где $p_i \in \Bbbk[t]$ приведены и неприводимы[1] (но не обязательно различны).

Доказательство. Импликация (1) ⇒ (2) очевидна. Проверка импликации (2) ⇒ (3) использует индукцию по $\dim V$ (при $\dim V = 1$ доказывать нечего) и то, что для каждого F-инвариантного подпространства $L \subset V$, пересечение $L \cap U$, будучи F-инвариантным подпространством в L, либо нулевое, либо совпадает с L. Если все инвариантные подпространства $L \subset V$ лежат в U, то $U = V$ в силу (2), и доказывать нечего. Если есть ненулевое F-инвариантное подпространство $L \subset V$ с $L \cap U = 0$, рассмотрим фактор $V' = V/L$ и проекцию $\pi : V \twoheadrightarrow V'$ с ядром L. Она инъективно отображает подпространство $U \subset V$ на ненулевое F-инвариантное подпространство $\pi(U) \subset V'$. Поскольку $\dim V' < \dim V$, при $\pi(U) \subsetneq V$ по индукции найдётся такое F-инвариантное подпространство $W' \subset V'$, что $V' = W' \oplus \pi(U)$. При $\pi(U) = V$ положим $W' = 0$. Возьмём в качестве $W \subset V$ полный прообраз $W = \pi^{-1}(W')$. Проверим, что $V = U + W$: проекция любого $v \in V$ на V' представляется в виде $\pi(v) = \pi(u) + w'$ с $u \in U$, $w' \in W'$, и разность $w = v - u \in W$, поскольку $\pi(w) = \pi(v) - \pi(u) = w' \in W'$; тем самым, $v = w + u$ с $w \in W$, $u \in U$. Если вектор $v \in U \cap W$, то $\pi(v) \in \pi(U) \cap W' = 0$, откуда $v \in \ker \pi = L$. Так как $L \cap U = 0$, мы заключаем, что $U \cap W = 0$ и $V = W \oplus U$.

Чтобы доказать импликацию (3) ⇒ (4), покажем сначала, что если свойство (3) выполнено для пространства V, то оно выполнено и для каждого F-инвариантного подпространства $H \subset V$. Рассмотрим любое инвариантное подпространство $U \subset H$ и отыщем в V такие инвариантные подпространства Q и R, что $V = H \oplus Q = U \oplus Q \oplus R$. Рассмотрим проекцию $\pi : V \twoheadrightarrow H$ с ядром Q и положим $W = \pi(R)$.

Упражнение 11.4. Проверьте, что $H = U \oplus W$.

Таким образом, если свойство (3) выполнено для прямой суммы фактор колец (11-1) из теор. 11.1, то оно выполнено и для каждого слагаемого этой суммы. Однако по сл. 11.2 при $m > 1$ пространство $\Bbbk[t]/(p^m)$ приводимо, но неразложимо.

Импликация (4) ⇒ (1) также немедленно вытекает из сл. 11.2. □

Следствие 11.4 (из доказательства предл. 11.1)
Ограничение полупростого оператора на инвариантное подпространство также является полупростым оператором.

[1] иными словами, в прямой сумме (11-1) из теор. 11.1 все показатели степеней $m_i = 1$

11.1.4. Характеристический многочлен. Пусть оператор $F : V \to V$ имеет матрицу F_v в каком либо базисе v пространства V. Характеристический многочлен $\det(tE - F_v)$ этой матрицы не меняется при переходе к любому другому базису $w = v\,C$, поскольку по форм. (8-13) на стр. 126 $F_w = C^{-1}F_vC$ и

$$\det\left(tE - F_w\right) = \det\left(tC^{-1}EC - C^{-1}F_vC\right) = \det\left(C^{-1}\left(tE - F_v\right)C\right) = \\ = \det C^{-1} \cdot \det\left(tE - F_v\right) \cdot \det C = \det\left(tE - F_v\right)\,.$$

Многочлен $\chi_F(t) \stackrel{\text{def}}{=} \det(tE - F_v)$ называется *характеристическим многочленом* оператора F. Предыдущее вычисление показывает, что подобные операторы имеют равные характеристические многочлены.

Упражнение 11.5. Пусть пространство с оператором (F, W) является прямой суммой пространств с операторами (G, U) и (H, V). Убедитесь, что $\chi_F(t) = \chi_G(t) \cdot \chi_H(t)$ в $\Bbbk[t]$.

Упражнение 11.6. Пусть $f \in \Bbbk[t]$ — любой приведённый многочлен. Убедитесь, что характеристический многочлен оператора умножения на t в фактор кольце $\Bbbk[t]/(f)$ равен f.

Из этих упражнений и теор. 11.1 мы получаем

Предложение 11.2
Характеристический многочлен равен произведению всех элементарных делителей. □

Упражнение 11.7. Выведите из предл. 11.2 новое доказательство теоремы Гамильтона – Кэли.

11.1.5. Минимальный многочлен. Для каждого неприводимого приведённого многочлена $p \in \Bbbk[t]$ обозначим через $m_p(F)$ максимальный показатель m, с которым p^m присутствует в наборе элементарных делителей оператора F, а для тех p, степени которых не представлены в $\mathcal{E}\ell\, F$, положим $m_p(F) = 0$. Таким образом, $m_p(F) = 0$ для всех p кроме конечного числа. Из теор. 11.1 вытекает, что приведённый многочлен $\mu_F(t)$ наименьшей возможной степени, аннулирующий оператор F, равен

$$\mu_F(t) = \prod_p p^{m_p(F)}\,,$$

где произведение берётся по всем приведённым неприводимым $p \in \Bbbk[t]$. Многочлен $\mu_F(t)$ называется *минимальным многочленом* оператора F. Отметим, что минимальный многочлен делит характеристический.

11.1.6. Циклические векторы. Вектор $v \in V$ называется *циклическим вектором* линейного оператора $F : V \to V$, если его F-орбита v, Fv, F^2v, F^3v,, … линейно порождает пространство V над полем $\Bbbk$. Иначе можно сказать, что v порождает модуль V_F над $\Bbbk[t]$.

Предложение 11.3
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) F обладает циклическим вектором

2) F подобен умножению на t в фактор кольце $\Bbbk[t]/(f)$, где $f \in \Bbbk[t]$ — какой-либо приведённый многочлен

3) каждый неприводимый $p \in \Bbbk[t]$ встречается в $\mathcal{E}\ell\, F$ не более одного раза

4) минимальный многочлен оператора F совпадает с характеристическим.

Доказательство. Условия (3) и (4) эквивалентны в силу предл. 11.2 и означают, что оператор F подобен умножению на t в прямой сумме фактор колец

$$\Bbbk[t]/\left(p_1^{m_1}\right) \oplus \Bbbk[t]/\left(p_2^{m_2}\right) \oplus \cdots \oplus \Bbbk[t]/\left(p_r^{m_r}\right) ,$$

в которой все неприводимые приведённые многочлены $p_1, p_2, \ldots, p_r$ попарно различны. По китайской теореме об остатках, эта сумма изоморфна $\Bbbk[t]/(f)$, где

$$f = \chi_F = \mu_F = \prod_{i=1}^{r} p_i^{m_i} .$$

Тем самым, (2) равносильно (3) и (4). Импликация (2) ⇒ (1) очевидна: в качестве циклического вектора для оператора умножения на t в фактор кольце $\Bbbk[t]/(f)$ можно взять $v = [1]$. Наоборот, если модуль V_F порождается над $\Bbbk[t]$ одним вектором v, то $V_F = \Bbbk[t]/R$, где $R = \ker \pi$ — ядро $\Bbbk[t]$-линейного эпиморфизма $\Bbbk[t] \twoheadrightarrow V_F$, преводящего 1 в v. Поскольку $\Bbbk[t]$ — кольцо главных идеалов, модмодуль $R \subset \Bbbk[t]$ имеет вид (f), где f-приведённый многочлен наименьшей степени со свойством $f(F)v = 0$. Тем самым, $V = \Bbbk[t]/(f)$. □

11.2. Собственные подпространства. Инвариантное для оператора $F : V \to V$ подпространство, на котором F действует как скалярное умножение на число $\lambda \in \Bbbk$, обозначается

$$V_\lambda \stackrel{\text{def}}{=} \{v \in V \mid F(v) = \lambda v\} = \ker(\lambda \operatorname{Id}_V - F)$$

и называется *собственным подпространством* оператора F. Ненулевые векторы $v \in V_\lambda$ называются *собственными векторами* оператора F с собственным числом λ.

Предложение 11.4
Любой набор собственных векторов с попарно различными собственными числами линейно независим.

Доказательство. Пусть собственные векторы $v_1, v_2, \ldots, v_m$ имеют попарно разные собственные числа $\lambda_1, \lambda_2, \ldots, \lambda_m$ и линейно зависимы. Рассмотрим зависимость, содержащую минимально возможное число векторов, и пусть это будут векторы $e_1, e_2, \ldots, e_k$. Тогда $k \geqslant 2$ и $e_k = x_1 e_1 + x_2 e_2 + \cdots + x_{k-1} e_{k-1}$, где все $x_i \in \Bbbk$ отличны от нуля. При этом $\lambda_k e_k = F(e_k) = \sum x_i F(e_i) = \sum x_i \lambda_i e_i$. Вычитая из этого равенства предыдущее, умноженное на λ_k получаем более короткую линейную зависимость

$$0 = x_1(\lambda_1 - \lambda_k) \cdot e_1 + x_1(\lambda_1 - \lambda_k) \cdot e_2 + \cdots + x_{k-1}(\lambda_{k-1} - \lambda_k) \cdot e_{k-1}$$

с ненулевыми коэффициентами. □

Следствие 11.5
Сумма ненулевых собственных подпространств с разными собственными числами является прямой. □

11.2.1. Спектр. Все $\lambda \in \Bbbk$, для которых $V_\lambda \neq 0$, называются *собственными числами* (или *собственными значениями*) оператора F. Совокупность собственных чисел оператора $F : V \to V$ обозначается $\operatorname{Spec} F$ и называется *спектром* оператора F в поле $\Bbbk$. По сл. 11.5

$$\sum_{\lambda \in \operatorname{Spec} F} \dim V_\lambda \leqslant \dim V\,. \tag{11-5}$$

В частности, любой оператор $F : V \to V$ имеет не более $\dim V$ собственных чисел.

Упражнение 11.8. Покажите, что $\operatorname{Spec} F$ содержится в множестве корней любого многочлена, аннулирующего F.

Поскольку условие $\ker(\lambda \operatorname{Id}_V - F) \neq 0$ равносильно условию $\det(\lambda \operatorname{Id}_V - F) = 0$, спектр оператора F совпадает с множеством всех различных корней его характеристического многочлена $\chi_F(t) = \det(tE - F)$. В частности, справедливо

Предложение 11.5
Над алгебраически замкнутым полем $\Bbbk$ любой оператор обладает хотя бы одним ненулевым собственным подпространством. □

Упражнение 11.9. Покажите, что над алгебраически замкнутым полем $\Bbbk$ оператор F нильпотентен тогда и только тогда, когда когда $\operatorname{Spec} F = \{0\}$, и приведите пример оператора, для которого неравенство (11-5) строгое.

Если известен спектр F, отыскание собственных подпространств сводится к решению систем линейных однородных уравнений $(\lambda \operatorname{Id}_V - F)\, v = 0$, которые гарантированно имеют ненулевые решения при $\lambda \in \operatorname{Spec} F$.

11.2.2. Диагонализуемые операторы. Оператор $F : V \to V$ называется *диагонализуемым*, если в V имеется базис, в котором F записывается диагональной матрицей. Такой базис состоит из собственных векторов оператора F, а элементы диагональной матрицы суть собственные числа F, и каждое $\lambda \in \operatorname{Spec} F$ встречается на диагонали ровно столько раз, какова кратность корня $t = \lambda$ в характеристическом многочлене $\chi_F(t)$ и какова размерность собственного подпространства V_λ.

Иначе можно сказать, что диагонализуемый оператор F подобен оператору умножения на t в прямой сумме фактор колец $\Bbbk[t]/(t - \lambda) \simeq \Bbbk$, где λ пробегает $\operatorname{Spec} F$, и каждое прямое слагаемое представлено $\dim V_\lambda$ раз.

Предложение 11.6
Следующие свойства оператора $F : V \to V$ эквивалентны:

1) F диагонализуем
2) пространство V линейно порождается собственными векторами оператора F
3) характеристический многочлен $\chi_F(t) = \det(tE - F)$ полностью раскладывается в $\Bbbk[t]$ на линейные множители, и кратность каждого его корня λ равна размерности собственного подпространства V_λ
4) все элементарные делители F имеют вид $(t - \lambda)$, $\lambda \in \Bbbk$
5) оператор F аннулируется многочленом f, раскладывающимся в $\Bbbk[t]$ в произведение попарно различных линейных множителей.

Доказательство. Эквивалентности (2) $\Longleftrightarrow$ (1) $\Longleftrightarrow$ (4) и импликация (1) $\Rightarrow$ (3) очевидны. Эквивалентность (4) $\Longleftrightarrow$ (5) следует из сл. 11.3. Из (3) вытекает, что $\sum \dim V_\lambda = \deg \chi_F = \dim V$. Поэтому прямая по сл. 11.5 сумма всех различных собственных подпространств V_λ совпадает с V, что даёт импликацию (3) $\Rightarrow$ (1). □

Следствие 11.6
Если оператор $F : V \to V$ диагонализуем, то его ограничение на любое инвариантное подпространство тоже диагонализуемо на этом подпространстве.

Доказательство. Это вытекает из свойства (5) предл. 11.6. □

Упражнение 11.10. Убедитесь, что над алгебраически замкнутым полем диагонализуемость равносильна полупростоте.

11.3. Аннулирующие многочлены. Если задан многочлен $f \in \Bbbk[x]$, аннулирующий линейный оператор[1] $F : V \to V$, и известно, как f раскладывается в $\Bbbk[t]$ на простые множители, то в силу сл. 11.3 это оставляет лишь конечное число возможностей для набора элементарных делителей $\mathcal{E}\ell(F)$ и часто позволяет явно описать разложение V в прямую сумму F-инвариантных подпространств во внутренних терминах действия F на пространстве V.

Пример 11.1 (инволюции)
Линейный оператор $\sigma : V \to V$ называется *инволюцией*, если он аннулируется многочленом $t^2 - 1$, т. е. удовлетворяет соотношению $\sigma^2 = \mathrm{Id}_V$. Тождественная инволюция $\sigma = \mathrm{Id}_V$ называется *тривиальной*. Так как $t^2 - 1 = (t+1)(t-1) = 0$ является произведением различных линейных множителей, все инволюции диагонализуемы. Пространство V с инволюцией σ распадается в прямую сумму собственных подпространств $V = V_+ \oplus V_-$ с собственными значениями ± 1, и любой вектор $v \in V$ однозначно представим в виде $v = v_+ + v_-$, где $v_+ = (v + Fv)/2 \in V_+ = \ker(\sigma - \mathrm{Id}_V) = \mathrm{im}(\sigma + \mathrm{Id}_V)$ и $v_- = (v - Fv)/2 \in V_- = \ker(\sigma + \mathrm{Id}_V) = \mathrm{im}(\sigma - \mathrm{Id}_V)$.

Предложение 11.7
Пусть оператор $F : V \to V$ аннулируется многочленом $q \in \Bbbk[t]$, раскладывающимся над полем $\Bbbk$ в произведение $q = q_1 \cdot q_2 \cdot \cdots \cdot q_r$ попарно взаимно простых многочленов $q_i \in \Bbbk[t]$. Положим $Q_j = q/q_j = \prod\limits_{\nu \neq j} q_\nu$. Тогда $\ker q_j(F) = \mathrm{im}\, Q_j(F)$ для каждого j, все эти подпространства F-инвариантны, и пространство V является прямой суммой тех из них, что отличны от нуля.

Доказательство. Поскольку $q(F) = q_j(F) \circ Q_j(F) = 0$, имеется включение

$$\mathrm{im}\, Q_j(F) \subset \ker q_j(F).$$

Из взаимной простоты $q_i(t)$ и $Q_i(t)$ вытекает, что сумма ядер $\ker q_i(F)$ прямая:

$$\ker q_i(F) \cap \sum_{j \neq i} \ker q_j(F) = 0.$$

[1] в силу тождества Гамильтона – Кэли по крайней мере один такой многочлен, а именно $\chi_F(t) = \det(tE - F)$, всегда можно предъявить явно

Действительно, подберём такие многочлены $g(t)$ и $h(t)$, что $1 = g(t)q_i(t) + h(t)Q_i(t)$, подставим в это равенство $t = F$ и применим оператор $E = g(F) \circ q_i(F) + h(F) \circ Q_j(F)$ к любому вектору $v \in \ker q_i(F) \cap \sum\limits_{j \neq i} \ker q_j$. Так как $\ker Q_j(F)$ содержит все $\ker q_j(F)$ с $j \neq i$, получим

$$v = Ev = g(F) \circ q_i(F)v + h(F) \circ Q_j(F)v = 0\,.$$

Наконец, из взаимной простоты многочленов $Q_1, Q_2, \ldots, Q_r$ вытекает, что V линейно порождается образами $\operatorname{im} Q_j(F)$: подберём такие многочлены $h_1, h_2, \ldots, h_r \in \Bbbk[t]$, что $\sum Q_j(t) \cdot h_j(t) = 1$, подставим в это равенство $t = F$ и применим обе части к любому вектору $v \in V$. Получим $v = Ev = \sum Q_j(F)h_j(F)v \in \sum \operatorname{im} Q_j(F)$. □

Пример 11.2 (проекторы)
Линейный оператор $\pi : V \to V$ называется *идемпотентом* или *проектором*, если он аннулируется многочленом $t^2 - t = t(t-1)$, т. е. удовлетворяет соотношению $\pi^2 = \pi$. По предл. 11.7 образ любого идемпотента $\pi : V \to V$ совпадает с подпространством его неподвижных векторов:

$$\operatorname{im}\pi = \ker(\pi - \mathrm{Id}_V) = \{v \mid \pi(v) = v\}\,,$$

и $V = \ker\pi \oplus \operatorname{im}\pi$, так что π проектирует V на $\operatorname{im}\pi$ вдоль $\ker\pi$. Отметим, что оператор $\mathrm{Id}_V - \pi$ тоже является идемпотентом и проектирует V на $\ker\pi$ вдоль $\operatorname{im}\pi$. Таким образом, задание прямого разложения $V = U \oplus W$ равносильно заданию пары идемпотентных эндоморфизмов пространства V: проектора $\pi_U : V \twoheadrightarrow U$ вдоль W и проектора $\pi_W : V \twoheadrightarrow U$ вдоль W, связанных соотношениями $\pi_U + \pi_W = 1$ и $\pi_U\pi_W = \pi_W\pi_U = 0$.

Предложение 11.8
Над полем вещественных чисел $\mathbb{R}$ любой оператор обладает одномерным или двумерным инвариантным подпространством.

Доказательство. Пусть $\chi_F = q_1 q_2 \ldots q_m$, где $q_i \in \mathbb{R}[t]$ — неприводимые приведённые линейные или квадратичные многочлены, не обязательно различные. Применим нулевой оператор $0 = q_1(F) \circ q_2(F) \circ \cdots \circ q_m(F)$ к какому-нибудь ненулевому вектору $v \in V$. Тогда при некотором $i \geqslant 0$ мы получим такой ненулевой вектор $w = q_{i+1}(F) \circ \cdots \circ q_m(F)\, v$, что $q_i(F)\, w = 0$. Если $q_i(t) = t - \lambda$ линеен, то $F(w) = \lambda w$, и мы имеем 1-мерное F-инвариантное подпространство $\Bbbk \cdot w$. Если $q_i(t) = t^2 - \alpha t - \beta$ квадратичен, то $F(Fw) = \alpha F(w) + \beta w$ лежит в линейной оболочке векторов w и Fw, которая тем самым является F-инвариантным подпространством, и её размерность не превышает 2. □

11.4. Разложение Жордана. Всюду в этом разделе мы считаем, что основное поле $\Bbbk$ алгебраически замкнуто. В этом случае неприводимые многочлены в $\Bbbk[t]$ исчерпываются линейными двучленами $(t - \lambda)$, и по теор. 11.1 каждый оператор $F : V \to V$ подобен оператору умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{\big((t-\lambda_1)^{m_1}\big)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\big((t-\lambda_s)^{m_s}\big)}\,, \tag{11-6}$$

причём операторы умножения на t в прямых суммах

$$\frac{\Bbbk[t]}{\big((t-\nu_1)^{n_1}\big)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\big((t-\nu_r)^{n_r}\big)} \quad \text{и} \quad \frac{\Bbbk[t]}{\big((t-\mu_1)^{m_1}\big)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\big((t-\mu_s)^{m_s}\big)}$$

подобны , если и только если $r = s$ и прямые слагаемые можно перенумеровать так, чтобы $\mu_i = \nu_i$ и $m_i = n_i$ при всех i. В фактор кольце $\Bbbk[t]/\left((t-\lambda)^m\right)$ оператор умножения на $t = \lambda + (t-\lambda)$ является суммой скалярного оператора $\lambda E : f \mapsto \lambda f$ и нильпотентного оператора $\eta : f \mapsto (t-\lambda)\cdot f$, для которого многочлены $(t-\lambda)^{m-1}$, $(t-\lambda)^{m-2}$, … , $(t-\lambda)$, 1 образуют жорданову цепочку длины m. В базисе из этих многочленов умножение на t задаётся двудиагональной $m \times m$-матрицей

$$J_m(\lambda) \stackrel{\text{def}}{=} \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \tag{11-7}$$

в остальных местах которой стоят нули. Эта матрица называется *жордановой клеткой* размера m с собственным числом λ.

Следствие 11.7 (жорданова нормальная форма)
Над алгебраически замкнутым полем $\Bbbk$ для любого оператора $F : V \to V$ в V существует базис, в котором матрица F имеет блочный вид

$$\begin{pmatrix} J_{m_1}(\lambda_1) & & & \\ & J_{m_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{m_k}(\lambda_k) \end{pmatrix} \tag{11-8}$$

по главной диагонали которого стоят жордановы клетки[1] $J_{m_1}(\lambda_1)$, $J_{m_2}(\lambda_2)$ … , $J_{m_k}(\lambda_k)$ вида (11-7), а в остальных местах — нули. С точностью до перестановки блоков матрица (11-8) не зависит от выбора такого базиса. Два оператора подобны тогда и только тогда, когда их матрицы (11-8) отличаются друг от друга перестановкой блоков. □

Определение 11.2
Матрица (11-8) называется *жордановой нормальной формой* оператора F. Всякий базис пространства V, в котором матрица оператора F имеет жорданову нормальную форму, называется *жордановым базисом* оператора F .

11.4.1. Корневое разложение. Для произвольного оператора $F : V \to V$ подмодуль $(t-\lambda)$-кручения в модуле V_F называется *корневым подпространством* оператора F, отвечающим собственному $\lambda \in \operatorname{Spec} F$ и обозначается

$$K_\lambda = \{v \in V \mid \exists\, m \in \mathbb{N} : (\lambda \operatorname{Id} - F)^m v = 0\} = \bigcup_{m \geqslant 1} \ker(\lambda \operatorname{Id} - F)^m = \ker(\lambda \operatorname{Id} - F)^{m_\lambda}, \tag{11-9}$$

где m_λ — максимальный из показателей степеней элементарных делителей F вида $(t-\lambda)^m$. Каждое корневое подпространство K_λ содержит ненулевое собственное подпространство V_λ и тем самым отлично от нуля. Разложение $\Bbbk[t]$-модуля V_F в прямую сумму $\Bbbk[t]$-

[1] ещё раз отметим, что числа λ_i и m_i могут повторяться

подмодулей $(t-\lambda)$-кручения из сл. 10.2 на стр. 159 имеет вид $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ и называется *корневым разложением* оператора F.

Упражнение 11.11. Получите корневое разложение как следствие предл. 11.7 и тождества Гамильтона – Кэли без использования сл. 10.2 и теоремы об элементарных делителях.

Количество жордановых клеток размера m с заданным собственным значением λ в жордановой нормальной форме оператора F равно количеству строк длины m в диаграмме Юнга ν нильпотентного оператора $(\lambda\operatorname{Id}-F)|_{K_\lambda} : K_\lambda \to K_\lambda$. Согласно форм. (11-4) на стр. 163 длина k-того столбца этой диаграммы равна

$$\nu_k^t = \dim\ker(\lambda\operatorname{Id}-F)^k - \dim\ker(\lambda\operatorname{Id}-F)^{k-1}. \tag{11-10}$$

Таким образом, для отыскания жордановой нормальной формы оператора F достаточно разложить характеристический многочлен $\chi_F(t)$ на множители (**??**) и для каждого корня λ и натурального k в пределах $1 \leqslant k \leqslant m_\lambda$ вычислить $\dim\ker(\lambda\operatorname{Id}-F)^k$, после чего построить диаграмму Юнга ν с длинами столбцов (11-10) и написать столько клеток $J_\ell(\lambda)$, сколько строк длины ℓ имеется в диаграмме ν.

11.4.2. Перестановочные операторы. Если линейные операторы $F, G : V \to V$ на векторном пространстве V над произвольным полем $\Bbbk$ коммутируют друг с другом: $FG = GF$, то ядро и образ любого многочлена от оператора F переводятся оператором G в себя, т. к. $f(F)v = 0 \;\Rightarrow\; f(F)Gv = Gf(F)v = 0$ и $v = f(F)w \;\Rightarrow\; Gv = Gf(F)w = f(F)Gw$. В частности, собственные подпространства $V_\lambda = \ker(F-\lambda E)$ и корневые подпространства $K_\lambda = \bigcup_n \ker(\lambda\operatorname{Id}-F)^n$ оператора F инвариантны относительно любого оператора G, перестановочного с F.

Лемма 11.1
Над алгебраически замкнутым полем любое множество коммутирующих операторов обладает общим собственным вектором. Над произвольным полем любое множество диагонализуемых коммутирующих операторов может быть диагонализовано одновременно в одном общем базисе.

Доказательство. Индукция по размерности пространства. Если она равна единице или если все операторы скалярны, то доказывать нечего — подойдут любой ненулевой вектор и, соответственно, любой базис. Если среди операторов есть нескалярный, то его собственные подпространства имеют меньшую размерность и инвариантны для всех операторов, причём если операторы были диагонализуемы во всём пространстве, то их ограничения на инвариантные подпространства будут диагонализуемы на этих подпространствах (см. сл. 11.6). Применяя к собственным подпространствам предположение индукции, получаем требуемое. □

Теорема 11.2 (разложение Жордана)
Над алгебраически замкнутым полем $\Bbbk$ для каждого оператора F существует единственная пара операторов F_s и F_n, таких что F_n нильпотентен, F_s диагонализуем, $F = F_s + F_n$ и $F_sF_n = F_nF_s$. Кроме того, операторы F_s и F_n являются многочленами с нулевым свободным членом от оператора F.

Доказательство. Представим F оператором умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{\left((t-\lambda_1)^{m_1}\right)} \oplus \cdots \oplus \frac{\Bbbk[t]}{\left((t-\lambda_s)^{m_s}\right)}, \tag{11-11}$$

и пусть[1] $\operatorname{Spec} F = \{\lambda_1, \lambda_2, \ldots, \lambda_r\}$. Для каждого $i = 1, 2, \ldots, r$ зафиксируем $a_i \in \mathbb{N}$, строго большее максимального показателя m_{λ_i}, с которыми $(t-\lambda_i)$ встречается в (11-11). По китайской теореме об остатках существуют многочлены $f_1, f_2, \ldots, f_r \in \Bbbk[t]$, такие что

$$f_\nu(t) \equiv \begin{cases} 1 \mod \left(t-\lambda_\nu\right)^{a_\nu} \\ 0 \mod \left(t-\lambda_\mu\right)^{a_\mu} \text{ при } \mu \neq \nu\,. \end{cases}$$

Если $\lambda_\nu \neq 0$, многочлен t обратим по модулю $(t-\lambda_\nu)^{a_\nu}$, и найдётся многочлен $g_\nu(t)$, такой что $t \cdot g_\nu(t) \equiv \lambda_\nu \mod \left(t-\lambda_\nu\right)^{a_\nu}$. Для $\lambda_\nu = 0$, положим $g_\nu = 0$. Тогда при всех ν многочлен

$$p_s(t) \stackrel{\text{def}}{=} t\sum_{\nu=1}^{r} g_\nu(t) f_\nu(t) \equiv \lambda_\nu \mod \left(t-\lambda_\nu\right)^{a_\nu}$$

и не имеет свободного члена. Поэтому умножение на $p_s(t)$ действует на каждом факторе $\Bbbk[t]/\left((t-\lambda_\nu)^m\right)$ из разложения (11-11) как умножение на λ_ν. Тем самым, оператор $F_s = p_s(F)$ диагонализуем. Оператор $F_n = F - F_s$ действует на $\Bbbk[t]/\left((t-\lambda_\nu)^m\right)$ умножением на $t-\lambda_\nu$ и, значит, нильпотентен. Будучи многочленами от F, операторы F_s и F_n перестановочны между собою и с F. Это доказывает существование операторов F_s, F_n и последнее утверждение.

Докажем единственность. Пусть есть ещё одно разложение $F = F'_s + F'_n$, удовлетворяющее условиям теоремы. Поскольку F'_s и F'_n перестановочны между собой, они перестановочны с $F = F'_s + F'_n$, а значит, и с построенными выше многочленами F_s, F_n от F. Поэтому каждое собственное подпространство V_λ оператора F_s переводится оператором F'_s в себя, и F'_s диагонализуем на V_λ. Если бы F'_s имел на V_λ собственный вектор v с собственным значением $\mu \neq \lambda$, то вектор v был собственным для оператора $F_n - F'_n = F_s - F'_s$ с ненулевым собственным числом $\lambda - \mu$, что невозможно, т. к. $F_n - F'_n$ нильпотентен.

Упражнение 11.12. Докажите это.

Следовательно $F'_s|_{V_\lambda} = \lambda\mathrm{Id}$, откуда $F'_s = F_s$ и $F'_n = F - F'_s = F - F_s = F_n$. □

Определение 11.3
Операторы F_s и F_n из теор. 11.2 называются, соответственно, *полупростой*[2] (или *диагонализуемой*) и *нильпотентной* составляющими оператора F.

Упражнение 11.13. Покажите, что если оператор $F : V \to V$ переводит некоторое подпространство $U \subset V$ в некоторое подпространство $W \subset V$, то его жордановы компоненты F_s, и F_n тоже переводят U в W.

[1] напомню, что $\lambda_1, \lambda_2, \ldots, \lambda_r$ это множество всех различных $\lambda_i \in \Bbbk$, встречающихся в (11-11)
[2] индекс «s» в обозначении F_s происходит от английского *semisimple*

11.5. Функции от оператора. Пусть основное поле $\Bbbk = \mathbb{C}$ и оператор F умножения на t в прямой сумме фактор колец

$$W = \frac{\mathbb{C}[t]}{\big((t-\lambda_1)^{s_1}\big)} \oplus \cdots \oplus \frac{\mathbb{C}[t]}{\big((t-\lambda_r)^{s_r}\big)} \tag{11-12}$$

имеет спектр[1] $\operatorname{Spec} F = \{\lambda_1, \lambda_2, \dots, \lambda_r\}$ и минимальный многочлен $\mu_F = \prod\limits_{\lambda \in \operatorname{Spec} F} (t-\lambda)^{m_\lambda}$.

Назовём подалгебру $\mathcal{C}$ в алгебре всех функций $f : \mathbb{C} \to \mathbb{C}$ *пригодной для вычисления* на операторе F, если $\mathcal{C}$ содержит алгебру многочленов и любая функция $f \in \mathcal{C}$ допускает при каждом $\lambda \in \operatorname{Spec} F$ представление в виде

$$f(z) = f(\lambda) + \frac{f'(\lambda)}{1!}(z-\lambda) + \cdots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!}(z-\lambda)^{m_\lambda-1} + g_\lambda(z)\cdot(z-\lambda)^{m_\lambda}, \tag{11-13}$$

где $g_\lambda \in \mathcal{C}$, а $f^{(k)} = \frac{d^k f}{dz^k}$ означает k-тую производную. В теор. 11.3 мы покажем, что существует единственный гомоморфизм алгебр

$$\operatorname{ev}_F : \mathcal{C} \to \operatorname{End}(W),$$

продолжающий гомоморфизм вычисления значений многочленов на операторе F на любую пригодную к вычислению на F алгебру функций $\mathcal{C} \supset \mathbb{C}[z]$. Для каждого подобного F оператора $G = CFC^{-1} : U \to U$ на любом пространстве U, связанным с W изоморфизмом $C : W \xrightarrow{\sim} U$, положим по определению $\operatorname{ev}_G = \operatorname{ev}_{CFC^{-1}} : f \mapsto C \circ \operatorname{ev}_F(f) \circ C^{-1}$.

Пример 11.3
Примером алгебры, пригодной для вычисления на данном операторе F, является алгебра $\mathcal{C}$ всех функций $f : \mathbb{C} \to \mathbb{C}$, которые раскладываются в круговой окрестности каждой точки $\lambda \in \operatorname{Spec} F$ в абсолютно сходящийся в этой окрестности ряд Тейлора. Тем самым, любой линейный оператор $G : V \to V$ можно подставить в любую функцию $f \in \mathcal{C}$. Например, для любого оператора F, спектр которого не содержит чисел вида $2\pi i k$, $k \in \mathbb{Z}$, определён оператор $\operatorname{th}(F)$. А если функция $f(z)$ является суммой степенного ряда, сходящегося всюду в $\mathbb{C}$, то оператор $f(F)$ определён вообще для каждого линейного оператора $F : V \to V$ на любом конечномерном векторном пространстве V. В частности, для всех операторов F определены операторы e^F, $\sin F$, $\operatorname{ch} F$ и т. п.

Теорема 11.3
Пусть алгебра $\mathcal{C} \supset \mathbb{C}[z]$ пригодна для вычисления на операторе $F : W \to W$ умножения на t в прямой сумме (11-12). Тогда вычисление $\operatorname{ev}_F : \mathbb{C}[z] \to \operatorname{End} W$ допускает единственное продолжение до гомоморфизма алгебр $\operatorname{ev}_F : \mathcal{C} \to \operatorname{End} W$. При этом $\forall\, f \in \mathcal{C}$

$$\operatorname{ev}_F(f) = P_{f,F}(F),$$

где $P_{f,F}(z) \in \mathbb{C}[z]$ — многочлен, значение которого в каждой точке $\lambda \in \operatorname{Spec} F$ вместе со значениями начальных $m_\lambda - 1$ производных те же, что у функции f:

$$P^{(k)}_{f,F}(\lambda) = f^{(k)}(\lambda) \quad \text{при всех } 0 \leqslant k \leqslant m_\lambda - 1.$$

(такой многочлен $P_{f,F}$ единствен по модулю минимального многочлена μ_F оператора F).

[1] ещё раз напомню, что $\lambda_1, \lambda_2, \dots, \lambda_r \in \mathbb{C}$ это все различные числа, присутствующие в (11-12), а $m_\lambda = m_{t-\lambda}(F)$ это максимальный показатель, встречающийся в (11-12) у элементарных делителей вида $(t-\lambda)^m$

Доказательство. Пусть искомое продолжение ev_F на алгебру $\mathcal{C}$ существует. Зафиксируем произвольную функцию $f \in \mathcal{C}$ и подставим $z = F$ в соотношение (11-13). Получим

$$f(F) = f(\lambda)\cdot E + f'(\lambda)\cdot(F-\lambda E) + \cdots + \frac{1}{(m_\lambda-1)!} f^{(m_\lambda-1)}(\lambda)(F-\lambda E)^{m_\lambda-1} + g_\lambda(F)(F-\lambda E)^{m_\lambda}\,. \quad (11\text{-}14)$$

Поскольку $(F-\lambda E)^m$ действует на прямой сумме фактор колец

$$W = \frac{\mathbb{C}[t]}{\big((t-\lambda_1)^{s_1}\big)} \oplus \cdots \oplus \frac{\mathbb{C}[t]}{\big((t-\lambda_r)^{s_r}\big)}$$

умножением на $(t-\lambda)^m$, последнее слагаемое в (11-14) аннулирует подмодуль $(t-\lambda)$-кручения[1]. Мы заключаем, что для каждого $\lambda \in \mathrm{Spec}(F)$ оператор $f(F)$ переводит подмодуль $(t-\lambda)$-кручения в себя и действует на нём как оператор умножения на многочлен

$$f(\lambda) + f'(\lambda)\cdot(t-\lambda) + \cdots + f^{(m_\lambda-1)}(\lambda)\cdot(t-\lambda)^{m_\lambda-1}/(m_\lambda-1)! \quad (11\text{-}15)$$

По китайской теореме об остатках существует единственный класс $[P_{f,F}] \in \Bbbk[t]\,/\,\big(\mu_F\big)$ сравнимый с многочленом (11-15) по модулю $(t-\lambda)^{m_\lambda}$ сразу для всех $\lambda \in \mathrm{Spec}\,F$, и действие оператора $f(F)$ на всём пространстве W совпадает с действием оператора $P_{f,F}(F)$. Это доказывает единственность продолжения и последнее утверждение теоремы.

Проверим теперь, что правило $f(F) \stackrel{\text{def}}{=} P_{f,F}(F)$ действительно задаёт гомоморфизм алгебр $\mathcal{C} \to \mathrm{End}\,W$. Обозначим через $s^m_\lambda : \mathcal{C} \to \mathbb{C}[t]/\big((t-\lambda)^m\big)$ отображение, сопоставляющее функции $f \in \mathcal{C}$ её $(m-1)$-*ю струю* в точке $\lambda \in \mathbb{C}$:

$$s^m_\lambda f \stackrel{\text{def}}{=} \sum_{k=0}^{m-1} \frac{1}{k!} f^{(k)}(\lambda)\,(t-\lambda)^k \mod (t-\lambda)^m$$

и рассмотрим прямое произведение таких отображений по всем точкам $\lambda \in \mathrm{Spec}\,F$:

$$\begin{aligned} s : \mathcal{C} &\to \prod_{\lambda\in\mathrm{Spec}\,F} \mathbb{C}[t]/\big((t-\lambda)^{m_\lambda}\big) \simeq \mathbb{C}[t]/\big(\mu_F\big) \\ f &\mapsto \Big(s^{m_{\lambda_1}-1}_{\lambda_1} f,\ \ldots\ , s^{m_{\lambda_r}-1}_{\lambda_r} f\Big)\,. \end{aligned} \quad (11\text{-}16)$$

Упражнение 11.14. Проверьте, что отображение (11-16) является гомоморфизмом алгебр. Композиция гомоморфизма (11-16) с гомоморфизмом $\mathrm{ev}_F : \mathbb{C}[t]/\big(\mu_F\big) \to \mathrm{End}\,W$ и является искомым гомомрфизмом вычисления. □

11.5.1. Интерполяционный многочлен. Многочлен $P_{f,F} \in \mathbb{C}[z]$ значение которого на операторе $F : V \to V$ равно значению функции $f \in \mathcal{C}$ на этом операторе, называется *интерполяционным многочленом* для вычисления $f(F)$. Он зависит как от функции f, так и от оператора[2] F и определён однозначно по модулю минимального многочлена μ_F оператора F. Если известно разложение характеристического многочлена оператора F в

[1] т. е. все слагаемые вида $\mathbb{C}[t]/\big((t-\lambda)^k\big)$

[2] в частности, значения $f(F) = P_{f,F}(F)$ и $f(G) = P_{f,G}(G)$ одной и той же функции f на разных операторах F и G получаются подстановкой этих операторов в *разные* интерполяционные многочлены $P_{f,F} \not\equiv P_{f,G} \mod \big(\mu_F\big)$

произведение степеней различных линейных двучленов: $\chi_F = \prod\limits_{\lambda\in\operatorname{Spec} F} (t-\lambda)^{N_\lambda}$, то в качестве $P_{f,F}$ годится единственный многочлен степени $\deg P_{f,F} < \deg \chi_F = \dim V$, имеющий $P^{(k)}_{f,F}(\lambda) = f^{(k)}(\lambda)$ для каждого $\lambda \in \operatorname{Spec} F$ при всех $0 \leqslant k \leqslant N_\lambda - 1$. Действительно, так как число N_λ, равное сумме показателей всех элементарных делителей $(t-\lambda)^m \in \mathcal{E}\ell\, F$, не меньше числа m_λ, равного максимальному из этих показателей, класс этого многочлена удовлетворяет условиям теор. 11.3.

Пример 11.4 (степенная функция и рекуррентные уравнения)
Задачу отыскания n-того члена числовой последовательности $z_n \in \mathbb{C}$, удовлетворяющей рекуррентному уравнению m-того порядка $z_n = \alpha_1 z_{n-1} + \alpha_2 z_{n-2} + \cdots + \alpha_m z_{n-m}$, если заданы её начальные m членов $(a_0, a_1, \ldots, a_{m-1})$, сводится к задаче вычисления n-той степени $m\times m$-матрицы

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_m \\ 1 & 0 & \ddots & 0 & \alpha_{m-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \alpha_2 \\ 0 & \cdots & 0 & 1 & \alpha_1 \end{pmatrix}$$

поскольку умножение фрагмента из m идущих подряд членов последовательности z_n справа на матрицу S приводит к сдвигу этого фрагмента на единицу вправо:

$$(z_{k+1}, z_{k+2}, \ldots, z_{k+m})\cdot S = (z_{k+2}, z_{k+3}, \ldots, z_{k+m+1}).$$

Таким образом, n-тый член последовательности z_n равен первой координате вектора

$$(a_0, a_1, \ldots, a_{m-1})\cdot S^n = (z_n, z_{n+1}, \ldots, z_{n+m-1}).$$

Согласно теор. 11.3 $S^n = P_{f,F}(S)$, где $P_{f,S} \in \mathbb{C}[z]$ — интерполяционный многочлен для вычисления функции $f(z) = z^n$ на матрице S.

Проиллюстрируем сказанное на примере матрицы $S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, задающей сдвиг в последовательности Фиббоначчи[1], что определяется уравнением $z_n = z_{n-1} + z_{n-2}$. Корни характеристического многочлена

$$\chi_S(t) = \det\begin{pmatrix} t & -1 \\ -1 & t-1 \end{pmatrix} = t^2 - t - 1 = (t-\lambda_+)(t-\lambda_-)$$

суть $\lambda_\pm = (1\pm\sqrt{5})/2$. Значения функции $f(z) = z^n$ на них суть $f(\lambda_\pm) = \lambda_\pm^n$. Коэффициенты интерполяционного многочлена $P_{f,S}(t) = at + b$ находятся из уравнений

$$\begin{cases} a\,\lambda_+ + b = \lambda_+^n \\ a\,\lambda_- + b = \lambda_-^n. \end{cases}$$

и равны $a = (\lambda_+^n - \lambda_-^n)/(\lambda_+ - \lambda_-)$, $b = \lambda_+^n - a\,\lambda_+ = (\lambda_+^{n-1} - \lambda_-^{n-1})(\lambda_+ - \lambda_-)$. Таким образом,

$$S^n = aS + bE = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}$$

[1] сравните это вычисление с проделанным ранее в n° 4.3.1 на стр. 54

Для классического начала $z_0 = 0$, $z_1 = 1$ получаем $\begin{pmatrix} z_n, z_{n+1} \end{pmatrix} = (0,1) \cdot S^n = (a, a+b)$, т. е.

$$z_n = a = \frac{\Big((1+\sqrt{5})/2\Big)^n - \Big((1-\sqrt{5})/2\Big)^n}{\sqrt{5}}.$$

Отметим, что знание матрицы S^n позволяет без дополнительных вычислений находить n-тый член последовательности, удовлетворяющей тому же рекуррентному уравнению, но имеющей другое начало.

Предложение 11.9
Спектр оператора $f(F)$ состоит из чисел $f(\lambda)$ с $\lambda \in \operatorname{Spec} F$. Если $f'(\lambda) \neq 0$, то элементарные делители $(t-\lambda)^m \in \mathcal{E}\ell(F)$ биективно соответствуют элементарным делителям $\big(t - f(\lambda)\big)^m \in \mathcal{E}\ell\big(f(F)\big)$ оператора $f(F)$. Если $f'(\lambda) = 0$, то элементарные делители вида $(t-\lambda)^m \in \mathcal{E}\ell(F)$, имеющие $m > 1$, распадаются в объединения элементарных делителей $\big(t - f(\lambda)\big)^\ell \in \mathcal{E}\ell\big(f(F)\big)$, имеющих $\ell < m$.

Доказательство. Из доказательства теор. 11.3 вытекает, что диагональная и нильпотентная составляющие ограничения оператора $f(F)$ на подмодуль $(t-\lambda)$-кручения равны, соответственно, $f_s(F) = f(\lambda) \cdot \mathrm{Id}$ и $f_n(F) = f'(\lambda) \cdot \eta + \frac{1}{2} f''(\lambda) \cdot \eta^2 + \cdots$, где через η обозначен нильпотентный оператор умножения на $(t-\lambda)$. На каждом слагаемом $\mathbb{C}[t]/\big((t-\lambda)^k\big)$ оператор η имеет ровно одну жорданову цепочку максимальной длины k. Если $f'(\lambda) \neq 0$, то $f_n^{k-1}(F) = f'(\lambda)^{m-1} \cdot \eta^{k-1} \neq 0$. Поэтому $f_n(F)$ тоже имеет ровно одну жорданову цепочку длины k. При $f'(l) = 0$ и $m > 1$ равенство $f_n^m(F) = 0$ наступит при $m < k$, так что цикловой тип N будет состоять из нескольких жордановых цепочек. □

11.5.2. Аналитический подход к распространению гомоморфизма вычисления многочленов на матрице $F \in \mathrm{Mat}_n(\mathbb{C})$ с алгебры $\mathbb{C}[z]$ на бóльшую алгебру функций $\mathcal{C} \supset \mathbb{C}[z]$ состоит в том, чтобы наделить пространства $\mathbb{C}[z]$ и $\mathrm{Mat}_n(\mathbb{C})$ той или иной топологией, представить функцию $f \in \mathcal{C}$ как предел последовательности многочленов и определить $f(F)$ как предел последовательности операторов $f_n(F) \in \mathrm{End}(V)$, после чего проверить, что $f(F)$ зависит только от f, а не от выбора сходящейся к f последовательности многочленов, а полученное отображение $\mathrm{ev}_F : \mathcal{C} \to \operatorname{End} V$ является гомоморфизмом алгебр[1]. Однако, как бы ни определялась сходимость в пространстве функций и какой бы ни была сходящаяся к функции f последовательность многочленов f_n, последовательность операторов $f_n(F)$ всегда лежит в конечномерном векторном пространстве, порождённом степенями F^m с $0 \leqslant m < \dim V$, и если переход к пределу в пространстве матриц перестановочен со сложением и умножением на константы[2], то предел последовательности $f_n(F)$ неминуемо будет *многочленом* от F степени, меньшей чем $\dim V$. Это означает, что какая бы аналитическая процедура не применялась для построения гомоморфизма $\mathrm{ev}_F : \mathcal{C} \to \mathrm{Mat}_n(\mathbb{C})$, значение этого гомоморфизма на заданной функции f *a priori* вычисляется по теор. 11.3.

[1] в качестве упражнения по анализу читателю настоятельно рекомендуется попробовать самостоятельно реализовать эту программу, используя на пространстве функций топологию, в которой сходимость последовательности функций означает равномерную сходимость в каждом круге в $\mathbb{C}$, а на пространстве $\mathrm{Mat}_n(\mathbb{C})$ — стандартную топологию пространства $\mathbb{C}^{n^2}$, где сходимость определяется покоординатно

[2] т. е. $\lim\limits_{n\to\infty} (\lambda F_n + \mu G_n) = \lambda \lim\limits_{n\to\infty} F_n + \mu \lim\limits_{n\to\infty} G_n$

Отметим также, что если операторы $F : V \to V$ и $G : W \to W$ подобны, т. е. $G = CFC^{-1}$ для некоторого изоморфизма $C : V \xrightarrow{\sim} W$, то и функции от них подобны: $f(G) = Cf(F)C^{-1}$, поскольку соотношение $f_n(G) = Cf_n(F)C^{-1}$ выполнено для всех многочленов, приближающих функцию f, а стало быть, останется выполненным и в пределе, при условии, что топология на пространствах $\operatorname{End} V$ и $\operatorname{End} W$ такова, что все *линейные* отображения $\operatorname{End} V \to \operatorname{End} W$ непрерывны.

Ответы и указания к некоторым упражнениям

Упр. 1.1. Ответ: 2^n.

Упр. 1.2. Ответ на второй вопрос: нет. Решение: пусть $X = \{1, 2\}$, $Y = \{2\}$; тогда все возможные значения пересечений и объединений между ними суть

$$X \cap Y = Y \cap Y = Y \cup Y = Y$$
$$X \cup Y = X \cup X = X \cap X = X$$

и любая формула, составленная из X, Y, $\cap$ и $\cup$, даст на выходе либо $X = \{1, 2\}$, либо $Y = \{2\}$, тогда как $X \setminus Y = \{1\}$.

Упр. 1.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. 1.5. Если множество X конечно, всякое отображение $X \to X$, которое инъективно или сюръективно, автоматически биективно. Если множество X бесконечно, то оно содержит подмножество, изоморфное $\mathbb{N}$, а у $\mathbb{N}$ есть инъективные небиективные эндоморфизмы (например, $n \mapsto (n+1)$) и сюръективные небиективные эндоморфизмы (например, $1 \mapsto 1$ и $n \mapsto (n-1)$ при $n \geqslant 2$), и их можно продолжить до эндоморфизмов $X \to X$ тождественным действием на $X \setminus \mathbb{N}$.

Упр. 1.6. Ответ: нет. Воспользуйтесь рассуждением Кантора: предположите, что все биекции $\mathbb{N} \to \mathbb{N}$ можно занумеровать натуральными числами, и, пользуясь этим списком, постройте биекцию, которая при каждом $k = 1, 2, 3, \ldots$ отображает число $k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 1.7. Ответ: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(k_1, k_2, \ldots, k_m)$ с суммой $\sum k_i = n$. Такой набор можно закодировать словом, составленным из $(m-1)$ букв 0 и n букв 1 : сначала пишем k_1 единиц, потом нуль, потом k_2 единиц, потом нуль, и т. д. (слово кончится k_m единицами, стоящими следом за последним, $(m-1)$-м нулём).

Упр. 1.8. Ответ: $\binom{n+k}{k}$. Каждая такая диаграмма представляет собою ломаную, ведущую из левого нижнего угла прямоугольника в правый верхний. В такой ломаной ровно n горизонтальных звеньев и ровно k вертикальных.

Упр. 1.9. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \ell \in \mathbb{Z}$. Тогда $x' + y' = x + y + n(k + \ell)$ и $x'y' = xy + n(\ell x + ky + k\ell n)$ сравнимы по модулю n с $x + y$ и xy соответственно, т. е. $[x' + y']_n = [x + y]_n$ и $[x'y']_n = [xy]_n$.

Упр. 1.10. Рефлексивность и симметричность очевидны. Транзитивность: если $(p, q) \sim (r, s)$ и $(r, s) \sim (u, w)$, т. е. $ps - rq = 0 = us - rw$, то $psw - rqw = 0 = usq - rwq$, откуда $s(pw - uq) = 0$, и $pw = uq$, т. е. $(p, q) \sim (u, w)$.

Упр. 1.11. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi/2$, то отражение относительно ℓ_1, а потом отражение относительно ℓ_2 — это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно ℓ_1 и ℓ_2 коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. 1.12. а) $\Rightarrow$ б). Левое обратное к вложению $f : X \hookrightarrow Y$ должно переводить $y = f(x) \in \operatorname{im} f$ в x, а на элементах $Y \setminus \operatorname{im} f$ может действовать как угодно. В частности, ответ на последний вопрос задачи — $(m-n)^n$.

б) ⇒ в). Равенство $g_1 = g_2$ получается из равенства $fg_1 = fg_2$ умножением обеих частей слева на любое левое обратное к f отображение.
в) ⇒ а). Если $f(x_1) = f(x_2)$ для каких-то $x_1 \neq x_2$, положим $g_1 = \mathrm{Id}_X$, а в качестве g_2 возьмём автоморфизм $X \to X$, который меняет между собой точки x_1 и x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$.

Упр. 1.13. Аналогично предыдущему упр. 1.12.

Упр. 1.14. Таблица композиций gf в симметрической группе S_3:

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

Упр. 2.2. Ответы: $1 + x$ и $xy + x + y$.

Упр. 2.3. При умножении числителя и знаменателя любой из дробей в левых частях равенств форм. (2-11) на стр. 17 на одно и то же число c, числитель и знаменатель дроби в правой части соответствующего равенства также умножатся на c. Отсюда следует корректность. Проверка выполнения аксиом бесхитростна.

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

Упр. 2.8. Существование. Если число n простое, то оно само и будет своим разложением; если n составное, представим его в виде произведения строго меньших по абсолютной величине чисел, которые в свою очередь или неприводимы или являются произведениями строго меньших по абсолютной величине чисел и т. д. Поскольку модуль целого числа нельзя бесконечно долго уменьшать, мы в конце концов получим требуемое разложение.

Единственность. Для любого простого числа p и любого целого числа z выполняется следующая альтернатива: либо нод$(z, p) = |p|$, и тогда z делится на p, либо нод$(z, p) = 1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ все сомножители просты. Поскольку $\prod q_i$ делится на p_1, число p_1, в силу лем. 2.3, не может быть взаимно просто с каждым q_i. Согласно упомянутой выше альтернативе, найдётся q_i (можно считать, что q_1) который делится на p_1. Поскольку q_1 прост, $q_1 = \pm p_1$. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.10. Класс $\binom{mp^n}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему после раскрытия скобок и приведения подобных слагаемых в биноме $(1 + x)^{mp^n}$ над полем $\mathbb{F}_p$. Последовательно применяя формулу форм. (2-19) на стр. 23, получаем

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

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

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

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

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

Упр. 3.3. Ответ: $(y^n - x^n)/(y-x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \cdots + yx^{n-2} + x^{n-1}$.

Упр. 3.5. Если $f(x) = \sum a_k x^k$, то $f(x+t) = \sum\limits_{k,\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu}t^\nu = \sum\limits_{\nu} t^\nu \cdot f_\nu(x)$, где

$$f_\nu(x) = \sum_{k\geqslant\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu} = \frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0} a_k x^k.$$

Упр. 3.7. Годятся дословно те же аргументы, что и в упр. 2.8.

Существование. 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.

Единственность. Для любого приведённого неприводимого многочлена p и любого многочлена g выполняется следующая альтернатива: либо $\text{нод}(p, g) = p$, и тогда g делится на p, либо $\text{нод}(p, g) = 1$, и тогда g взаимно прост с p. Пусть в равенстве

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

все сомножители неприводимы. Деля p_1 на старший коэффициент, мы можем считать, что он приведён. Поскольку $\prod q_i$ делится на p_1, многочлен p_1, в силу лем. 2.3, не может быть взаимно прост с каждым q_i. Согласно упомянутой выше альтернативе, найдётся q_i (скажем, q_1), который делится на p_1. Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 3.10. Единственность вытекает из сл. 3.2: разность двух многочленов степени n, принимающих одинаковые значения в $n+1$ точках, обращается в нуль в этих $n+1$ точках, т. е. имеет $n+1$ разных корней, что возможно только если эта разность нулевая. Существование: приведённый многочлен степени n, равный нулю во всех точках a_ν кроме i-той, есть $\prod\limits_{\nu\neq i}(x - a_\nu)$. Деля этот многочлен на его значение в точке a_i, получаем многочлен $f_i(x) = \prod\limits_{\nu\neq i}(x-a_\nu)/\prod\limits_{\nu\neq i}(a_i - a_\nu)$, такой что

$$f_i(a_\nu) = \begin{cases} 1, \text{ при } \nu = i \\ 0, \text{ при } \nu \neq i. \end{cases}$$

Таким образом, искомый многочлен равен $\sum_{i=0}^{n} b_i \cdot f_i(x) = \sum_{i=0}^{n} b_i \prod_{\nu\neq i}(x-a_\nu)/(a_i-a_\nu)$.

Упр. 3.11. Если многочлен степени $\leqslant 3$ приводим, то он имеет делитель степени один, корень которого будет корнем исходного многочлена.

Упр. 3.12. См. упр. 1.9 на стр. 11.

Упр. 3.13. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x-\alpha)$ в качестве констант сюръективно, поскольку число $\alpha \in \Bbbk$ переходит в класс $[x]$, и значит, для любого $g \in \Bbbk[x]$ число $g(\alpha)$ переходит в класс $[g]$.

Упр. 3.14. Обратным элементом к произвольному ненулевому $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ является $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Кольцо в (а) содержит делители нуля: $[t+1]\cdot[t^2-t+1] = [0]$ и, тем самым, не является полем. Кольцо в (б) является полем: многочлен $p = \vartheta^3 + 2$ не имеет корней в $\mathbb{Q}$, и значит, не делится в $\mathbb{Q}[x]$ ни на какой многочлен первой или второй степени; следовательно, p взаимно прост со всеми $g \in \mathbb{Q}[x]$, не делящимися на p, т. е. для любого $[g] \neq [0]$ существуют $h_1, h_2 \in \mathbb{Q}[x]$, такие что $h_1 g + h_2 p = 1$; тем самым, $[h_1] = [g]^{-1}$.

Упр. 3.15. Указание: достаточно рассмотреть случай $a_1 = 1$ и найти обратные ко всем элементам $\vartheta - a$; для этого воспользуйтесь алгоритмом Евклида (см. n° 3.2.2): класс $h(\vartheta)$, обратный к классу $\vartheta - a$, задаётся таким многочленом $h \in \mathbb{Q}[x]$, что

$$h(x)(x-a) + g(x)(x^2+x+1) = 1$$

для некоторого $g \in \mathbb{Q}[x]$; остаток от деления x^2+x+1 на $x-a$ равен a^2+a+1, так что алгоритм Евклида остановится уже на втором шагу.

Упр. 3.17. Число $\zeta = \cos(2\pi/5) + i\cdot\sin(2\pi/5)$ является корнем многочлена

$$z^5 - 1 = (z-1)(z^4+z^3+z^2+z+1).$$

Уравнение $z^4+z^3+z^2+z+1 = 0$ можно решить в радикалах, деля обе части на z^2 и вводя новую переменную $t = z + z^{-1}$.

Упр. 3.18. Пусть $\zeta = \zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Докажите более сильное утверждение: среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ, которые делятся на $\text{нод}(k,n)$, ибо равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$.

Упр. 3.19. См. листок № $3\frac{2}{3}$.

Упр. 3.20. Из равенства $z_1 z_2 = 1$ вытекает равенство $|z_1|\cdot|z_2| = 1$ на длины. Поскольку гауссово число $z \neq 0$ имеет $|z|^2 \in \mathbb{N}$, обратимым может быть только z с $|z| = 1$. Таких чисел в $\mathbb{Z}[i]$ ровно четыре: ± 1 и $\pm i$, и все они обратимы.

Упр. 3.23. Это сразу следует из теоремы сл. 6.1 на стр. 90 о существовании базиса в конечномерном векторном пространстве: если $\operatorname{char}\mathbb{F} = p$, то $\mathbb{F} \supset \mathbb{F}_p$ и является конечномерным векторным пространством над $\mathbb{F}_p$. Выбирая в нём базис $e_1, e_2, \ldots, e_n$, заключаем, что $\mathbb{F}$ состоит из p^n векторов $x_1e_1 + x_2e_2 + \cdots + x_ne_n$, где каждый коэффициент x_i независимо пробегает $\mathbb{F}_p$ (см. прим. 6.10 на стр. 91). Менее геометрическое решение заключается в том, чтобы получить конечное поле $\mathbb{F}$ последовательными расширениями простого подполя $\mathbb{F}_p \subset \mathbb{F}$. Каждый шаг этого построения заключается в присоединении к очередному, уже

построенному полю $\mathbb{F}'$, такому что $\mathbb{F}_p \subset \mathbb{F}' \subset \mathbb{F}$, какого-нибудь элемента $\zeta \in \mathbb{F} \smallsetminus \mathbb{F}'$. Число элементов в получающемся поле $\mathbb{F}[\zeta] \supset \mathbb{F}'$ является n-той степенью числа элементов в поле $\mathbb{F}'$, откуда нужное утверждение следует по индукции.

Упр. 3.24. Равенство $(b_1 b_2)^k = 1$ равносильно равенству $b_1^k = b_2^{m_2-k}$. Тогда

$$b_2^{m_1(m_2-k)} = b_1^{m_1 k} = 1\,,$$

откуда $m_1(m_2 - k)$ делится на m_2, а значит, k делится на m_2 . В силу симметрии между b_1 и b_2, показатель k делится также и на m_1. А так как m_1 и m_2 взаимно просты, k делится на $m_1 m_2$. Поскольку $(b_1 b_2)^{m_1 m_2} = 1$, $\operatorname{ord}(b_1 b_2) = m_1 m_2$.

Упр. 3.25. Надо отправить в ℓ_1 все простые делители числа m_1, входящие в разложение числа m_1 в бóльшей степени, чем в разложение числа m_2.

Упр. 3.26. Если $g(x) = h_1(x) \cdot h_2(x)$, то $h_1(\zeta) = 0$ или $h_2(\zeta) = 0$, поэтому степень одного из сомножителей не меньше, чем $\deg g$. Если $f(\zeta) = 0$, то деля f на g с остатком: $f = gh + r$, и вычисляя при $x = \zeta$, получаем $r(\zeta) = 0$. Так как $\deg r < \deg g$, заключаем, что $r = 0$.

Упр. 3.27. Запишите элементы поля $\mathbb{F}_p$ в строку вида:

$$-[(p-1)/2]\,,\ \ldots\,,\ -[1]\,,\ [0]\,,\ [1]\,,\ \ldots\,,\ [(p-1)/2]$$

и покажите, что[1] $a \in \mathbb{F}_p^*$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» от умножения на a, чётно, после чего примените это к $a = 2$.

Упр. 4.3. Равенство несократимых записей $p/q = r/s$ означает равенство $ps = qr$, в котором p взаимно просто с q, а s взаимно просто с r. Из лем. 2.3 следует, что в этом случае $p = rf$, а $q = sg$, откуда $frs = grs$ и $f = g$. Поскольку запись p/q предполагалась несократимой, $\deg f = 0$.

Упр. 4.5. Согласно правилу дифференцирования композиции $\left(f^m\right)' = m \cdot f^{m-1} \cdot f'$, имеем $\frac{d}{dx}(1-x)^{-m} = \left(\left(\frac{1}{1-x}\right)^m\right)' = m(1-x)^{-m-1}$, откуда нужная формула легко получается по индукции.

Упр. 4.7. Продифференцируйте обе части.

Упр. 4.9. Линейность отображений $f(D)$ следует из линейности отображения D и того, что суммы и композиции линейных отображений также являются линейными отображениями.

Упр. 4.11. Ответы: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$, $a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30$$
$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12$$
$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500\,.$$

Упр. 4.13. $\nabla(x^n) = (-1)^n n x^{n-1} +$ младшие члены , $D = -\ln(1-\nabla) = -\sum\limits_{k\geqslant 1} \nabla^k/k$.

[1] это утверждение известно как *лемма Гаусса о квадратичных вычетах*

Упр. 4.14. Первое вытекает из рекурсивной формулы для биномиальных коэффициентов

$$\binom{x+k-1}{k-1} + \binom{x+k-1}{k} = \binom{x+k}{k}.$$

Если $f = \sum\limits_{\nu} c_\nu \gamma_\nu$, то $\nabla^k f(-1) = \sum\limits_{\nu} c_\nu \gamma_{\nu-k}(-1) = c_k$, поскольку $\gamma_m(-1) = 0$ при $m \neq 0$. Существование разложения устанавливается индукцией по $n = \deg f$: пусть $g = \sum\limits_{k=0}^{n} \nabla^k f(-1)\gamma_k$. Тогда $g(-1) = f(-1)$ и, т. к. $\deg \nabla f < n$, по индукции $\nabla f = \sum\limits_{k=0}^{n-1} \nabla^{k+1} f(-1)\gamma_k = \nabla g$; тем самым f и g принимают равные значения во всех целых точках, а значит, $f = g$ в $\mathbb{Q}[x]$.

Упр. 4.15. Надо подобрать многочлены $p_i, q_i \in \Bbbk[x]$ ограниченной степени так, чтобы ряды

$$P(t,x) = p_0(x) + p_1(x)\,t + p_2(x)\,t^2 + \cdots \quad \text{и} \quad Q(t,x) = q_0(x) + q_1(x)\,t + q_2(x)\,t^2 + \cdots,$$

удовлетворяли равенству $AP + BQ = 1$. Приравняем у обеих частей коэффициенты при t^k:

$$\begin{aligned} a_0\,p_0 + b_0 q_0 &= 1 && \text{(при } k = 0\text{)} \\ a_0 p_k + b_0 q_k &= -\sum_{i=1}^{k-1} (a_i p_{k-i} + b_i q_{k-i}) && \text{(при } k \geqslant 1\text{)}. \end{aligned}$$

Так как a_0 и b_0 взаимно просты, и $\deg a_i < \deg a_0$, $\deg b_i < \deg b_0$ при всех $i > 0$, написанные соотношения однозначно определяют многочлены p_i и q_i степеней, строго меньших, чем $\deg a_0$ и $\deg b_0$ соответственно.

Упр. 4.16. Если m и $\vartheta(t)$ решают модифицированную задачу, то для первой модификации они же решают и исходную задачу, а для второй и третьей модификаций решение исходной задачи даётся тем же m и рядами $\vartheta(t)/a_n(t^q)$ и $\vartheta(t) + a_{n-1}(t^q)/n$ соответственно.

Упр. 4.17. Пусть многочлен $f(x) = a_0(t) + a_1(t)\,x + \cdots + a_n(t)\,x^n$ имеет коэффициенты $a_i(t)$ в поле рядов Пюизо. Обозначим общий знаменатель всех показателей всех рядов a_i через m и положим $t = u^m$. Тогда $a_i(t) = a_i(u^m) \in \Bbbk((u))$ и по лем. 4.5 после ещё одной подстановки $u = s^q$ у многочлена f появится корень в поле $\Bbbk((s))$. Возвращаясь к старому параметру $t = s^{qm}$ получаем корень многочлена f в виде ряда Пюизо от $t^{\frac{1}{qm}}$.

Упр. 4.19. Утверждение (а) очевидно. В (б) длины горизонтальных проекций всех рёбер ломаной Ньютона для уравнения на x_1 строго меньше длины ℓ горизонтальной проекции ребра, выбранного для отыскания ε_1, всегда, кроме случая, когда c_1 является ℓ-кратным корнем многочлена $f_\gamma(x,1)$. В этом случае $f_\gamma(x,1) = \alpha \cdot (x - c_1)^\ell$, где α — ненулевая константа. Поэтому выбранное ребро содержит все без исключения мономы x^ν с $0 \leqslant \nu \leqslant \ell$, а значит, вектор нормали к этому ребру имеет координаты $(d, 1)$ с $d \in \mathbb{N}$, откуда $\varepsilon_1 = d \in \mathbb{N}$.

Из (а), (б) и (в) вытекает, что всякий раз, когда ε_i не является целым, максимальная из длин горизонтальных проекций рёбер ломаной Ньютона для уравнения на x_i будут строго меньше, чем на предыдущем шаге. Поэтому в последовательности ε_i имеется лишь конечное число нецелых показателей, и у них есть общий знаменатель.

Упр. 5.1. Импликации (а)⇒(б)⇒(в) очевидны. Если $s \in I$ обратим, то среди его кратных есть единица, а среди её кратных — все элементы кольца. Значит, (в)⇒(а).

Упр. 5.2. Первое утверждение очевидно, во втором можно взять $M = I$.

Упр. 5.3. Если a и b являются старшими коэффициентами многочленов $f(x)$ и $g(x)$ из идеала I, причём $\deg f = m$ и $\deg g = n$, где $m \geqslant n$, то $a + b$ либо равно нулю, либо является старшим коэффициентом многочлена $f(x) + x^{m-n} \cdot g(x) \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 5.4. Повторите доказательство теор. 5.1, следя за младшими коэффициентами вместо старших.

Упр. 5.6. Обозначим через I_0 идеал, образованный всеми аналитическими функциями[1], обращающимися в нуль на множестве $\mathbb{Z} \subset \mathbb{C}$, а через I_k — идеал всех функций, обращающихся в нуль на множестве $\mathbb{Z} \smallsetminus \{1, 2, \ldots, k\}$. Убедитесь, что $\sin(2\pi z) / \prod\limits_{\alpha=1}^{k} (z - \alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 5.7. Из того, что I является абелевой подгруппой в K немедленно вытекает, что отношение $a_1 \equiv a_2 \pmod{I}$ рефлексивно, транзитивно и симметрично. Корректность операций проверяется так же, как в упр. 1.9: если $[a']_I = [a]_I$ и $[b']_I = [b]_I$, т. е. $a' = a + x$, $b' = b + y$ с некоторыми $x, y \in I$, то $a' + b' = a + b + (x + y)$ и $a'b' = ab + (ay + bx + xy)$ сравнимы по модулю I с $a + b$ и ab соответственно, поскольку суммы в скобках лежат в I (именно в этот момент мы пользуемся тем, что идеал вместе с каждым элементом содержит и все его кратные); таким образом, $[a' + b']I = [a + b]_I$ и $[a'b']_I = [ab]_I$.

Упр. 5.8. Рассмотрим эпиморфизм факторизации $\pi : K \twoheadrightarrow K/I$. Полный прообраз $\pi^{-1}(J)$ любого идеала $J \subset K/I$ является идеалом в K. Классы элементов, порождающих этот идеал в K порождают идеал J в K/I.

Упр. 5.9. Множество отличных от всего кольца идеалов, содержащих данный идеал J непусто, частично упорядочено по включению, и любое семейство вложенных друг в друга идеалов из этого множества содержится в идеале, полученном объединением всех идеалов семейства. По лемме Цорна[2] в нём найдётся такой идеал $I \supset J$, что для любого элемента $a \in K \smallsetminus I$, идеал $(a, I) \supsetneq I$ будет совпадать со всем кольцом.

Упр. 5.10. Всякий идеал в $\mathbb{C}[x]$ является главным. Если фактор кольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. Для ответа на второй вопрос подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 5.11. С помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $X \to \mathbb{R}$ на произвольном компакте X найдётся точка $p \in X$, в которой все функции из идеала обращаются в нуль, что даёт включение $I \subset \ker \mathrm{ev}_p$.

Упр. 5.13. Если в каждом из идеалов $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ имеется элемент $x_\nu \in \mathfrak{a}_\nu \smallsetminus \mathfrak{p}$, то произведение этих элементов $x_1 x_2 \ldots x_m \in \bigcap \mathfrak{a}_\nu \subset \mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

Упр. 5.15. Если $\exists\, b^{-1}$, то $v(ab) \leqslant v(abb^{-1}) = v(a)$. Наоборот, если $v(ab) = v(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $v(r) < v(ab) = v(a)$, либо $r = 0$. Из равенства $r = a(1 - bq)$ вытекает, что либо $v(r) \geqslant v(a)$, либо $1 - bq = 0$. С учётом предыдущего, такое

[1] функция $\mathbb{C} \to \mathbb{C}$ называется *аналитической*, если она задаётся сходящимся всюду в $\mathbb{C}$ степенным рядом из $\mathbb{C}[\![z]\!]$

[2] другие примеры использования леммы Цорна см. в зам. 6.4. на стр. 91

возможно только при $1-bq=0$ или $r=0$. Во втором случае $a(1-bq)=0$, что тоже влечёт $1-bq=0$. Следовательно $bq=1$ и b обратим.

Упр. 5.16. Если $b=ax$ и $a=by=axy$, то $a(1-xy)=0$, откуда $xy=1$.

Упр. 5.17. Многочлены x и y не имеют в $\mathbb{Q}[x,y]$ никаких общих делителей, кроме констант. Общими делителями элементов 2 и x в $\mathbb{Z}[x]$ являются только ±1.

Упр. 5.18. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta=a+b\sqrt{5}$ число $\overline{\vartheta}=a-b\sqrt{5}$, и будем называть *нормой* числа $\vartheta=a+b\sqrt{5}$ целое число $||\vartheta||=a^2-5b^2=\vartheta\cdot\overline{\vartheta}$. Легко видеть, что $\overline{\vartheta_1\vartheta_2}=\overline{\vartheta}_1\cdot\overline{\vartheta}_2$, так что $||\vartheta_1\vartheta_2||=\vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2=||\vartheta_1||\cdot||\vartheta_2||$. Поэтому $\vartheta\in\mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $||\vartheta||=\pm1$, и в этом случае $\vartheta^{-1}=\pm\overline{\vartheta}$. Поскольку $||2||=4$, а $||1\pm\sqrt{5}||=-4$, разложение этих элементов в произведение с необратимыми x и y возможно только, если $||x||=||y||=\pm2$. Однако элементов с нормой ±2 в $\mathbb{Z}[\sqrt{5}]$ нет, т. к. равенство $a^2-5b^2=\pm2$ при редукции по модулю 5 превращается в равенство $a^2=\pm2$ в поле $\mathbb{F}_5$, где ±2 не являются квадратами.

Упр. 5.20. Это следует из равенства $a_0q^n+a_1q^{n-1}p+\cdots+a_{n-1}qp^{n-1}+a_np^n=0$

Упр. 5.21. Ответ: $(x^2-2x+2)(x^2+2x+2)$.

Упр. 6.1. Пусть $0\cdot v=w$. Тогда $w+v=0\cdot v+1\cdot v=(0+1)\cdot v=1\cdot v=v$. Прибавляя к обеим частям этого равенства $-v$, получаем $w=0$. Из равенства $0\cdot v=0$ вытекает, что $\lambda\cdot0=\lambda(0\cdot v)=(\lambda\cdot0)\cdot v=0\cdot v=0$. Наконец, равенство $(-1)\cdot v+v=(-1)\cdot v+1\cdot v=((-1)+1)\cdot v=0\cdot v=0$ означает, что $(-1)\cdot v=-v$.

Упр. 6.3. По индукции проверяется, что каждый моном x^m (где $m=0,1\ldots,n$) линейно выражается через многочлены $f_0,f_1,\ldots,f_m$, а значит, и любой многочлен степени $\leqslant m$ линейно выражается через $f_0,f_1,\ldots,f_m$. Для доказательства единственности такого выражения заметим, что в равенстве $\sum\lambda_if_i=\sum\mu_if_i$ старший моном x^n появляется в обеих частях только из многочлена f_n. Поэтому сравнение коэффициента при x^n в обеих частях приводит к равенству $\lambda_n=\mu_n$. Вычитая из обеих частей $\lambda_nf_n=\mu_nf_n$, получаем равенство между многочленами меньшей степени, к которому применимо то же рассуждение.

Упр. 6.4. Пространство со счётным базисом равномощно множеству конечных слов, составленных из элементов основного поля, а пространство рядов равномощно множеству бесконечных последовательностей элементов основного поля, которое строго более мощно, чем множество конечных слов.

Упр. 6.7. Ответ: нет из соображений размерности.

Упр. 6.8. Пусть какая-то конечная линейная комбинация векторов из объединения всех наборов обратилась в нуль. Каждый вектор из этой комбинации лежит в одном из наборов цепочки, а значит, и все они лежат в одном из наборов цепочки (том, что содержит остальные — такой существует, поскольку про любые два набора цепочки известно, что один из них является подмножеством другого). Так как каждый набор из цепочки предполагался линейно независимым, все коэффициенты этой линейной комбинации нулевые.

Упр. 6.9. Рассмотрим множество всех пар (G,E), таких что $G\subset\mathcal{G}$, $E\subset\mathcal{E}$, G равномощно E, и после замены в $\mathcal{G}$ векторов из G на векторы из E набор остаётся порождающим. Первый шаг доказательства лем. 6.2 показывает, что это множество пар непусто. Введём на нём частичный порядок, полагая $(G,E)\leqslant(G',E')$, если $G\subset G'$ и $E\subset E'$. Поскольку любая линейно упорядоченная цепочка пар мажорируется парой, у которой G- и E-множества

являются объединениями всех G- и E-множеств рассматриваемой цепочки, по лемме Цорна найдётся пара (G, E), не содержащаяся строго ни в какой большей паре. Если при этом $E \neq \mathcal{E}$, то же рассуждение, что и в доказательстве лем. 6.2 позволит добавить к множествам G и E ещё по одному элементу, что противоречит максимальности пары (G, E).

Упр. 6.12. Это частный случай предл. 7.2 на стр. 106.

Упр. 6.13. Это следует из теор. 7.1 на стр. 107.

Упр. 6.14. Пусть $W \not\subseteq U$ два подпространства в V. Выберем вектор $w \in W \setminus U$. Если $W \cup U$ — подпространство, то $\forall\, u \in U \;\; w + u \in W \cup U$. Поскольку $w + u \notin U$ (т. к. $w \notin U$), $w + u \in W$, откуда $u \in W$, т. е. $U \subset W$.

Упр. 6.15. Каждый вектор $w \in V$ представляется в виде $w = \frac{\xi(w)}{\xi(v)} \cdot v + u$, где $u = w - \frac{\xi(w)}{\xi(v)} \cdot v$ лежит в $\ker \xi$, поскольку $\xi\left(w - \frac{\xi(w)}{\xi(v)} \cdot v\right) = \xi(w) - \frac{\xi(w)}{\xi(v)} \cdot \xi(v) = 0$.

Упр. 6.16. Индукция по числу подпространств с использованием разобранного перед этим случая двух подпространств.

Упр. 6.17. Поскольку каждый вектор $v \in V$ имеет единственное представление в виде $v = \sum u_i$ с $u_i \in U_i$, гомоморфизм *сложения* $\bigoplus U_i \to V$, $(u_1, u_2, \dots, u_m) \mapsto \sum u_i$, биективен.

Упр. 6.21. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала (ср. с упр. 5.7).

Упр. 6.23. Пусть $B \subset A_1 \cup A_2 \cup \ldots \cup A_m$. Переход к фактору по A_m и индукция по m сводят задачу к случаю $m = 2$. Если $B \subset A_1 \cup A_2$ и $b_1 \in (B \cap A_1) \setminus A_2$, $b_2 \in (B \cap A_2) \setminus A_1$, то $b_1 + b_2 \in B \supset A_1 \cup A_2$ не может лежать ни в A_1, ни в A_2, поскольку в $b_1 + b_2 \in A_1 \Rightarrow b_2 \in A_1$, а $b_1 + b_2 \in A_2 \Rightarrow b_1 \in A_2$ вопреки выбору b_1 и b_2.

Упр. 7.4. Набор $v_1, v_2, \dots, v_n \in V$ линейно независим, поскольку применяя ξ_i к обеим частям соотношения $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$ получаем $\lambda_i = 0$ (и так для каждого i). Поскольку $\dim V = n$, этот набор является базисом, тогда из условия вытекает, что ξ_i составляют двойственный базис, т. е. являются координатами вдоль v_i.

Упр. 7.5. Если линейная форма зануляется на неких векторах, то она зануляется и на любой их линейной комбинации.

Упр. 7.8. Типичный для алгебры перенос из левой части в правую:

$$\langle\, G^* F^* \xi\,,\, v\,\rangle = \langle\, F^* \xi\,,\, Gv\,\rangle = \langle\, \xi\,,\, FGv\,\rangle$$

Упр. 7.9. При проекции $c_I : \Bbbk^n \twoheadrightarrow E_I$ векторы w_i перейдут в строки этой подматрицы, и для того, чтобы $c_I|_U$ была изоморфизмом, необходимо и достаточно, чтобы размерность их линейной оболочки была r.

Упр. 7.10. Эквивалентность свойств (а) – (г) и единственность базиса (г) следуют из предл. 6.7 на стр. 100, применённой к подпространству $\operatorname{Ann} U \subset \Bbbk^{n*}$. Покажем, что $u_\mu^\perp = e^*_{j_\mu} + \tau_\mu$ с

$$\tau_\mu = -\sum_{\nu=1}^{r} \left\langle\, e^*_{j_\mu}\,,\, w_\nu \,\right\rangle \cdot e^*_{i_\nu}$$

составляют базис в $\operatorname{Ann} U$. Они лежат в $\operatorname{Ann} U$, поскольку

$$\left\langle u_\mu^\perp , u_\nu \right\rangle = \left\langle e^*_{j_\mu} + \tau_\mu \ , \ e_{i_\nu} + w_\nu \right\rangle = \left\langle e^*_{j_\mu} , w_\nu \right\rangle + \left\langle \tau_\mu , e_{i_\nu} \right\rangle =$$
$$= \left\langle e^*_{j_\mu} , w_\nu \right\rangle - \sum_{\alpha=1}^{r} \left\langle e^*_{j_\mu} , w_\alpha \right\rangle \cdot \left\langle e^*_\alpha , e_{i_\nu} \right\rangle = \left\langle e^*_{j_\mu} , w_\nu \right\rangle - \left\langle e^*_{j_\mu} , w_\nu \right\rangle = 0$$

и линейно независимы, так как $e^*_{j_\mu}$ линейно независимы.

Упр. 7.11. Векторы $u_\nu^\perp$ линейно независимы, поскольку базисный ковектор $e^*_{j_\nu}$ входит только в u_ν и не может быть сокращён никакой линейной комбинацией остальных u_μ. Они все лежат в $\operatorname{Ann} U$, так как

$$\left\langle u_\nu^\perp , u_\mu \right\rangle = \left\langle e^*_{j_\nu} - \sum_k \alpha_{kj_\nu} e^*_{i_k} , e_{i_\mu} + \sum_\ell \alpha_{\mu j_\ell} e_{j_\ell} \right\rangle = \alpha_{\mu j_\nu} \left\langle e^*_{j_\nu} , e_{j_\nu} \right\rangle - \alpha_{\mu j_\nu} \left\langle e^*_{i_\mu} , e_{i_\mu} \right\rangle = 0$$

Упр. 7.12. Поскольку пространство V^i порождается пространством V^{i+1} и вектором e_i, пространство $U \cap V^i$ содержится в линейной оболочке $U \cap V^{i+1}$ и вектора e_i, размерность которой, отличается от $\dim(U \cap V_{i+1})$ не больше, чем на единицу.

Упр. 7.13. Для такого подпространства $d_i = \dim \pi_i(U)$ равна числу ненулевых строк в подматрице, сосредоточенной в первых i столбцах.

Упр. 7.14. Если отнять из произвольной матрицы комбинаторного типа I матрицу E_I, в столбцах I которой стоит единичная $r \times r$ подматрица, а в остальных местах нули, получится матрица имеющая нули в столбцах I, а также при всех $\nu = 1, \ldots, r$ нули в строке ν в позициях с 1-й по i_ν-тую включительно. Такие матрицы составляют в $\operatorname{Mat}_{r\times n}(\Bbbk)$ векторное подпространство указанной коразмерности $r^2 + \sum\limits_{\nu=1}^{r} (i_\nu - \nu + 1)$.

Упр. 8.1. Первое доказывается выкладкой $0 \cdot a = (b + (-1) \cdot b)a = ba + (-1)ba = 0$, второе — выкладкой $e' = e' \cdot e'' = e''$.

Упр. 8.2. $E_{ij}E_{k\ell} = \begin{cases} E_{i\ell} & \text{при } j = k \\ 0 & \text{в остальных случаях} \end{cases}$. В частности, $E_{12}E_{21} \neq E_{21}E_{12}$. Полный список коммутационных соотношений таков:

$$[E_{ij}, E_{k\ell}] \stackrel{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{при } j = k \text{ и } i = \ell \\ E_{i\ell} & \text{при } j = k \text{ и } i \neq \ell \\ -E_{kj} & \text{при } j \neq k \text{ и } i = \ell \\ 0 & \text{в остальных случаях.} \end{cases}$$

Упр. 8.3. Пусть $AB = C$, $B^tA^t = D$, тогда $c_{ij} = \sum\limits_k a_{ik}b_{kj} = \sum\limits_k a^t_{ki}b^t_{jk} = \sum\limits_k b^t_{jk}a^t_{ki} = d_{ji}$.

Упр. 8.7. По по теореме о ранге матрицы[1] линейная зависимость строк $n \times n$-матрицы A равносильна линейной зависимости её столбцов и означает, что размерность образа линейного оператора $A : \Bbbk^n \to \Bbbk^n$ с матрицей A меньше n. Поэтому $\ker A \neq 0$, и стало быть оператор A не биективен, а значит, не обратим.

[1] см. сл. 7.4 на стр. 109

Упр. 8.9. См. указания к упр. 8.1

Упр. 8.11. Легко видеть, что $\det(FG) = \det F \cdot \det G$. Поэтому, если матрица F обратима, то $\det F \cdot \det F^{-1} \det(FF^{-1}) = \det E = 1$, и тем самым $\det F$ обратим. То, что формула (8-6) при обратимом $\det F$ даёт обратную матрицу, устанавливается прямым вычислением.

Упр. 8.12. Можно воспользоваться тем, что

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Упр. 9.1. Любая перестановка $g = (g_1, g_2, \dots, g_n)$ символов $\{1, 2, \dots, n\}$ является композицией $g = \sigma \circ g'$ транспозиции σ — символов n и g_n и перестановки $g' = \sigma \circ g$, оставляющей на месте элемент n. По индукции g' раскладывается в композицию транспозиций, не затрагивающих элемента n.

Упр. 9.3. При условии, что все точки пересечения двойные и трансверсальные, две нити, идущие из i и из j пересекаются между собою нечётное число раз, если пара (i, j) инверсна, и чётное число раз, если пара не инверсна (в действительности, картинку всегда можно нарисовать так, чтобы количества точек пересечения в этих двух ситуациях равнялись 1 и 0 соответственно). Знак тасующей перестановки $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$ равен $(-1)^{|I|+\frac{1}{2}k(k+1)}$, где *вес* $|I| \stackrel{\text{def}}{=} \sum_\nu i_\nu$. Действительно, нити, выходящие из чисел $i_1, i_2, \dots, i_k$ верхней строчки не пересекаются между собою и пересекают, соответственно, $i_1 - 1$, $i_2 - 2$, $\dots$, $i_k - k$ начинающихся левее нитей, выходящих из j-точек и тоже между собою не пересекающихся.

Упр. 9.4. Если g является композицией транспозиций $\sigma_k \sigma_{k-1} \cdots \sigma_1$, то $g^{-1} = \sigma_1 \sigma_2 \dots \sigma_k$ является произведением тех же транспозиций в противоположном порядке.

Упр. 9.5. Индукция по m. При $m = 1$ только нулевой многочлен $f \in \Bbbk[x]$ имеет бесконечно много корней. В общем случае запишем $f \in \Bbbk[x_1, x_2, \dots, x_m]$ как многочлен от x_m с коэффициентами в $\Bbbk[x_1, x_2, \dots, x_{m-1}]$ и вычислим коэффициенты в произвольной точке $\Bbbk^{m-1}$. Получится многочлен из $\Bbbk[x]$. Он равен нулю в каждой точке $\Bbbk$, только если все коэффициенты равны нулю. По индукции, все коэффициенты — нулевые многочлены, а значит и $f = 0$. Над полем $\mathbb{F}_q$ множество всех отображений $\mathbb{F}_q^m \to \mathbb{F}$ конечно (состоит из q^{q^m} элементов), а множество многочленов бесконечно.

Упр. 9.6. При чётном n центр алгебры $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ линейно порождается мономами чётных степеней, при нечётном n — мономами чётных степеней и старшим мономом $\xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n$ (имеющим в этом случае нечётную степень).

Упр. 9.7. Это сразу следует из равенства $\det A = \det A^t$.

Упр. 9.10. Если стоящие в левых частях уравнений (9-30) линейные формы

$$\alpha_i = \left(a_{i,0}, a_{i,1}, \dots, a_{i,n}\right) \in \Bbbk^{n+1^*}$$

линейно независимы, то по лемме о замене[1] ими можно заменить подходящие n ковекторов стандартного базиса в $\Bbbk^{n+1^*}$. Пусть это будут последние n векторов. Так как ковекторы $(1, 0, \dots, 0)$ и $\alpha_1, \alpha_2, \dots, \alpha_n$ образуют базис, определитель, составленный из строк их

[1] см. лем. 6.2 на стр. 89

координат, отличен от нуля. Раскладывая его по строке $(1,\ 0,\ \dots\ ,\ 0)$, видим, что он равен A_0, откуда $A_0 \neq 0$. Если же строки матрицы A линейно зависимы, то все $A_i = 0$.

Упр. 10.1. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 5.7 на стр. 72).

Упр. 10.2. Изоморфизм $M_1/\ker(\varphi) \xrightarrow{\sim} \operatorname{im}(\varphi)$ переводит класс $m \pmod{\ker \varphi}$ в $\varphi(m)$. Проверка корректности и биективности стандартна.

Упр. 10.8. Если $\lambda_1 m_1 = 0$ и $\lambda_2 m_2 = 0$, то $\lambda_1\lambda_2(m_1 \pm m_2) = 0$, где $\lambda_1\lambda_2 \neq 0$, т. к. в K нет делителей нуля. Кроме того, $\forall\, \mu \in K \quad \lambda_1(\mu m_1) = \lambda_2(\mu m_2) = 0$.

Упр. 10.11. Если $\lambda' = \lambda + x$ и $a' = a + v$, где $x \in I$, $v \in IM$, то $\lambda' a' = \lambda a + (xa + \lambda v + xv)$, где взятая в скобки сумма лежит в IM.

Упр. 10.16. Рассмотрим в грассмановой алгебре $K\langle \xi_1, \xi_2, \dots, \xi_m\rangle$ два набора линейных форм $\eta = \xi \cdot A$ и $\zeta = \eta \cdot C = \xi \cdot F$, где $F = AC$. Тогда грассмановы мономы степени k от η и ζ суть $\eta_I = \sum\limits_J \xi_J a_{JI}$ и $\zeta_K = \sum\limits_L \xi_L f_{LK}$. Поскольку $\zeta_I = \sum\limits_J \eta_J c_{JI}$, мы получаем $f_{LK} = \sum\limits_J a_{LJ} c_{JK}$.

Упр. 10.17. Пусть проделанные с матрицей C преобразования строк заключаются в последовательном умножении слева на матрицы $S_k \dots S_2 S_1$, а проделанные преобразования столбцов — в умножении справа на $R_1 R_2\ \dots\ R_\ell$. Тогда $F = S_k \cdots S_2 S_1 E$ и $G = E R_1 R_2\ \dots\ R_\ell$.

Упр. 10.19. Равносильность условий (а), (б) и (в) очевидна после перехода к взаимным базисам $\mathbb{Z}^m$ и подрешётки. Равносильность (в) и (г) вытекает прямо из определения ранга.

Упр. 10.20. Равенство $\varphi_n = 0$ при $n \geqslant m$ очевидно. Пусть $0 \leqslant n < m$. Если $\varphi_n(x) = 0$, то $p^n x = p^m y$ для некоторого $y \in K$, откуда $x = p^{m-n} y$, т. к. в K нет делителей нуля. Наоборот, если $x = p^{m-n} y$, то $p^n x = 0 \mod p^m$. Тем самым, $\ker \varphi_n = \operatorname{im} \varphi_{m-n}$. Правило $x \mod p^n \mapsto p^{m-n} x \mod p^m$ корректно задаёт инъективный гомоморфизмом K-модулей $K/\left(p^n\right) \to K/\left((p^m\right)$, который изоморфно отображает $K/\left(p^n\right)$ на $\operatorname{im} \varphi_{m-n}$.

Упр. 10.21. Достаточно проверить это для каждого отдельного слагаемого $K/\left(p^m\right)$. В этом случае фактор $\ker \varphi_i \ker \varphi_{i-1}$ состоит из классов вида $[p^{n-i}x] \in K/\left(p^m\right)$ по модулю классов вида $[p^{n-i+1}y]$, и все они аннулируются[1] умножением на p. Поэтому умножение на классы из $K/(p)$ определено корректно.

Упр. 11.2. Пусть $\Bbbk[t]/\left(t^n\right) = U \oplus W$, где U и W переводятся в себя умножением на t. Оба этих подпространства не могут целиком содержаться в образе оператора умножения на t (иначе их сумма тоже бы в нём содержалась), поэтому в одном из них, скажем, в U, есть класс $a \pmod{t^n}$, где $a \in \Bbbk$ отлично от нуля. Но тогда в U лежат все классы $at^m \pmod{t^n}$ с $0 \leqslant m \leqslant (n-1)$, а они линейно порождают всё пространство $\Bbbk[t]/\left(t^n\right)$.

Упр. 11.3. Если $V = U \oplus W$, где U и W F-инвариантны, то $V^* = \operatorname{Ann} U \oplus \operatorname{Ann} W$ и оба подпространства $\operatorname{Ann} U$ и $\operatorname{Ann} W$ будут F^*-инвариантны: скажем, если $\xi \in \operatorname{Ann} U$, то $\forall\, u \in U$ $\langle\, F^*\xi\,,\, u\,\rangle = \langle\, \xi\,,\, Fu\,\rangle = 0$, поскольку $Fu \in U$, и значит, $F^*\xi \in \operatorname{Ann} U$. Обратная импликация получается по двойственности в силу изоморфизма $V^{**} = V$.

Упр. 11.4. Так как любой вектор $h \in H$ представляется в V как $h = u + q + r$ с $u \in U$, $q \in Q$, $r \in R$, в U выполняется равенство $h = \pi(h) = \pi(u) + \pi(r)$, в котором $\pi(u) = u \in U$ и $\pi(r) \in W$, т. е. $U + W = H$. Если $u \in U \cap W$, то $u = \pi(r)$ для некоторого $r \in R$, и $\pi(u - r) = \pi(u) - \pi(r) = u - u = 0$, откуда $u - r \in \ker \pi = Q$, что возможно только при $u = r = 0$. Поэтому $U \cap W = 0$.

[1] по модулю $p^{n-i+1}K$

Упр. 11.5. В согласованном с разложением в прямую сумму базисе матрица $tE - F$ имеет блочно диагональный вид $\begin{pmatrix} tE-G & 0 \\ 0 & tE-H \end{pmatrix}$. С другой стороны, для любых матриц $A \in \mathrm{Mat}_n(\Bbbk)$, $C \in \mathrm{Mat}_m(\Bbbk)$, $B \in \mathrm{Mat}_{n\times m}(\Bbbk)$ определитель $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det A \cdot \det C$ согласно формуле для разложения определителя по первым n столбцам.

Упр. 11.6. Пусть $f = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$. Напишите матрицу F оператора умножения на t в фактор кольце $\Bbbk[x]/(f)$ в базисе из классов мономов t^{n-1}, t^{n-2}, $\cdots$, t, 1 и разложите $\det(tE - F)$ по первому столбцу.

Упр. 11.7. Поскольку умножение на произведение всех элементарных делителей полностью аннулирует прямую сумму форм. (11-1) на стр. 162, оператор $\chi_F(F)$ нулевой для любого оператора F над любым полем $\Bbbk$. Поскольку теорема Гамильтона-Кэли для матрицы A представляет собою набор тождеств между многочленами с целыми коэффициентами от элементов матрицы A, достаточно убедиться в её справедливости для всех матриц с рациональными элементами, т. е. для любого оператора над полем $\mathbb{Q}$.

Упр. 11.8. Если $\lambda \in \operatorname{Spec} F$ и $g(\lambda) \neq 0$, то $g(F)$ действует на ненулевом собственном подпространстве V_λ умножением на ненулевое число $g(\lambda)$. Тем самым, $g(F) \neq 0$.

Упр. 11.9. Над алгебраически замкнутым полем всякий многочлен имеющий только один корень 0 равен t^m. Поэтому $\chi_F(t) = t^m$ и по теореме Гамильтона – Кэли $F^m = 0$.

Упр. 11.11. Разложение характеристического многочлена оператора F в виде произведения степеней попарно разных линейных форм $\chi_F(t) = \prod\limits_{\lambda\in\operatorname{Spec} F} (t-\lambda)^{N_\lambda}$ удовлетворяет условиям предл. 11.7 с $q_i = (t-\lambda)^{N_\lambda}$, а корневые подпространства $K_\lambda = \ker(\lambda\,\mathrm{Id} - F)^{N_\lambda}$.

Упр. 11.12. Если $a^n = 0$, $b^m = 0$ и $ab = ba$, то по формуле Ньютона $(a+b)^{m+n-1} = 0$.

Упр. 11.14. Отображение (11-16) линейно. Равенство $s(fg) = s(f)s(g)$ достаточно проверять отдельно для каждой струи s^m_λ. По формуле Лейбница $(fg)^{(k)} = \sum\limits_{\nu+\mu=k} \binom{k}{\nu} f^{(\nu)} g^{(\mu)}$. Поэтому имеют место следующие сравнения по $\mathrm{mod}(t-\lambda)^m$:

$$s^m_\lambda(fg) \equiv \sum_k \frac{(t-\lambda)^k}{k!} \sum_{\nu+\mu=k} \frac{k!}{\nu!\,\mu!} f^{(\nu)}(\lambda) g^{(\mu)}(\lambda) \equiv$$

$$\equiv \sum_k \sum_{\nu+\mu=k} \frac{f^{(\nu)}(\lambda)}{\nu!}(t-\lambda)^\nu \cdot \frac{g^{(\mu)}(\lambda)}{\mu!}(t-\lambda)^\mu \equiv s^m_\lambda(f) s^m_\lambda(g)$$