Министерство образования и науки Российской Федерации
Московский Физико-Технический Институт
(национальный исследовательский университет)

А.В. Ершов

ЛЕКЦИИ ПО ЛИНЕЙНОЙ АЛГЕБРЕ

Москва
2024

Оглавление

Предисловие

Предмет линейной алгебры играет исключительно важную роль в университетском математическом образовании. Ее связи с другими разделами математики глубоки и многообразны, и вряд ли могут быть сколько-нибудь полно описаны в рамках введения. Также она имеет широчайшие применения в других науках, в особенности в физике. Например, не будет сильным преувеличением сказать, что квантовая механика — это линейная алгебра, которой придали физическую интерпретацию.

Данный текст основан на курсе линейной алгебры, который на протяжении ряда лет автор читает в МФТИ. В программе этого курса сконцентрирован опыт преподавательской работы ряда выдающихся математиков и педагогов, работавших и продолжающих работать на кафедре высшей математики МФТИ. В последние годы в некоторых школах МФТИ (включая ЛФИ) курс аналитической геометрии и линейной алгебры был расширен, в частности, за счет включения в него элементов общей алгебры — теории групп, колец и полей. Данный текст содержит также краткое изложение этих тем.

При написании текста автор стремился к максимально подробному изложению лекционного материала, чтобы он подходил и для самостоятельного изучения. В текст включено большое количество примеров, которые иллюстрируют теорию. Некоторые примеры даны в виде задач, зачастую с решениями.

Можно сказать, что на протяжении данного курса мы движемся от алгебры к геометрии. К примеру, сначала мы вводим матрицы и операции с ними (например, умножение), и уже потом получаем их важнейшую геометрическую интерпретацию как координатной записи линейных отображений, а их умножения — как композиции таких отображений. Другой аналогичный пример дает операция транспонирования матриц, которая впоследствии получает интерпретацию как переход к сопряженному отображению. Переход от матриц к линейным отображениям — движение в сторону большей абстракции, в мир более чистых идей. На первый взгляд это кажется парадоксальным, но на более абстрактном уровне теория идейно упрощается, в чем читатель сможет убедиться (например, изложенные в этом тексте теоремы о системах линейных уравнений проще понимать и доказывать на языке линейных отображений).

Вообще, полезно сразу понять место базисов в линейной алгебре. Математиками была постепенно осознана польза от инвариантных (не использующих базисов и координат) определений математических понятий. Мы тоже по возможности даем инвариантные определения и формулировки (и, где это возможно, доказательства). С другой стороны, использование базисов неизбежно, если нам нужно решить конкретную, “числовую”, задачу.

Большое влияние на автора и в плане отбора материала, и в плане его изложения оказал учебник [11]. Также целый ряд ценных идей автор почерпнул из учебников [7], [13], [15], [16], [17], а также из статьи [22].

Благодарности

Автор выражает глубокую благодарность своим учителям, коллегам и студентам. Особая благодарность — Ю. Кашпуровичу, В. Коротневу и А. Хомутову, приславшим список опечаток и предложений по улучшению текста, многие из которых были учтены при подготовке итогового варианта.

Советы студентам

Как уже говорилось выше, данный текст основан на лекциях по линейной алгебре для МФТИ. Он представляет собой расширенный конспект лекций, снабженный теоретическими задачами и дополнительным материалом, призванным помочь вдумчивому студенту достичь более глубокого понимания предмета. Мы не стремились к краткости и "линейности" изложения; наоборот, мы часто приводим несколько разных доказательств ряда важных результатов (например, читатель найдет по три варианта доказательства теоремы Гамильтона-Кэли и теоремы о существовании собственного вектора самосопряженного оператора в евклидовом пространстве).

Хотя значительная часть представленного здесь материала выходит за рамки обязательной программы для большинства факультетов МФТИ (и других университетов с семестровым курсом Линейной алгебры), мы старались сделать данный текст удобным и для тех студентов, которые хотят ограничиться изучением только обязательных разделов курса: для удобства таких читателей дополнительный материал набран мелким шрифтом и может быть пропущен без ущерба для логической связности изложения.

Заметим, что в тексте почти ничего не сказано о многочисленных приложениях линейной алгебры в физике: об этом (а также о ряде дополнительных тем, таких как аффинная и проективная геометрии) заинтересованный читатель может прочитать в замечательной книге [17].

Отметим, что в данный текст вошли в основном теоретические задачи, поэтому их решение не отменяет необходимости решить достаточное количество стандартных, вычислительных задач, например, из задачника [9]. В качестве решебника по таким задачам автор рекомендует [12]. Тем, кто хочет углубить свое понимание линейной алгебры и дополнительно потренироваться в решении теоретических задач, можно рекомендовать [6].

Требования к подготовке читателя

Предполагается, что читатель освоил стандартный курс аналитической геометрии. В частности, знако́м с понятием свободного вектора, элементами векторной алгебры в пространствах размерности 2 и 3, определителями и матрицами малых порядков. Предполагается также знакомство с языком элементарной теории множеств (обычно проходимом в начале курса математического анализа), методом математической индукции и другими темами из программы средней школы.

Mathematics is not about numbers, equations, computations,
or algorithms: it is about understanding.

William Thurston

1 Начальные сведения из алгебры

Данная глава носит вспомогательный характер: в ней для удобства читателя приведены определения некоторых понятий, которые используются в дальнейшем. Можно начинать чтение со следующей главы, обращаясь к данной по мере необходимости.

1.1 Некоторые теоретико-множественные определения

Если X и Y — два множества, то для произвольных $x \in X$ и $y \in Y$ через (x, y) обозначим соответствующую упорядоченную пару. Две упорядоченные пары (x, y) и (x', y') равны тогда и только тогда, когда $x = x'$ и $y = y'$.

Определение 1.1. *Декартовым произведением* $X \times Y$ множеств X и Y называется множество всех упорядоченных пар

$$\{(x, y) \mid x \in X, y \in Y\}.$$

Через $|X|$ мы будем обозначать мощность множества X.

Задача 1.2. *Пусть* $|X| = n$, $|Y| = m$. *Докажите, что* $|X \times Y| = nm$.

В частности, определен *декартов квадрат* $X \times X$ множества X. Например, $\mathbb{R} \times \mathbb{R}$ — множество упорядоченных пар действительных чисел. Любой выбор декартовой системы координат в плоскости определяет биекцию между множеством точек плоскости и $\mathbb{R} \times \mathbb{R}$. Аналогично для множества точек трехмерного пространства и множества $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Множество $\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$ (декартово произведение множества $\mathbb{R}$ на себя n раз) часто обозначается $\mathbb{R}^n$, его элементами являются строки (или столбцы) длины (высоты) n из действительных чисел.

Для множеств X и Y определим множество X^Y всех отображений $Y \to X$.

Задача 1.3. *Пусть* $|X| = n$, $|Y| = m$. *Докажите, что* $|X^Y| = n^m$.

В частности, $|X^X| = n^n$.

Пусть теперь

$$S(X) := \{f \colon X \to X \mid f \text{ биективно}\}.$$

Задача 1.4. *Пусть* $|X| = n$. *Докажите, что* $|S(X)| = n!$.

В частности, вероятность того, что случайно выбранное отображение $X \to X$ является биекцией, стремится к нулю при $n \to \infty$ (поскольку $\lim_{n\to\infty} \frac{n!}{n^n} = 0$).

Отметим, что для конечных множеств X и Y одинаковой мощности условия того, что отображение $f\colon X \to Y$ 1) инъективно; 2) сюръективно и 3) биективно, эквивалентны.

В дальнейшем будет полезно следующее элементарное предложение.

Предложение 1.5. *Пусть S и T — произвольные множества, а $f\colon S \to T$, $g\colon T \to S$ — такие отображения, что $gf = \mathrm{id}_S$, $fg = \mathrm{id}_T$. Тогда f и g — взаимно обратные биекции. Верно и обратное.*

Доказательство. Из $gf = \mathrm{id}_S$ следует, что f инъективно а g сюръективно. В самом деле, если f не инъективно, то $\exists\, s_1 \neq s_2 \in S$ такие, что $f(s_1) = f(s_2)$. Тогда $g(f(s_1)) = g(f(s_2))$, что противоречит тому, что $g(f(s_1)) = s_1 \neq g(f(s_2)) = s_2$. С другой стороны, для любого элемента $s \in S$ имеем $s = g(f(s))$, что доказывает сюръективность g.

Аналогично, из $fg = \mathrm{id}_T$ следует инъективность g и сюръективность f. Значит f и g биективны и $f(s) = t$ тогда и только тогда, когда $g(t) = s$, откуда $g = f^{-1}$ и $f = g^{-1}$. Обратное утверждение очевидно. ∎

Задача 1.6. *Пусть $|Y| = m$. Постройте биекцию между множествами X^Y и $X \times X \times \ldots \times X$ (m сомножителей).*

Задача 1.7. *Постройте биекцию между множествами $X^{Y\times Z}$ и $(X^Y)^Z$.*

Подсказка. Пусть, например, задано отображение $f\colon Y \times Z \to X$. Тогда для фиксированного $z \in Z$ функция $f(\cdot\,, z)$ от первого аргумента представляет собой функцию $Y \to X$. Рассматривая теперь $f(\cdot, z)$ как функцию от z, получаем отображение $Z \to X^Y$. Тем самым мы определили некоторое отображение $X^{Y\times Z} \to (X^Y)^Z$. ∎

Для данного множества X обозначим множество всех его подмножеств (включая пустое и само множество X) через 2^X. Последнее также называется *булеаном* множества X. Подчеркнем, что элементами множества 2^X являются подмножества множества X.

Предложение 1.8. *Существует биекция между множеством 2^X и множеством $\{0,1\}^X$ всех отображений $X \to \{0,1\}$. В частности, если $|X| = n$, то $|2^X| = 2^n$.*

Доказательство. Пусть $A \subset X$ — подмножество (эквивалентно, $A \in 2^X$); сопоставим ему функцию (=отображение) $\chi_A\colon X \to \{0,1\}$, определенную следующим правилом:

$$\chi_A(x) = \begin{cases} 0, & \text{если } x \notin A; \\ 1, & \text{если } x \in A. \end{cases}$$

Обратно, функции $f\colon X \to \{0,1\}$ сопоставим подмножество $S_f \subset X$ задаваемое как $S_f := \{x \in X \mid f(x) = 1\}$. Теперь легко проверить, что определенные нами сопоставления $A \mapsto$

χ_A, $f \mapsto S_f$ удовлетворяют тождествам $S_{\chi_A} = A$, $\chi_{S_f} = f$. Значит, согласно Предложению 1.5, они задают взаимно обратные биекции между множествами 2^X и $\{0,1\}^X$. ∎

Определим биномиальный коэффициент $\binom{n}{k}$ как количество k-элементных подмножеств в n-элементном множестве.

Следствие 1.9.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Задача 1.10. *Докажите, что* $\binom{n}{k} = \binom{n}{n-k}$. *(Указание: постройте биекцию между множеством k-элементных и множеством $n-k$-элементных подмножеств n-элементного множества. Или для функции $f\colon X \to \{0,1\}$ как в доказательстве предыдущего Предложения, рассмотрите функцию $1 - f$.)*

Задача 1.11. *Докажите тождество*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Решение. Пусть $X := \{1, 2, \ldots, n\}$ — n-элементное множество. Тождество означает, что количество подмножеств в X, состоящих из четного числа элементов равно количеству подмножеств, состоящих из нечетного числа. Покажем, что это действительно так.

Пусть $S \subset X$ — некоторое подмножество. Сопоставим ему новое подмножество $\widehat{S} \subset X$ по следующему правилу:

$$\widehat{S} = \begin{cases} S \cup 1, & \text{если } 1 \notin S; \\ S \backslash 1, & \text{если } 1 \in S. \end{cases}$$

Легко видеть, что сопоставление $S \mapsto \widehat{S}$ определяет взаимно-обратные биекции между множествами подмножеств в X из четного и нечетного количества элементов. ∎

Задача 1.12. *Докажите формулу*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

1.2 Отношения эквивалентности

Определение 1.13. (*Бинарным*) *отношением* на множестве X называется произвольное подмножество $R \subset X \times X$.

Пример 1.14. *Диагональ* $\Delta_X := \{(x, x) \mid x \in X\} \subset X \times X$ задает *отношение равенства* на X.

Изучение какой-либо части окружающего мира обычно связано с классификацией ее объектов. Классификация элементов некоторого множества X — разбиение этого множества на классы. Например, в курсе аналитической геометрии рассматриваются две классификации плоских кривых второго порядка — аффинная и метрическая (с точностью до движений плоскости). Любое такое разбиение происходит из (и, в свою очередь, определяет) некоторого *отношения эквивалентности* на X.

Определение 1.15. Отношение R на множестве X называется *отношением эквивалентности* на X, если оно обладает свойствами:

1) *рефлексивности*: $(x, x) \in R$ для любого $x \in X$;

2) *симметричности*: $(x, y) \in R \Rightarrow (y, x) \in R$

3) *транзитивности*: $(x, y) \in R$ и $(y, z) \in R \Rightarrow (x, z) \in R$.

Например, отношение равенства является отношением эквивалентности.

Рассмотрим еще примеры отношений. На множестве людей X отношение

$$R_1 = \{(x, y) \mid y \text{ знает } x\}$$

не является отношением эквивалентности (например, отсутствует симметричность); отношение

$$R_2 = \{(x, y) \mid y \text{ знако́м с } x\}$$

также не является отношением эквивалентности (оно симметрично, но не транзитивно), а отношения "быть родственником"[1] или "жить в одном доме" — отношения эквивалентности.

Пусть R — отношение эквивалентности на множестве X. В этом случае вместо $(x, y) \in R$ пишут $x \sim_R y$ или просто $x \sim y$, если ясно, какое отношение эквивалентности имеется в виду.

Пусть X — множество, на котором задано отношение эквивалентности $\sim$. *Классом эквивалентности* элемента $x \in X$ назовем подмножество $[x] \subset X$, состоящее из всех элементов, эквивалентных x, то есть $[x] := \{y \in X \mid y \sim x\}$. Произвольный элемент $y \in [x]$ называется *представителем* класса эквивалентности $[x]$.

Например, для отношения эквивалентности "жить в одном доме" классы эквивалентности — жители одного дома. Произвольный житель дома является представителем такого класса.

Предложение 1.16. $[x] = [x'] \Leftrightarrow x \sim x'$.

[1] хотя, возможно, транзитивность этого отношения не очевидна.

Доказательство. Пусть $[x] = [x']$. Так как $x \sim x$, то $x \in [x] = [x']$, а значит, $x \sim x'$.

Наоборот, предположим, что $x \sim x'$. Пусть $y \in [x] \;\Rightarrow\; y \sim x \;\Rightarrow\; y \sim x' \;\Rightarrow y \in [x']$. Таким образом, $[x] \subset [x']$. Тогда в силу симметричности отношения эквивалентности $[x] = [x']$. ∎

Определение 1.17. *Разбиением* множества X называется представление его в виде объединения непересекающихся[2] непустых подмножеств, то есть в виде $X = \bigcup_{\alpha\in A} X_\alpha$, $\varnothing \neq X_\alpha \subset X$, причем $X_\alpha \bigcap X_\beta = \varnothing$ при $\alpha \neq \beta$.

Предложение 1.18. *Классы эквивалентности отношения эквивалентности $\sim$ на X образуют разбиение множества X.*

Доказательство. Так как $x \in [x]$, то каждый элемент множества X принадлежит некоторому классу эквивалентности. Покажем, что если классы $[x]$, $[x']$ имеют непустое пересечение, то они совпадают. Пусть $y \in [x] \cap [x']$. Тогда $y \sim x \;\Rightarrow\; x \sim y$, а также $y \sim x' \;\Rightarrow\; x \sim x' \;\Rightarrow\; [x] = [x']$ по Предложению 1.16. ∎

Заметим, что верно и обратное: по любому разбиению $X = \bigcup_{\alpha\in A} X_\alpha$ множества X определяется единственное отношение эквивалентности на X, для которого X_α, $\alpha \in A$, являются классами эквивалентности. То есть *существует естественное взаимно однозначное соответствие между отношениями эквивалентности на множестве X и разбиениями X.*

Задача 1.19. *Докажите, что на множестве из 4-х элементов существует ровно 15 различных отношений эквивалентности.*

Теперь заметим, что классы эквивалентности отношения эквивалентности $\sim$ на X сами можно рассматривать как элементы некоторого множества, которое называется *факторомножеством множества X по отношению эквивалентности* $\sim$. Факторомножество множества X по отношению эквивалентности $\sim$ обозначается $X/\sim$. Оно задано вместе с сюръективным отображением $\pi\colon X \to X/\sim$, $\pi(x) = [x]$, называемым *факторотображением.*

Рассмотрим примеры. Факторомножество множества людей по отношению эквивалентности “жить в одном доме” — множество домов (мы считаем, что каждый человек живет в доме, причем единственном).

Пример 1.20. Пусть Π — евклидова (точечная) плоскость, $O \in \Pi$ — ее фиксированная точка. Рассмотрим на множестве Π следующее отношение эквивалентности: $P \sim Q \;\Leftrightarrow\; |OP| = |OQ|$. Классы этой эквивалентности образуют семейство концентрических окружностей плоскости Π с центром в точке O (включая окружность нулевого радиуса); сопоставляя такой окружности ее радиус мы получаем биекцию между факторомножеством и множеством неотрицательных действительных чисел $\mathbb{R}_{\geq 0}$.

[2] То есть имеющих пустое пересечение.

Задача 1.21. *Пусть F_1, $F_2 \in \Pi$ — две различные точки на плоскости. Определите отношение эквивалентности на множестве точек плоскости, классами эквивалентности которого являются эллипсы с фокусами в F_1 и F_2 а также отрезок, соединяющий точку F_1 с F_2.*

Пример 1.22. (Свободные векторы на плоскости.) *Направленным отрезком AB* на плоскости называется упорядоченная пара $(A,\ B)$ точек на плоскости. Два направленных отрезка AB и $A'B'$ называются *эквивалентными*, если середины AB' и $A'B$ совпадают. Читателю предлагается убедиться, что это — действительно отношение эквивалентости и что его классы эквивалентности — в точности свободные векторы на плоскости.

Пусть $f\colon X \to Y$ — произвольное отображение множеств. Тогда полные прообразы

$$f^{-1}(y) := \{x \in X \mid f(x) = y\} \subset X$$

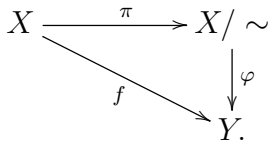
точек y из образа f образуют разбиение множества X. Оно соответствует следующему отношению экивалентности на X:

$$x_1 \sim x_2 \ \Leftrightarrow\ f(x_1) = f(x_2). \tag{1}$$

Пусть теперь $f\colon X \to Y$ — произвольное сюръективное отображение множеств. Пусть $\sim$ — отношение эквивалентности (1) на X. Тогда существует вполне определенная биекция

$$\varphi\colon X/\sim \to Y,\ \ \varphi([x]) = f(x)$$

(проверку корректности определения φ и его биективности оставляем читателю в качестве упражнения). Отображение f можно отождествить с факторотображением, поскольку они входят в коммутативную диаграмму



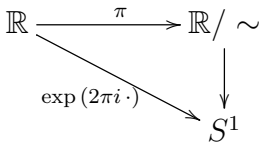
Пример 1.23. На множестве действительных чисел $\mathbb{R}$ рассмотрим следующее отношение: $a \sim b \Leftrightarrow b - a \in \mathbb{Z}$. Читателю предлагается убедиться, что это — действительно отношение эквивалентости и что его классы эквивалентности — подмножества в $\mathbb{R}$, состоящие из действительных чисел, имеющих одинаковые дробные части. Такие классы можно записать следующим образом:

$$[a] = \{a + n \mid n \in \mathbb{Z}\} \subset \mathbb{R}.$$

Функция $t \mapsto \exp(2\pi i t)$ обладает следующим свойством:

$$\exp(2\pi i a) = \exp(2\pi i b)\ \Leftrightarrow\ a \sim b.$$

Ее образом является единичная окружность $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ в комплексной плоскости. Заметим, что диаграмма



коммутативна, где вертикальная стрелка — биекция, тем самым мы отождествили $\exp(2\pi i\,\cdot)\colon \mathbb{R} \to S^1$ с факторотображением π (а S^1 — с фактормножеством $\mathbb{R}/\sim$).

Задача 1.24. *Постройте биекцию между* 1*-периодическими функциями на прямой* $\mathbb{R}$ *и функциями на окружности* S^1*.*

Пример 1.25. Для данного натурального числа n рассмотрим следующее отношение на множестве целых чисел $\mathbb{Z}$: $a \sim b \Leftrightarrow n|(b-a)$ ($n|m$ обозначает "n делит m"). Читателю предлагается убедиться, что это — действительно отношение эквивалентости и что его классы эквивалентности — подмножества в $\mathbb{Z}$, состоящие из целых чисел, имеющих одинаковые остатки при делении на n. Класс, содержащий $a \in \mathbb{Z}$, можно записать следующим образом:

$$[a] = \{a + kn \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$$

(в данной записи a и n фиксированы, а k пробегает все целые числа). То есть в данном случае мы имеем в точности n классов эквивалентности. Класс эквивалентности, содержащий целое число a, называется *классом вычетов* a *по модулю* n. Таким образом, элементами фактормножества являются классы вычетов. Например, при $n = 2$ один из классов состоит из четных, а другой — из нечетных целых чисел. Читатель легко убедится, что для натурального n $\{[0], [1], \ldots, [n-1]\}$ — все классы вычетов по модулю n, то есть их в точности n штук. При этом например $[2] = [n+2] = [2-3n] = \ldots$. Множество классов вычетов по модулю n обозначается $\mathbb{Z}_n$.

Пример 1.26. (Рациональные числа.) Рассмотрим множество упорядоченных пар целых чисел $(m,\, n)$, $m,\, n \in \mathbb{Z},\ n \neq 0$. Определим на данном множестве отношение

$$(m,\, n) \sim (m',\, n') \ \Leftrightarrow\ mn' = m'n. \tag{2}$$

Рефлексивность и симметричность такого отношения очевидны. Проверим транзитивность. Пусть $(m',\, n') \sim (m'',\, n'')$, то есть $m'n'' = m''n'$. Умножая обе части равенства в (2) на n'', а обе части предыдущего равенства — на n, получаем $mn'n'' = m'nn''$; $m'n''n = m''n'n$, откуда, сокращая на n' (и используя $n' \neq 0$), получаем $mn'' = m''n$. Класс эквивалентности этого отношения называется *рациональным числом.* Множество рациональных чисел обозначается $\mathbb{Q}$.

1.3 Алгоритм Евклида

Пусть a и b — натуральные числа. Их *наибольшим общим делителем* (обозначение: (a, b)) называется такой их натуральный общий делитель, который делится на все их общие делители. То есть $(a, b) \mid a,\ (a, b) \mid b$ и если $d \in \mathbb{N}$ и $d \mid a,\ d \mid b$, то $d \mid (a, b)$. Ясно, что если (натуральный) наибольший делитель существует, то он единственен. Вскоре мы докажем, что наибольший общий делитель существует для любой пары натуральных чисел.

В школе было доказано следующее утверждение: если $a,\ b \in \mathbb{Z}$, причем $b > 0$, то существует и единственна такая пара чисел $q,\ r \in \mathbb{Z}$, что $0 \leq r < b$ и $a = qb + r$. Число q при этом называется *неполным частным*, а r — *остатком* от деления a на b.

Если натуральные числа a и b разложить на простые множители:

$$a = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}, \quad b = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s},$$

где $p_1, p_2, \dots, p_s$ — различные простые числа, а $k_i,\ l_i \geq 0$, то

$$(a, b) = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s},$$

где $m_i = \min(k_i,\ l_i)$.

Однако разложение числа на простые множители является вычислительно сложной задачей. Между тем, существует классический алгоритм Евклида (*Начала*, примерно 300 год до н.э.), позволяющий найти наибольший общий делитель двух натуральных чисел без нахождения их разложения на простые множители. А именно, рассмотрим цепочку равенств

$$a = q_1 b + r_1,\ \ b = q_2 r_1 + r_2,\ \ r_1 = q_3 r_2 + r_3, \dots.$$

Строго убывающая цепочка натуральных чисел

$$b > r_1 > r_2 > r_3 > \dots,$$

обязательно оборвется на конечном шаге и мы придем к равенствам

$$r_{n-2} = q_n r_{n-1} + r_n,\ \ r_{n-1} = q_{n+1} r_n.$$

Оказывается, последний ненулевой остаток в этой цепочке и является наибольшим общим делителем.

Предложение 1.27. *$(a, b) = r_n$, причем существуют такие $u,\ v \in \mathbb{Z}$, что $r_n = au + bv$.*

Доказательство. Двигаясь по описанной цепочке снизу вверх, имеем:

$$r_n \mid r_{n-1},\ r_n \mid r_{n-2},\ \dots, r_n \mid r_3,\ r_n \mid r_2,\ r_n \mid r_1,\ r_n \mid b,\ r_n \mid a.$$

Таким образом, r_n — общий делитель чисел a и b.

Наоборот, двигаясь сверху вниз, имеем

$$r_1 = a - q_1 b = au_1 + bv_1,\ r_2 = b - q_2 r_1 = -q_2 a + (1 + q_1 q_2)b = au_2 + bv_2,$$

$$r_3 = au_3 + bv_3, \ldots, r_n = au_n + bv_n$$

(доказательство существования таких представлений производится по индукции). Таким образом, r_n можно представить в виде $au + bv$. Отсюда следует, что если $d \mid a$, $d \mid b$, то $d \mid r_n$. Значит, $r_n = (a, b)$. ∎

Представление наибольшего общего делителя (a, b) в виде $(a, b) = au + bv$ называется *тождеством Безу*.

Натуральные a и b называются *взаимно простыми*, если $(a, b) = 1$.

Следствие 1.28. *Если* $(a, b) = 1$, *то существуют такие* u, $v \in \mathbb{Z}$, *что* $au + bv = 1$.

1.4 Абелевы (коммутативные) группы

Исторически понятие числа расширялось, начиная с натуральных чисел, затем положительных рациональных, целых, рациональных, действительных и комплексных. Математически имеем включения числовых множеств:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

(мы используем стандартные обозначения натуральных, целых, рациональных, действительных и комплексных чисел). Причем все расширения, кроме $\mathbb{Q} \subset \mathbb{R}$, можно описать чисто алгебраически из потребности расширить класс разрешимых алгебраических уравнений. Множества рациональных, действительных и комплексных чисел объединяет то, что с алгебраической точки зрения они являются *полями*[3].

Ниже мы объясним, что такое поле. Для этого нам придется начать с более элементарного понятия *группы*.

Говоря кратко, группа — это множество, на котором задана *бинарная операция*, обладающая некоторыми свойствами.

Определение 1.29. Говорят, что на множестве X задана *бинарная операция* $*$, если любой *упорядоченной паре* (x_1, x_2) элементов из X поставлен в соответствие некоторый элемент $x_1 * x_2 \in X$.

Другими словами, бинарная операция $*$ на X — то же, что отображение (= функция)

$$X \times X \to X,\ \ X \times X \ni (x_1,\ x_2) \mapsto x_1 * x_2 \in X.$$

[3]термин *поле* в математике многозначен, например существуют векторные поля. В данном тексте мы будем использовать поле только для обозначения указанного алгебраической понятия.

Задача 1.30. *Найдите количество различных бинарных операций на множестве из n элементов.*

Примерами бинарных операций являются операции сложения и умножения на указанных числовых множествах или, например, векторное произведение векторов трехмерного ориентированного евклидова пространства. Вычитание тоже определяет бинарную операцию на всех указанных числовых множествах кроме $\mathbb{N}$ (почему?). С делением сложнее: во-первых, нельзя делить на нуль, во-вторых, даже если выбросить нуль из $\mathbb{Z}$, результат деления может оказаться нецелым числом. В то же время если $\mathbb{K}$ — любое из приведенных выше числовых полей ($\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$), то на множестве $\mathbb{K}^* := \mathbb{K}\backslash\{0\}$ его ненулевых элементов деление является бинарной операцией. Скалярное и смешанное произведения не являются бинарными операциями на множестве векторов евклидова пространства (почему?).

Рассмотрим множество целых чисел $\mathbb{Z}$ с операцией сложения. Какими абстрактными свойствами обладает эта операция? Во-первых, она *ассоциативна*: для любых целых чисел k, l, m имеет место тождество $(k+l)+m = k+(l+m)$. Во-вторых, существует *нейтральный элемент* 0, обладающий свойством $k + 0 = k = 0 + k$ для любого целого числа k. В третьих, для любого целого числа k существует *противоположное* число $(-k)$, такое что $k + (-k) = 0 = (-k) + k$. Наконец, в четвертых, она *коммутативна*: для любых целых чисел k, l верно тождество $k + l = l + k$.

Рассмотрим также множество ненулевых рациональных чисел $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$ с операцией умножения. Какими абстрактными свойствами обладает эта операция? Во-первых, она *ассоциативна*: для любых ненулевых рациональных чисел $(pq)r = p(qr)$. Во-вторых, для нее существует *нейтральный элемент* 1, обладающий свойством $p1 = p = 1p$ для любого $p \in \mathbb{Q}^*$. В третьих, для любого $p \in \mathbb{Q}^*$ существует *обратное* число p^{-1}, такое что $pp^{-1} = 1 = p^{-1}p$. Наконец, операция умножения *коммутативна*: $pq = qp$ для любых p, $q \in \mathbb{Q}^*$.

Если в двух приведенных примерах абстрагироваться от того, что множества целых и ненулевых рациональных чисел различны, а сосредоточиться только на указанных абстрактных свойствах (ассоциативности, существование нейтрального и противоположного = обратного элементов, коммутативности) операций на указанных множествах, то очевидно, что этими свойствами обладает и операция сложения целых чисел, и операция умножения ненулевых рациональных чисел.

В то же время операция вычитания на множестве $\mathbb{Z}$ (или операция деления на множестве $\mathbb{Q}^*$) указанными свойствами не обладает, например, читатель легко убедится, что она неассоциативна.

Следующее Определение выделяет общие свойства целых чисел с операцией сложения и ненулевых рациональных чисел с операцией умножения. В нем в качестве обозначения операции мы выбрали $+$, что привычно во многих примерах, но не принципиально.

Определение 1.31. Пара $(A,\, +)$, состоящая из множества A и заданной на нем бинарной операции

$$A \times A \xrightarrow{+} A, \quad (a,\, b) \mapsto a + b$$

(называемой "сложением") называется *коммутативной*, или *абелевой группой*, если выполнены следующие условия ("аксиомы абелевой группы"):

1) сложение *коммутативно*, то есть $a + b = b + a$ для любых $a,\, b \in A$;

2) сложение *ассоциативно*, то есть $\forall\, a,\, b,\, c \in A \quad (a + b) + c = a + (b + c)$;

3) в A существует *нуль* (называемый также *нейтральным элементом*), обозначаемый 0 и характеризующийся свойством $a + 0 = a\ \forall\, a \in A$;

4) для каждого $a \in A$ существует *противоположный элемент*, обозначаемый $(-a)$ и характеризующийся свойством $a + (-a) = 0$.

Таким образом, $(\mathbb{Z},\, +)$ и $(\mathbb{Q}^*,\, \cdot)$ являются абелевыми группами.

Задача 1.32. *Из аксиом абелевой группы выведите следующие следствия:*

- *единственность нуля;*
- *единственность противоположного элемента $-a$ для каждого $a \in A$;*
- *однозначную разрешимость в $(A,\, +)$ уравнения вида $x + a = b$, где $a,\, b \in A$. (Ясно, что решение этого уравнения есть элемент $b + (-a) \in A$, он называется разностью элементов b и a и обозначается $b - a$).*

Кроме того, из ассоциативности сложения следует, что сумма произвольного конечного числа (а не только трех) элементов абелевой группы не зависит от расстановки скобок.

Задача 1.33. *Какие из следующих множеств с операциями являются абелевыми группами, а какие — нет и почему?* $(\mathbb{N},\, +)$, $(\mathbb{Z},\, \cdot)$, $(\mathbb{Z},\, -)$, $(\mathbb{Q},\, +)$, $(\mathbb{Q},\, \cdot)$, $(\mathbb{Q},\, \div)$, $(\mathbb{R}^*,\, \cdot)$.

Задача 1.34. *Постройте биекцию $f\colon \mathbb{R} \to \mathbb{R}_{>0}$ между множеством всех действительных $\mathbb{R}$ и положительных действительных $\mathbb{R}_{>0}$ чисел, удовлетворяющую условию $f(a + b) = f(a) \cdot f(b)$ для произвольных $a,\, b \in \mathbb{R}$.*

Замечание 1.35. Заметим, биекция между $\mathbb{R}$ и $\mathbb{R}_{>0}$, которая строится в предыдущей задаче, переводит "таблицу умножения" в группе $(\mathbb{R},\, +)$ в "таблицу умножения" в группе $(\mathbb{R}_{>0},\, \cdot)$:

$$\begin{array}{c|c} + & a \\ \hline b & a + b \end{array} \qquad \begin{array}{c|c} \cdot & f(a) \\ \hline f(b) & f(a)f(b) \end{array},$$

что свидетельствует о том, что группы $(\mathbb{R},\, +)$ и $(\mathbb{R}_{>0},\, \cdot)$ "устроены одинаково" как множества с бинарной операцией. Такие группы называются *изоморфными*.

Ниже вместо $(A,\,+)$ мы часто будем писать A, явно указывая только множество элементов группы, если из контекста ясно, какая операция подразумевается.

Определение 1.36. Пусть $B \subset A$ — подмножество множества элементов абелевой группы $(A,\,+)$, причем

1) B содержит ноль, то есть $0 \in B$;

2) B замкнуто относительно операции $+$, то есть $b_1,\, b_2 \in B \;\;\Rightarrow\;\; b_1 + b_2 \in B$;

3) B замкнуто относительно операции взятия противоположного элемента, то есть $\forall\, b \in B \Rightarrow (-b) \in B$.

Тогда пара $(B,\,+)$[4] называется *подгруппой* группы $(A,\,+)$.

Заметим, что вместо условия 1) в предыдущем определении можно было бы потребовать непустоты множества B. Очевидно, что подгруппа абелевой группы сама является абелевой группой (относительно той же операции).

Рассмотрим примеры абелевых групп и их подгрупп.

Самая "маленькая" (по включению) подгруппа группы $(A,\,+)$ — подгруппа, состоящая только из нуля, самая "большая" — совпадает со всей группой. Также имеем вложения подгрупп $(\mathbb{Z},\,+) \subset (\mathbb{Q},\,+) \subset (\mathbb{R},\,+) \subset (\mathbb{C},\,+)$ и $(\mathbb{Q}^*,\,\cdot) \subset (\mathbb{R}^*,\,\cdot) \subset (\mathbb{C}^*,\,\cdot)$. Еще пример: $(\{\pm 1\},\,\cdot)$ является подгруппой в $(\mathbb{Q}^*,\,\cdot)$, состоящей из двух элементов. Ещё пример: подгруппу в $(\mathbb{Z},\,+)$ образуют все целые числа, кратные фиксированному натуральному n.

Задача 1.37. *Докажите, что единичная окружность*

$$\{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}$$

в комплексной плоскости является подгруппой группы $(\mathbb{C}^*,\,\cdot)$.

Пример 1.38. В этом примере мы найдем все подгруппы в $\mathbb{Z}$. Во-первых, есть подгруппа, состоящая из одного нуля (нейтрального элемента), она так и называется *нулевой*. Пусть $B \subset \mathbb{Z}$ — произвольная ненулевая подгруппа. Заметим, что $b \in B \;\Leftrightarrow\; -b \in B$. Пусть n — наименьшее натуральное число, содержащееся в B и $m \in B$ — произвольное. Мы хотим доказать, что $n \mid m$. В самом деле, поделим m на n с остатком: $m = qn + r$, где $0 \leq r < n$. Пусть $r \neq 0$. Но $r = m - qn$ и, поскольку m и n лежат в B, то и $r \in B$. Тем самым, предположив $r \neq 0$, мы получили противоречие с минимальностью n. Таким образом, все подгруппы в $\mathbb{Z}$ имеют вид $n\mathbb{Z}$, где $n \in \mathbb{N} \cup \{0\}$. Заметим, что все они состоят из счетного множества элементов, за исключением нулевой подгруппы.

[4] чтобы не усложнять обозначения, операция $+$ на A и ее ограничение на подмножество $B \subset A$ обозначаются одним и тем же символом.

К настоящему моменту мы познакомились с двумя видами структур на множествах — отношениями эквивалентности и бинарными операциями. Допустим теперь, что на одном и том же множестве X одновременно задано отношение эквивалентности $\sim$ и бинарная операция $*$. Интересным и очень важным для абстрактной алгебры является вопрос о том, когда эти структуры согласованы.

Определение 1.39. Отношение эквивалентности $\sim$ называется *согласованным* с бинарной операцией $*$, если из $x \sim x'$ и $y \sim y'$ следует $x * y \sim x' * y'$.

Читатель легко убедится, что условие согласованности из предыдущего Определения — в точности то, что нужно потребовать для того, чтобы формула

$$[x] \circ [y] := [x * y] \quad \forall\, x,\, y \in X$$

корректно определяла бинарную операцию на фактормножестве $X/\sim$. Более того, если $(X,\, *)$ — абелева группа, то и $(X/\sim,\, \circ)$ абелева группа.

Пример 1.40. Проверим, что отношение сравнимости по модулю n, введенное в Примере 1.25, согласовано с операциями сложения и умножения в $\mathbb{Z}$. Если $k \sim k',\ l \sim l'$, то $(k+l) \sim (k'+l')$, поскольку если $n \mid (k'-k),\ n \mid (l'-l)$, то $n \mid (k'+l'-(k+l))$.

Для операции умножения аналогично: если $k \sim k',\ l \sim l'$, то $kl \sim k'l'$, поскольку если $n \mid (k'-k),\ n \mid (l'-l)$, то $n \mid (k'l'-kl) = (k'-k)l' + k(l'-l)$.

Тем самым на множестве классов вычетов $\mathbb{Z}_n$ формулы $[k]+[l] := [k+l]$, $[k]\cdot[l] := [kl]$ корректно определяют бинарные операции $+$ и $\cdot$. Читателю предлагается убедиться, что $(\mathbb{Z}_n,\, +)$ — абелева группа. (Заметим на будущее, что $(\mathbb{Z}_n,\, +,\, \cdot)$ — коммутативное кольцо).

Задача 1.41. *Убедитесь, что отношение эквивалентности из Примера 1.22 согласовано с операцией сложения векторов по правилу треугольника. Тем самым мы получаем бинарную операцию сложения свободных векторов.*

Задача 1.42. *Подумайте, как задать операции на множестве упорядоченных пар целых чисел, согласованные с отношением эквивалентности из Примера 1.26, которые приведут к операциям сложения и умножения рациональных чисел.*

1.5 Некоммутативные группы

Помимо коммутативных групп в дальнейшем нам встретятся и некоммутативные группы, дадим поэтому общее определение группы.

Определение 1.43. *Группой* называется пара $(G,\, \cdot)$, состоящая из множества G и заданной на нем бинарной операции $\cdot$, обладающая следующими свойствами:

(i) операция $\cdot$ ассоциативна: для любых g_1, g_2, g_3 из G имеет место тождество $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$;

(ii) существует элемент $e \in G$, такой что $g \cdot e = g = e \cdot g$ для любого $g \in G$; такой элемент называется *нейтральным*;

(iii) для любого $g \in G$ существует *обратный* элемент, то есть такой $h \in G$, что $g \cdot h = e = h \cdot g$. Обратный для g обычно[5] обозначается g^{-1}.

Заметим, что если вдобавок к перечисленным условиям выполнено также условие коммутативности:

(iv) для любых $g_1, g_2 \in G$ имеет место равенство $g_1 \cdot g_2 = g_2 \cdot g_1$,

то мы снова возвращаемся к определению коммутативной группы (с тем единственным отличием от Определения 1.31, что для обозначения операции на этот раз вместо $+$ использован знак $\cdot$).

Задача 1.44. *Докажите, что*

1) нейтральный элемент в группе $(G, \cdot)$ единственен, то есть если $e' \in G$ — еще один элемент такой, что $g \cdot e' = g = e' \cdot g \ \ \forall\, g \in G$, то $e = e'$;

2) для каждого $g \in G$ обратный элемент g^{-1} единственен;

3) $\forall\, g, h \in G$ уравнения $x \cdot g = h, \quad g \cdot y = h$ имеют единственные решения (именно, $x = h \cdot g^{-1}$ и $y = g^{-1} \cdot h$ соответственно).

Кроме того, из ассоциативности операции в группе следует, что произведение произвольного конечного числа элементов группы не зависит от расстановки скобок. Читатель может попытаться доказать это, используя индукцию по числу элементов в произведении.

Определение 1.45. Непустое подмножество $H \subset G$ называется *подгруппой* группы $(G, \cdot)$, если $\forall\, h_1, h_2 \in H \ \Rightarrow \ h_1 \cdot h_2 \in H; \quad \forall\, h \in H \ \Rightarrow \ h^{-1} \in H$.

Заметим, что тогда пара $(H, \cdot)$[6] сама является группой. Нейтральный элемент группы G при этом будет нейтральным элементом в подгруппе $H \subset G$.

Ниже мы будем для группы $(G, \cdot)$ использовать упрощенное обозначение G если ясно, какая операция подразумевается.

Группы часто возникают как группы обратимых преобразований какого-либо множества, сохраняющих некоторую структуру на нем, с операцией — композицией преобразований. Читатель, вероятно, знает группу аффинных преобразований плоскости, которая

[5] при условии, если операция обозначается как умножение, что имеет место в нашем случае; если операцию записывать как сложение, то обратный к g естественно обозначить $(-g)$.

[6] чтобы не усложнять обозначения, операцию $\cdot$ на G и ее ограничение на подмножество $H \subset G$ мы обозначаем одним и тем же символом.

дает пример некоммутативной группы. Она содержит группу движений плоскости в качестве подгруппы (это такие преобразования плоскости, которые сохраняют расстояния между точками). Еще пример некоммутативной группы дает группа поворотов трехмерного пространства относительно фиксированной точки. Примерами некоммутативных групп из конечного числа элементов являются группы симметрий правильных многоугольников или многогранников. Например, группа всех симметрий правильного n-угольника — некоммутативная группа из $2n$ элементов.

В дальнейшем в курсе мы определим важные примеры некоммутативных групп — группу $\mathrm{GL}(V)$ невырожденных линейных преобразований n-мерного векторного пространства V над полем $\mathbb{K}$ (относительно операции композиции), а также группу $\mathrm{O}(V)$ ортогональных преобразований n-мерного евклидова пространства V. Выбор базиса в V определяет изоморфизм (см. Определение 4.1) группы $\mathrm{GL}(V)$ с группой $\mathrm{GL}_n(\mathbb{K})$ (относительно операции умножения) невырожденных матриц порядка n над полем $\mathbb{K}$ (соответственно в случае евклидова пространства выбор ортонормированного базиса определяет изоморфизм группы $\mathrm{O}(V)$ с группой $\mathrm{O}(n)$ ортогональных матриц порядка n[7]).

1.6 Кольца и поля

В математике большую роль играют множества, на которых заданы сразу две бинарные операции, которые в определенном смысле друг с другом согласованы. Вот определение важнейшего класса таких структур.

Определение 1.46. *Кольцом* называется множество R, на котором заданы две бинарные операции $+$ и $\cdot$, называемые соответственно *сложением* и *умножением*, причем

1) $(R, +)$ является абелевой группой;

2) сложение и умножение связаны законом дистрибутивности:

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca \quad \forall a,\, b,\, c \in R.$$

Следующие условия являются дополнительными и в произвольном кольце могут не выполняться:

- ассоциативность (мультипликативная) $(ab)c = a(bc)$;
- наличие мультипликативной единицы 1, то есть такого элемента, что $a1 = 1a = a$;
- коммутативность $ab = ba$.

[7] при этом упомянутая выше группа поворотов трехмерного пространства отождествляется с подгруппой ортогональных матриц порядка 3 и определителем, равным 1.

Эти условия выделяют специальные классы колец: ассоциативные кольца, кольца с единицей и коммутативные кольца соответственно.

Задача 1.47. *Докажите, что в произвольном кольце*

a) $a0 = 0a = 0 \ \ \forall a \in R$;

b) $a(-b) = (-a)b = -ab \ \ \forall a, b \in R$;

c) $a(b-c) = ab - ac$ *и* $(a-b)c = ac - bc \ \ \forall\, a, b, c \in R$.

Задача 1.48. *Докажите, что если в кольце существует мультипликативная единица, то она единственна.*

Замечание 1.49. Если $1 = 0$, то для любого элемента $a \in R$ имеем

$$a = a1 = a0 = 0,$$

т.е. кольцо состоит из одного нуля. Таким образом, если кольцо содержит более одного элемента, то $1 \neq 0$.

Целые числа дают важнейший пример ассоциативного коммутативного кольца с единицей. Еще одним примером такого кольца является кольцо многочленов над полем $\mathbb{K}$, обозначаемое $\mathbb{K}[x]$ (см. пункт 5.2).

Вот еще важный для дальнейшего пример.

Пример 1.50. В Примере 1.40 мы убедились, что $(\mathbb{Z}_n, +)$ — абелева группа и умножение классов вычетов $[k] \cdot [l] = [kl]$ по модулю n корректно определено. Дистрибутивность сложения относительно умножения следует из аналогичного свойства для кольца $\mathbb{Z}$:

$$[k] \cdot ([l] + [m]) = [k] \cdot [l + m] = [k(l + m)] = [kl + km] = [kl] + [km] = [k] \cdot [l] + [k] \cdot [m].$$

Таким образом, $(\mathbb{Z}_n, +, \cdot)$ — кольцо. Очевидно, оно ассоциативно, коммутативно и обладает единицей $[1]$. Кольцо $(\mathbb{Z}_n, +, \cdot)$ (или, кратко, $\mathbb{Z}_n$) называется *кольцом классов вычетов* по модулю n.

Элемент a^{-1} кольца с единицей называется *обратным* к элементу a, если

$$aa^{-1} = a^{-1}a = 1.$$

(В коммутативном кольце достаточно требовать, чтобы $aa^{-1} = 1$). Элемент, для которого существует обратный, называется *обратимым*.

Задача 1.51. *Докажите, что в ассоциативном кольце с единицей для любого элемента существует не более одного обратного.*

Задача 1.52. *Докажите, что в кольце $\mathbb{Z}_n$ элемент $[k]$ обратим тогда и только тогда, когда $(k, n) = 1$.*

Определение 1.53. Подмножество L кольца R называется *подкольцом*, если

1) $(L, +)$ является подгруппой $(R, +)$;

2) L замкнуто относительно умножения.

Очевидно, что всякое подкольцо само является кольцом относительно тех же операций. При этом оно наследует такие свойства, как коммутативность и ассоциативность.

Пример 1.54. Для любого $n \in \mathbb{N}$ подмножество $n\mathbb{Z} \subset \mathbb{Z}$ является подкольцом (без единицы при $n \neq 1$).

Теперь мы готовы дать определение по́ля.

Определение 1.55. *Полем* называется ассоциативное коммутативное кольцо $(\mathbb{K}, +, \cdot)$ с единицей 1, в котором $0 \neq 1$ и все ненулевые элементы обратимы.

Например, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ являются полями, а $(\mathbb{N}, +, \cdot)$ и $(\mathbb{Z}, +, \cdot)$ — нет (почему?).

В дальнейшем для упрощения обозначений вместо $(\mathbb{K}, +, \cdot)$ мы будем писать $\mathbb{K}$, считая операции сложения и умножения известными. Кроме того, мы, как правило, будем опускать точку при записи умножения.

Задача 1.56. *Докажите, что в любом поле* $\mathbb{K}$ *выполнено соотношение*

$$(-1)a = -a \ \ \forall\, a \in \mathbb{K}.$$

Определение 1.57. Подмножество $\mathbb{L}$ поля $\mathbb{K}$ называется *подполем*, если

1) $\mathbb{L}$ является подкольцом кольца $\mathbb{K}$;

2) $a \in \mathbb{L}$, $a \neq 0 \ \ \Rightarrow \ \ a^{-1} \in \mathbb{L}$;

3) $1 \in \mathbb{L}$.

Очевидно, всякое подполе является полем относительно тех же операций.

Например, $\mathbb{Q}$ является подполем в $\mathbb{R}$ и $\mathbb{C}$, а $\mathbb{R}$ — в $\mathbb{C}$. В то же время $\mathbb{Z}$ не является подполем в $\mathbb{Q}$.

Подполе поля комплексных чисел $\mathbb{C}$ иногда называется *числовым полем*. Существует множество числовых полей помимо перечисленных выше (например, поле чисел вида $a + b\sqrt{2}$, a, $b \in \mathbb{Q}$), есть также нечисловые поля. Часто наши конструкции работают над произвольным полем.

Есть поля с довольно экзотическими свойствами, например в некоторых выполняется тождество $1+1 = 0$. Примером такого поля является поле из двух элементов (это наименьшее возможное поле, поскольку в любом поле $0 \neq 1$). Читателю в качестве упражнения предлагается его построить.

Задача 1.58. *Докажите, что поле $\mathbb{Q}$ не имеет нетривиальных (то есть отличных от него самого) подполей.*

Задача 1.59. *Докажите, что кольцо классов вычетов $\mathbb{Z}_n$ является полем $\Leftrightarrow$ n является простым числом.*

1.7 Векторные пространства

В следующем определении нам понадобится понятие *внешней* бинарной операции, а именно произвольного отображения

$$\varphi\colon K \times L \to L,$$

где $K \neq L$.

Определение 1.60. *Векторным* (или *линейным*) *пространством* над полем $\mathbb{R}$ называется тройка $(V, +, \cdot)$, состоящая из множества V, на котором заданы две бинарные операции:

внутренняя, называемая *сложением*: $V \times V \xrightarrow{+} V$, $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} + \mathbf{v}$, и

внешняя, называемая *умножением* на числа ("скаляры") $\lambda \in \mathbb{R}$: $\mathbb{R} \times V \xrightarrow{\cdot} V$, $(\lambda, \mathbf{v}) \mapsto \lambda \cdot \mathbf{v}$,

удовлетворяющие следующим условиям ("аксиомам векторного пространства"):

1) $(V, +)$ — абелева группа (называемая *аддитивной группой векторного пространства* V);

2) умножение на скаляры обладает свойствами: a) $1 \cdot \mathbf{v} = \mathbf{v}$ $(1 \in \mathbb{R})$ $\forall\, \mathbf{v} \in V$, b) $(\lambda\, \mu) \cdot \mathbf{v} = \lambda \cdot (\mu \cdot \mathbf{v})$ $\forall\, \lambda, \mu \in \mathbb{R}$, $\forall\, \mathbf{v} \in V$;

3) сложение и умножение связаны законами дистрибутивности: a) $(\lambda + \mu) \cdot \mathbf{v} = \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{v}$ $\forall\, \lambda, \mu \in \mathbb{R}$, $\forall\, \mathbf{v} \in V$, b) $\lambda \cdot (\mathbf{u} + \mathbf{v}) = \lambda \cdot \mathbf{u} + \lambda \cdot \mathbf{v}$ $\forall\, \lambda \in \mathbb{R}$, $\forall\, \mathbf{u}, \mathbf{v} \in V$.

Элементы произвольного векторного пространства называются *векторами*. Заметим, что в определении векторного пространства вместо поля $\mathbb{R}$ можно взять произвольное поле $\mathbb{K}$, получив определение векторного пространства над полем $\mathbb{K}$. Линейные пространства над полем $\mathbb{R}$ называются *вещественными*, а над полем $\mathbb{C}$ — *комплексными*.

В дальнейшем мы будем опускать обозначение $\cdot$ умножения числа на вектор, записывая $\lambda \cdot \mathbf{v}$ просто как $\lambda\, \mathbf{v}$. Кроме того, вместо тройки $(V, +, \cdot)$ мы будем писать просто V, подразумевая, что операции в векторном пространстве ясны из контекста.

Укажем некоторые следствия аксиом векторного пространства, не являющиеся следствиями аксиом абелевой группы. Читателю предлагается доказать их в качестве задачи.

Задача 1.61. *Докажите, что в произвольном векторном пространстве $(V, +, \cdot)$ имеют место тождества:*

1) $\lambda\,\mathbf{0} = \mathbf{0} \quad \forall\,\lambda \in \mathbb{R}$;

2) $\lambda\,(-\mathbf{v}) = -\lambda\,\mathbf{v} \quad \forall\,\lambda \in \mathbb{R},\ \mathbf{v} \in V$;

3) $0\mathbf{v} = \mathbf{0} \quad \forall\,\mathbf{v} \in V$;

4) $(-1)\mathbf{v} = -\mathbf{v} \quad \forall\,\mathbf{v} \in V$.

Заметим, что приведенный в Определении 1.60 список аксиом векторного пространства 1)—3) не является независимым. Например, как показывает следующая задача, коммутативность аддитивной группы векторного пространства — следствие остальных аксиом.

Задача 1.62. *Докажите, что коммутативность сложения векторов является следствием остальных аксиом векторного пространства.*

Решение. Применяя оба варианта аксиомы дистрибутивности к выражению $(1+1)(u+v)$, получим $u+u+v+v = u+v+u+v$. Далее, прибавляя к обеим частям полученного тождества слева $(-u)$ и справа $(-v)$ и используя то, что $(V,\,+)$ — группа, получим $u+v = v+u$, то есть что эта группа коммутативна. ■

Интересный вопрос: всякая ли коммутативная группа изоморфна аддитивной группе некоторого векторного пространства (над каким-то полем)? Ответ на этот вопрос отрицательный. Читатель, знакомый с понятием характеристики поля, может попробовать доказать, что группа $\mathbb{Z}$ не изоморфна аддитивной группе никакого векторного пространства.

Рассмотрим примеры векторных пространств.

Пример 1.63. Множество $\mathrm{Mat}_{m\times n}(\mathbb{R})$ матриц данного размера $m \times n$ с операциями сложения и умножения на числа (в частности, множество столбцов высоты n, часто вместо $\mathrm{Mat}_{n\times 1}(\mathbb{R})$ обозначаемое $\mathbb{R}^n$) является векторным пространством над $\mathbb{R}$.

Пример 1.64. Множество комплексных чисел $\mathbb{C}$ можно рассматривать как двумерное векторное пространство над $\mathbb{R}$ с базисом $\{1,\,i\}$. Действительно, относительно сложения комплексные числа образуют абелеву группу; кроме того, операция умножения на действительные числа обладает требуемыми свойствами пункта 2) Определения 1.60 и, наконец, выполнены законы дистрибутивности из пункта 3) того же Определения. Кроме того, всякое комплексное число $z \in \mathbb{C}$ однозначно записывается в виде $\lambda \cdot 1 + \mu \cdot i$, где $\lambda,\,\mu \in \mathbb{R}$, следовательно, $\{1,\,i\}$ — базис в векторном пространстве $\mathbb{C}$ над полем $\mathbb{R}$. Это дает возможность изображать комплексные числа векторами на плоскости[8]. Про связь геометрии евклидовой плоскости с комплексными числами можно почитать, например, в [3].

Пример 1.65. Из курса аналитической геометрии (см. например [10]) читателю должны быть известны “геометрические” примеры вещественных векторных пространств — пространства свободных векторов на плоскости и в пространстве относительно обычных операций сложения векторов и умножения их на числа (см. Пример 1.22 и Задачу 1.41).

[8] заметим, что вместо $\{1,\,i\}$ в качестве базиса в $\mathbb{C}$ над $\mathbb{R}$ можно взять любую упорядоченную пару неколлинеарных векторов на плоскости $\mathbb{C}$.

Определение 1.66. Пусть $U \subset V$ — подмножество множества векторов векторного пространства $(V, +, \cdot)$ такое, что

1) $(U, +)$ — подгруппа аддитивной группы $(V, +)$;

2) $\mathbf{u} \in U \;\Rightarrow\; \lambda\,\mathbf{u} \in U \;\; \forall\, \lambda \in \mathbb{R}$.

Тогда $(U, +, \cdot)$ называется векторным (= линейным) *подпространством* пространства $(V, +, \cdot)$.

Заметим, что подпространство само является векторным пространством относительно операций, ограниченных с объемлющего пространства.

Приведем некоторые примеры векторных подпространств.

Самое "маленькое" подпространство в $(V, +, \cdot)$ состоит только из нулевого вектора, самое "большое" — совпадает со всем пространством $(V, +, \cdot)$.

Если зафиксировать какую-нибудь прямую на плоскости или в трехмерном пространстве, то множество всех свободных векторов, параллельных ей, образуют подпространство в пространстве свободных векторов соответственно на плоскости или в пространстве. То же для фиксированной плоскости в пространстве. Подпространство образует также подмножество всех симметричных (или кососимметричных) матриц в $\mathrm{Mat}_n(\mathbb{R})$. Множество действительных чисел $\mathbb{R}$ является (вещественным) подпространством пространства $\mathbb{C}$ из Примера 1.64.

Важным результатом о системах линейных уравнений является то, что множество всех решений *однородной* системы является линейным пространством (подпространством в пространстве столбцов высоты, равной числу неизвестных). Более того, любое подпространство в $\mathbb{R}^n$ можно задать как пространство решений некоторой системы линейных однородных уравнений от n неизвестных.

1.8 Базисы

Пусть V — векторное пространство.

Определение 1.67. *Системой* n ($n \in \mathbb{N} \cup \{0\}$) векторов пространства V называется произвольное отображение $f\colon \{1, 2, \ldots, n\} \to V$.

Заметим, что при $n = 0$ получаем *пустую систему*, состоящую из пустого множества векторов.

Систему n векторов мы будем записывать в виде $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, где $f(k) = \mathbf{v}_k, \quad k = 1, \ldots, n$. Заметим, что система векторов отличается от подмножества двумя свойствами: во-первых, векторы системы имеют естественный порядок (занумерованы числами $1, 2, \ldots, n$), и, во-вторых, в систему элемент может входить более одного раза (то есть возможны повторения).

Линейной комбинацией системы векторов $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ пространства V называется выражение вида

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n.$$

После проведения всех вычислений (умножений на скаляры и сложений) такое выражение будет некоторым конкретным вектором $\mathbf{v} \in V$. В этом случае говорят, что вектор $\mathbf{v}$ *представляется в виде линейной комбинации* системы $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ или *раскладывается* по данной системе. По определению, линейная комбинация пустой системы векторов равна нулевому вектору.

Вообще говоря, данный вектор может раскладываться по данной системе векторов многими способами. Оказывается, единственность (или неединственность) разложения векторов по данной системе — свойство системы, а не конкретного вектора, который мы по ней раскладываем. Другими словами, если какой-то один вектор раскладывается по системе неединственным образом, то это верно и для любого другого вектора, который по ней раскладывается. Такие системы называются *линейно зависимыми*.

Напомним формальное определение. Система $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ называется *линейно независимой*, если нулевой вектор по ней раскладывается единственным образом — с нулевыми коэффициентами, то есть если из $\lambda_1\mathbf{v}_1+\lambda_2\mathbf{v}_2+\ldots+\lambda_n\mathbf{v}_n = \mathbf{0}$ следует, что $\lambda_1 = \ldots = \lambda_n = 0$. В противном случае система линейно зависима.

То есть система $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *линейно зависима*, если найдется набор $\lambda_1, \ldots, \lambda_n$ элементов из $\mathbb{R}$, среди которых не все нулевые, такой, что $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n = \mathbf{0}$.

Из курса аналитической геометрии читателю должны быть известны характеризации линейно зависимых и независимых систем в пространствах размерности 1, 2 и 3 (вроде “три вектора линейно зависимы тогда и только тогда, когда они компланарны”). Это, в частности, наглядно демонстрирует то, что за исключением тривиальных случаев, в данном пространстве много разных базисов.

Определение 1.68. *Базисом* в векторном пространстве V называется такая система векторов $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ пространства V, что произвольный вектор $\mathbf{v} \in V$ однозначно представляется в виде линейной комбинации

$$\mathbf{v} = v_1\mathbf{e}_1 + \ldots + v_n\mathbf{e}_n \tag{3}$$

векторов данной системы. Упорядоченный набор чисел $(v_1, \ldots, v_n)$ называется *координатами вектора* $\mathbf{v}$ *в базисе* $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$[9].

Однозначность разложения (3) (при условии существования) равносильна линейной независимости системы $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, в то время как существование разложения произвольного вектора связано с максимальностью такой системы среди всех линейно независимых систем.

[9]Координаты вектора обычно записываются в столбец.

Не во всяком векторном пространстве есть базис в смысле данного выше определения. Ниже мы докажем теорему о том, что если в пространстве существует базис из n векторов, то любой другой базис этого пространства также содержит n векторов. Число элементов произвольного базиса (при условии существования) в V называется *размерностью* пространства V и обозначается $\dim V$. В пространстве, состоящем только из нулевого вектора, базисом по определению является пустая система (и, таким образом, его размерность равна нулю). Если базиса в линейном пространстве (в смысле данного выше определения) не существует, то можно считать что $\dim V = \infty$.

В данном курсе мы в основном будем заниматься пространствами, в которых есть базис в указанном смысле; такие пространства называются *конечномерными*.

1.9 Алгебры над полем

Многие интересные кольца являются одновременно векторными пространствами, причем эти алгебраические структуры в определенном смысле согласованы. Это сильно облегчает изучение таких колец, поэтому дадим соответствующее определение.

Определение 1.69. *Алгеброй над полем* $\mathbb{K}$ называется множество A, снабженное тремя операциями (двумя внутренними и одной внешней):

$$A \times A \to A, \quad (a_1,\, a_2) \mapsto a_1 + a_2, \quad A \times A \to A, \quad (a_1,\, a_2) \mapsto a_1 a_2,$$

$$\mathbb{K} \times A \to A, \quad (\lambda,\, a) \mapsto \lambda a,$$

называемыми соответственно сложением, умножением и умножением на скаляры (=элементы поля $\mathbb{K}$), обладающими следующими свойствами:

1) относительно операций сложения и умножения A является кольцом;

2) относительно сложения и умножения на скаляры A является векторным пространством;

3) $(\lambda a)b = a(\lambda b) = \lambda(ab) \;\; \forall\, \lambda \in \mathbb{K},\; a,\, b \in A.$

Коротко можно сказать, что алгебра состоит из векторного пространства V с заданным на нем билинейным отображением $V \times V \to V$. (В самом деле, последнее задает умножение в алгебре, и его билинейность равносильна дистрибутивности и условию 3) из Определения выше).

Алгебра называется ассоциативной (коммутативной, с единицей), если соответствующее кольцо ассоциативно (коммутативно, с единицей).

Основным для нас примером ассоциативной алгебры над полем $\mathbb{K}$ будет алгебра линейных операторов на векторном пространстве V над полем $\mathbb{K}$, обозначаемая $\mathcal{L}(V)$. В ней операции сложения, умножения и умножения на скаляры задаются соответственно

сложением линейных операторов, их композицией и умножением операторов на скаляры. Выбор базиса в V определяет некоторый изоморфизм $\mathcal{L}(V)$ с алгеброй матриц $\mathrm{Mat}_n(\mathbb{K})$, где $n = \dim V$ (изоморфизм — биекция, сохраняющая все операции). Алгебра $\mathcal{L}(V)$ обладает единицей (тождественным оператором) и некоммутативна при $n > 1$.

Пример коммутативной ассоциативной алгебры с единицей над полем $\mathbb{K}$ дает алгебра многочленов $\mathbb{K}[x]$. Поле комплексных чисел $\mathbb{C}$ является алгеброй над полем $\mathbb{R}$. Более того, если $\mathbb{F}$ — подполе поля $\mathbb{K}$, то $\mathbb{K}$ является $\mathbb{F}$-алгеброй. В частности, $\mathbb{R}$ и $\mathbb{C}$ являются алгебрами над полем $\mathbb{Q}$. Интересным примером алгебры над полем $\mathbb{R}$ является алгебра кватернионов $\mathbb{H}$[10], которая является ассоциативной некоммутативной алгеброй с единицей, в которой всякий ненулевой элемент обратим. Таким образом, $\mathbb{H}$ является некоммутативным аналогом поля; такие алгебраические структуры называются *телами*. Можно распространить понятие векторного пространства на случай, когда вместо основного поля рассматривается тело, только в случае тел нужно различать понятия левого и правого векторного пространства[11].

Примером неассоциативной алгебры является 3-мерное евклидово ориентированное пространство с векторным произведением в качестве умножения. Это пример алгебры из важнейшего класса неассоциативных алгебр — алгебр Ли.

Заметим, что иногда бывает полезно забыть часть алгебраической структуры. Например, забывая структуру векторного пространства на алгебре $\mathbb{K}[x]$, мы получаем кольцо $\mathbb{K}[x]$ (обозначаемое обычно тем же символом, что редко приводит к путанице).

2 Алгебра матриц

Данный раздел посвящен изучению операций с матрицами, которые представляют собой основной вычислительный аппарат линейной алгебры.

2.1 Определение и виды матриц

Определение 2.1. *Матрицей* размера $m \times n$ с элементами из поля $\mathbb{K}$ называется прямоугольная таблица

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{4}$$

с $a_{ij} \in \mathbb{K}$, $1 \le i \le m$, $1 \le j \le n$, в которой m строк и n столбцов.

[10] Подробнее о кватернионах написано в книгах [3], [11], [6].

[11] Можно пойти еще дальше, введя объекты, аналогичные векторным пространствам, для которых роль поля играет ассоциативное кольцо с единицей R. Такие объекты существуют и играют очень важную роль в алгебре. Они называются *модулями*. Мы немного расскажем о них в параграфе 9.6.

Читатель заметил, что в нашей записи элемент a_{ij} матрицы стоит на пересечении i-й строки и j-го столбца. То есть первый индекс обозначает номер строки, второй — столбца. Матрицы мы будем обозначать заглавными латинскими буквами $A, B, C, \ldots$. Краткая запись матрицы (4)

$$A = (a_{ij})_{\substack{1\le i\le m,\\ 1\le j\le n}}$$

или просто $A = (a_{ij})$, если размеры уже указаны.

Если число столбцов $n = 1$, то матрица называется *столбцом*, если число строк $m = 1$, то матрица называется *строкой*. Если число строк равно числу столбцов, то есть $m = n$, то матрица называется *квадратной*. Квадратную матрицу размера $n \times n$ также называют матрицей *порядка* n. *Главная диагональ* матрицы A порядка n образована элементами a_{ii}, $1 \le i \le n$. Квадратная матрица называется *диагональной*, если все ее элементы вне главной диагонали равны нулю: $a_{ij} = 0$ при $i \ne j$. Другими словами, все ее ненулевые элементы (если они есть) стоят на главной диагонали. Диагональную матрицу порядка n с элементами $\lambda_1, \ldots, \lambda_n$ на главной диагонали мы в дальнейшем иногда будем обозначать $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Матрица порядка n называется *единичной*, если она диагональна и на главной диагонали стоят единицы:

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Единичная матрица порядка n обозначается E_n или просто E.

Пусть $\mathrm{Mat}_{m\times n}(\mathbb{K})$ (соответственно $\mathrm{Mat}_n(\mathbb{K})$) обозначает множество всех $m \times n$-матриц (соответственно матриц порядка n) над полем $\mathbb{K}$. Заметим, что две матрицы A и B над одним и тем же полем *равны*, если они имеют одинаковые размеры и соответствующие элементы матриц равны, $a_{ij} = b_{ij}$.

2.2 Операции с матрицами

Для любых двух матриц A, $B \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ одинакового размера определена их *сумма* $A+B \in \mathrm{Mat}_{m\times n}(\mathbb{K})$, которая является матрицей того же размера. Матрицы складываются покомпонентно: если $C := A + B$, $C = (c_{ij})$, то

$$c_{ij} = a_{ij} + b_{ij}, \quad 1 \le i \le m,\ 1 \le j \le n.$$

Из определения суммы матриц и свойств операции сложения элементов поля сразу следуют свойства операции сложения матриц:

1) $\forall A,\ B,\ C \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \quad (A + B) + C = A + (B + C)$ (*ассоциативность* сложения матриц);

2) $\exists O \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ (а именно, *нулевая* матрица, состоящая из одних нулей) такая, что $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K})\ \ A+O = A = O+A$ (существование *нейтрального*, в данном случае нулевого, элемента);

3) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K})\ \exists(-A) \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ (*противоположная* к A матрица, у которой на (i,j)-м месте стоит $-a_{ij}$) такая, что $A+(-A) = O = (-A)+A$ (существование *обратного*, в данном случае противоположного элемента);

4) $\forall A,\ B \in \mathrm{Mat}_{m\times n}(\mathbb{K})\quad A+B = B+A$ (*коммутативность* сложения матриц).

Выполнение условий 1)—3) означает, что множество $\mathrm{Mat}_{m\times n}(\mathbb{K})$ с операцией сложения является *группой*, а дополнительное условие 4) означает, что эта группа *коммутативна*, или *абелева*.

Кроме того, для любой матрицы $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ и элемента поля (= скаляра) $\lambda \in \mathbb{K}$ определена матрица $A' := \lambda A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ с элементами $a'_{ij} = \lambda a_{ij},\ \ 1 \le i \le m,\ 1 \le j \le n$ (то есть λA получается из A умножением всех ее элементов на λ).

Из определения легко выводятся свойства операции умножения матриц на скаляры:

5) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K}),\ \forall\,\lambda,\ \mu \in \mathbb{K}\quad (\lambda\mu)A = \lambda(\mu A)$;

6) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K})\quad 1A = A$ (здесь 1 обозначает единицу поля $\mathbb{K}$).

Кроме того, непосредственно проверяется, что операции сложения матриц и умножения матриц на скаляры связаны *законами дистрибутивности:*

7) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K}),\ \forall\,\lambda,\ \mu \in \mathbb{K}\quad (\lambda+\mu)A = \lambda A + \mu A$;

8) $\forall A,\ B \in \mathrm{Mat}_{m\times n}(\mathbb{K}),\ \forall\lambda \in \mathbb{K}\quad \lambda(A+B) = \lambda A + \lambda B$.

Выполнение свойств 1)—8) означает, что имеет место следующая Теорема.

Теорема 2.2. *Для любой пары натуральных чисел m, n множество* $\mathrm{Mat}_{m\times n}(\mathbb{K})$ *матриц размера $m \times n$ с операциями сложения и умножения на скаляры является векторным пространством (см. Определение 1.60) над полем* $\mathbb{K}$.

Определим mn матриц

$$E_{ij} = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \dots & 0 & \dots & 1 & \dots \\ & \vdots & \ddots & \vdots & \\ \dots & 0 & \dots & 0 & \dots \\ & \vdots & & \vdots & \ddots \end{pmatrix} \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \quad 1 \le i \le m,\ 1 \le j \le n,$$

в которых единственный ненулевой элемент — единица, стоя́щая на пересечении i-й строки и j-го столбца. Эти матрицы называются *матричными единицами* (не путать с единичной матрицей). Они образуют базис в пространстве $\mathrm{Mat}_{m\times n}(\mathbb{K})$. Действительно, произвольная матрица $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ единственным образом раскладывается по нему следующим образом:

$$A = \sum_{1\le i\le m,\, 1\le j\le n} a_{ij}E_{ij},$$

то есть координатами являются ее матричные элементы.

Перейдем теперь к наиболее интересной и наименее тривиальной операции над матрицами — их произведению. Конечно, можно было бы определить произведение двух матриц $A = (a_{ij})$, $B = (b_{ij})$ одинаковых размеров $m \times n$ как такую матрицу $C = (c_{ij})$, что $c_{ij} = a_{ij}b_{ij}$, но это "произведение"[12] не представляет для нас интереса, хотя и обладает рядом "хороших" свойств. "Настоящее" произведение матриц определяется иначе.

Произведение AB матрицы A размера $m \times n$ на матрицу B размера $k \times p$ существует тогда и только тогда, когда $n = k$, то есть когда число столбцов первой матрицы равно числу строк второй (значит, произведение BA существует тогда и только тогда, когда $p = m$), и в последнем случае имеет размер $m \times p$ (соотв. $k \times n$). Все это будет следовать из определения произведения матриц, которое мы сейчас дадим.

Итак, пусть $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(\mathbb{K})$, $B = (b_{ij}) \in \mathrm{Mat}_{n\times p}(\mathbb{K})$. Тогда у матрицы $C = AB = (c_{ij})$ элемент c_{ij} вычисляется по формуле

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \quad 1 \le i \le m,\ 1 \le j \le p, \tag{5}$$

то есть является суммой произведений элементов i-й строки матрицы A на соответствующие элементы j-го столбца матрицы B (кратко это правило может быть сформулировано так: матрицы перемножаются по правилу "строка на столбец"). Чтобы такое произведение было определено, нужно, чтобы длина строк матрицы A была равна высоте столбцов матрицы B. Кроме того, индекс i пробегает номера строк матрицы A, а j — номера столбцов матрицы B, отсюда получаем, что произведение AB является матрицей размера $m \times p$, как и утверждалось.

Замечание 2.3. Так как правило умножения матриц на первый взгляд выглядит искусственно, приведем две его интерпретации — одну практическую, другую — физическую.

Предположим, что имеется m предприятий, выпускающих n видов изделий. Через a_{ij} обозначим количество изделий j-го вида, выпускаемых i-м предприятием за один год (мы предполагаем, что эта величина постоянна год от года). Пусть A — матрица размера $m\times n$ с элементами a_{ij}. Пусть b_{jk} обозначает стоимость изделия j-го вида в k-м году, где $1 \le k \le s$. Из чисел b_{jk} составим матрицу B размера $n\times s$. Тогда легко видеть, что (i,k)-й элемент матрицы AB — стоимость продукции, выпущенной i-м предприятием за k-й год.

[12] оно называется *произведением Адамара*.

Приведем теперь физическую интерпретацию умножения матриц[13] (для простоты рассмотрим случай квадратных матриц). Пусть у нас есть физическая система с n состояниями $\{1, 2, \ldots, n\}$ (например, с n уровнями энергии). Матрица A порядка n описывает применение к указанной системе некоторого физического воздействия. Более точно, ее i, j-й элемент a_{ij} является "амплитудой перехода" из состояния i в состояние j[14]. Например, если амплитуда перехода из состояния i в состояние j равна амплитуде обратного перехода, то матрица A будет симметричной (определение симметричной матрицы см. ниже). Пусть помимо физического воздействия на систему, отвечающего матрице A, есть также физическое воздействие, описываемое матрицей B. Какой матрице C отвечает применение сначала воздействия A, а затем воздействия B? Сделаем физическое предположение: если процесс является композицией процессов, то его амплитуда есть произведение амплитуд, а если процесс может произойти несколькими альтернативными путями, то его амплитуда является суммой амплитуд всех таких путей. Тогда амплитуда c_{ij} перехода из состояния i в состояние j в результате указанной композиции воздействий в точности дается выражением (5). Действительно, указанное выражение говорит нам, что система из состояния i в состояние j может перейти через любое промежуточное состояние $1, 2, \ldots, n$ и произведение $a_{ik}b_{kj}$ есть амплитуда перехода из i в j через промежуточное состояние k[15].

Разберем несколько частных случаев умножения матриц. Например, определено произведение строки длины n на столбец высоты n, которое является матрицей размера 1×1[16]. В обратном порядке их произведение также определено и является уже матрицей размера $n \times n$.

Задача 2.4. *Проверьте, что матричные единицы E_{ij} перемножаются по следующему правилу:*

$$E_{ij}E_{kl} = \delta_{jk}E_{il}. \tag{6}$$

Задача 2.5. *Покажите, что умножение произвольной матрицы $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ на матричную единицу E_{ij} порядка m слева дает матрицу $E_{ij}A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$, у которой в i-й строке стоит j-я строка матрицы A, а в остальных местах нули. Аналогично, умножение матрицы A на матричную единицу E_{ij} порядка n справа дает матрицу, у которой в j-м столбце стоит i-й столбец матрицы A, а в остальных местах — нули.*

Задача 2.6. *Любую ли матрицу размера $m \times n$ можно представить в виде произведения столбца высоты m на строку длины n при $m, n > 1$?*

Также определено произведение $A\mathbf{b}$ матрицы A размера $m \times n$ на столбец $\mathbf{b}$ высоты n,

[13] Физический смысл с точки зрения квантовой механики она имеет для комплексных матриц.

[14] Для комплексных матриц квадрат модуля амплитуды равен вероятности.

[15] Интересно заметить, что в случае комплексных амплитуд при вычислении квадрата модуля c_{ij} возникают характерные для квантовой механики интерференционные эффекты между разными путями, которыми данный переход $i \mapsto j$ может произойти.

[16] Заметим, что считать матрицу порядка 1 "просто числом" неправильно: число (скаляр) можно умножать на любую матрицу, в то время как матрицу порядка 1 можно умножать слева только на строку, а справа — только на столбец.

которое является столбцом высоты m. Посчитаем это произведение:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + a_{12}b_2 + \dots + a_{1n}b_n \\ a_{21}b_1 + a_{22}b_2 + \dots + a_{2n}b_n \\ \dots \\ a_{m1}b_1 + a_{m2}b_2 + \dots + a_{mn}b_n \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} b_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} b_2 + \dots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} b_n. \tag{7}$$

Таким образом, столбец $A\mathbf{b}$ является линейной комбинацией столбцов матрицы A с коэффициентами из столбца $\mathbf{b}$.

Пусть $\mathbf{b}_i$, $i = 1, \dots, p$ — столбцы матрицы B, то есть $B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_p)$. Тогда из определения умножения матриц следует, что $AB = (A\mathbf{b}_1, A\mathbf{b}_2, \dots, A\mathbf{b}_p)$, то есть i-й столбец матрицы AB есть произведение A на $\mathbf{b}_i$. Таким образом, нами доказано следующее Предложение.

Предложение 2.7. *i-й столбец матрицы AB ($i = 1, \dots, p$) является линейной комбинацией столбцов матрицы A с коэффициентами из i-го столбца матрицы B. Аналогично, i-я строка матрицы AB является линейной комбинацией строк матрицы B с коэффициентами из i-й строки матрицы A.*

Пример 2.8. Заметив, что столбцы $\{c_1, c_2, c_3\}$ матрицы

$$C := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

связаны соотношением $2c_2 = c_1 + c_3$, представим ее в виде произведения матриц A и B размеров соответственно 3×2 и 2×3. В качестве A возьмем, например, матрицу, состоящую из первых двух столбцов C, тогда в качестве B необходимо взять матрицу, в i-м столбце которой стоят коэффициенты разложения i-го столбца матрицы A по выбранной системе столбцов (в нашем случае это c_1 и c_2), то есть $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 4 & 5 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$.

Заметим, что не любую матрицу порядка 3 можно представить в виде произведения матриц размеров 3×2 и 2×3 а только такую, столбцы которой линейно зависимы.

Следующее Предложение проверяется прямым вычислением (или, даже проще, выводится из ассоциативности произведения базисных элементов — матричных единиц (ср. формулу (6)).

Предложение 2.9. *Умножение матриц ассоциативно всякий раз когда оно определено. То есть если одно из произведений $(AB)C$ или $A(BC)$ существует, то существует и другое, и они равны: $(AB)C = A(BC)$ (в частности, это всегда верно для квадратных матриц одного порядка). Кроме того, если $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$, то $E_m A = A = AE_n$, где E_m и E_n — единичные матрицы порядков m и n соответственно.*

В дальнейшем, при изучении связи матриц с линейными отображениями, мы получим более концептуальную интерпретацию свойств операций с матрицами.

Замечание 2.10. Как уже отмечалось выше, произведение строки длины n на столбец высоты n — матрица порядка 1, а не число. Действительно, в противном случае нарушилась бы ассоциативность: произведение матриц $((1 \times n)(n \times 1))(m \times k)$ было бы определено, а $(1 \times n)((n \times 1)(m \times k))$ при $m \neq 1$ — нет.

Кроме того, сложение и умножение матриц связаны законами дистрибутивности:

$$A(B + C) = AB + AC, \quad (A + B)C = AC + BC$$

и для любого $\lambda \in \mathbb{K}$ выполнены равенства $(\lambda A)B = A(\lambda B) = \lambda(AB)$ (всюду размеры матриц предполагаются согласованными, чтобы операции имели смысл).

Из сформулированных свойств сложения и умножения матриц а также их умножения на скаляры следует, что множество $\mathrm{Mat}_n(\mathbb{K})$ матриц фиксированного порядка n относительно указанных операций является ассоциативной алгеброй с единицей над полем $\mathbb{K}$.

Задача 2.11. *Покажите, что при умножении произвольной матрицы $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$ на матрицу $P_{ij}(\lambda) := E + \lambda E_{ij}$ (см. (10)) порядка m слева дает матрицу $P_{ij}(\lambda)A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$, которая получается из A прибавлением к i-й строке ее j-й строки, умноженной на λ. Аналогично, умножение матрицы A на на матрицу $P_{ij}(\lambda) := E + \lambda E_{ij}$ порядка n справа дает матрицу, которая получается из A прибавлением к j-му столбцу ее i-го столбца. (Указание: используйте задачу 2.5).*

Перечисленные до сих пор свойства умножения в случае квадратных матриц фиксированного порядка (ассоциативность, существование нейтрального элемента, дистрибутивность относительно сложения) аналогичны свойствам умножения чисел. Однако есть и принципиальные отличия. Во-первых, умножение (даже квадратных) матриц, вообще говоря, некоммутативно. Читатель легко убедится в этом, перемножив, например, матрицы

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{8}$$

Две матрицы A, B называются *перестановочными*, если $AB = BA$ (в частности, они обязательно квадратные одного порядка). Матрицы вида λE (где E, как обычно, обозначает единичную матрицу) называются *скалярными*.

Задача 2.12. *Докажите, что матрица данного порядка n перестановочна со всеми матрицами порядка n тогда и только тогда, когда она скалярна.*

Во-вторых, пример с матрицами (8) показывает, что произведение ненулевых матриц может равняться нулевой матрице. Есть даже ненулевые матрицы, некоторая степень которых равна нулевой матрице (например, квадрат второй из матриц (8)). С этим связано третье отличие: не всякая ненулевая матрица имеет обратную.

Определение 2.13. Матрица B называется *обратной* для матрицы A, если

$$AB = E = BA.$$

Матрица, для которой существует обратная, называется *обратимой*. Обратная матрица обычно обозначается A^{-1}.

Замечание 2.14. Легко видеть, что предыдущее определение имеет смысл только для квадратных матриц. Мотивировка его следующая: число b называется обратным для числа a, если $ab = 1$; аналогом числа 1 (нейтрального элемента по умножению) в случае квадратных матриц является единичная матрица; из-за некоммутативности умножения матриц помимо равенства $AB = E$ требуется также выполнение равенства $BA = E$.

Задача 2.15. *Докажите, что если обратная матрица для данной матрицы существует, то она единственна.*

Задача 2.16. *Докажите, что произведение обратимых матриц одинакового порядка обратимо.*

Задача 2.17. *Пусть для матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$ существует такая ненулевая матрица $C \in \mathrm{Mat}_{n\times p}(\mathbb{K})$, что $AC = O$. Тогда для A не может существовать обратной.*

Задача 2.18. *Докажите, что для матриц из $AB = AC$, вообще говоря, не следует $B = C$. Каков критерий того, что на A можно сокращать слева (справа)?*

Из-за некоммутативности умножения матриц матричные уравнения $AX = B$ и $YA = B$, даже если матрица A обратима, имеют, вообще говоря, разные решения $X = A^{-1}B \neq BA^{-1} = Y$. То есть для матриц есть левое и правое деления.

Не следует думать, что перечисленные "отрицательные" свойства являются "недостатками" операций с матрицами. Например, матрицы можно использовать для описания поворотов трехмерного пространства, причем композиция последних отвечает произведению матриц. Легко проверить, что композиция поворотов, вообще говоря, некоммутативна. Поэтому возможность данного применения матриц связана с некоммутативностью их произведения. Кроме того, матрицы используются в математическом аппарате квантовой механики и некоммутативность их умножения связана с соотношением неопределенностей Гейзенберга.

Есть еще одна важная операция с матрицами — транспонирование. Пусть A — матрица размера $m \times n$. Тогда ее транспонированная матрица A^T имеет размер $n \times m$ и характеризуется тем, что ее i-й столбец равен i-й строке матрицы A при $i = 1, \ldots, m$. Если $A^T = (a_{ij}^T)$, то $a_{ij}^T = a_{ji}$.

Предложение 2.19. *Операция транспонирования матриц* $\mathrm{Mat}_{m\times n}(\mathbb{R}) \to \mathrm{Mat}_{n\times m}(\mathbb{R})$, $A \mapsto A^T$ *обладает следующими свойствами:*

1) $\forall A, B \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ $(A+B)^T = A^T + B^T$;

2) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, $\lambda \in \mathbb{R}$ $(\lambda A)^T = \lambda A^T$

3) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ $(A^T)^T = A$ *(в частности, любая матрица является транспонированной к некоторой, а именно к* A^T*);*

4) $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$, $B \in \mathrm{Mat}_{n\times k}(\mathbb{R})$ $(AB)^T = B^T A^T$;

5) При условии что $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$*, обратима,* $(A^T)^{-1} = (A^{-1})^T$.

Доказательство. Проверка первых трех свойств тривиальна. Докажем последние два.

4) Обозначим $C := AB$. Имеем

$$c_{ki}^T = c_{ik} = \sum_j a_{ij} b_{jk} = \sum_j b_{jk} a_{ij} = \sum_j b_{kj}^T a_{ji}^T,$$

откуда и следует требуемое $C^T = B^T A^T$.

5) Проверим, что обратной к $(A^{-1})^T$ является A^T. В самом деле,

$$A^T (A^{-1})^T = (A^{-1} A)^T = E, \quad (A^{-1})^T A^T = (A A^{-1})^T = E.$$

Тогда в силу единственности обратной матрицы $(A^{-1})^T = (A^T)^{-1}$. ∎

Матрица A называется *симметричной* (соответственно *кососимметричной*), если $A^T = A$ (соответственно $A^T = -A$). Легко видеть, что матрица A симметрична (соответственно кососимметрична) тогда и только тогда, когда все ее матричные элементы удовлетворяют тождеству $a_{ij} = a_{ji}$ (соответственно тождеству $a_{ij} = -a_{ji}$). То есть в симметричной матрице (которая обязательно является квадратной) на симметричных относительно главной диагонали местах стоят равные элементы, а у кососимметричной такие элементы отличаются знаком (в частности, на главной диагонали кососимметричной матрицы стоят нули).

Множество всех симметричных (соответственно кососимметричных) матриц порядка n обозначим $\mathrm{Mat}_n^+(\mathbb{R})$ (соответственно $\mathrm{Mat}_n^-(\mathbb{R})$).

Задача 2.20. *Используя свойства 1) и 2) из предыдущего Предложения докажите, что множества* $\mathrm{Mat}_n^+(\mathbb{R})$ *и* $\mathrm{Mat}_n^-(\mathbb{R})$ *являются линейными подпространствами (см. Определение 1.66) в* $\mathrm{Mat}_n(\mathbb{R})$*. Каковы их размерности?*

Следующая задача показывает, что можно построить такую биекцию между комплексными числами и некоторым двумерным пространством вещественных матриц порядка 2, что сложение и умножение комплексных чисел перейдут соответственно в сложение и умножение матриц.

В самом деле, рассмотрим подпространство матриц

$$A := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,\, b \in \mathbb{R} \right\} \subset \mathrm{Mat}_2(\mathbb{R}).$$

Из представления $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = aE + bJ$, где $J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ легко видеть, что A — двумерное векторное пространство над $\mathbb{R}$ с базисом $\{E,\, J\}$. Также легко проверить, что $J^2 = -E$ (матричный аналог соотношения $i^2 = -1$).

Оказывается, A — не просто подпространство в $\mathrm{Mat}_2(\mathbb{R})$, а кольцо, и даже поле, изоморфное полю $\mathbb{C}$ (относительно обычных операций сложения и умножения матриц).

Задача 2.21. *Докажите, что отображение*

$$\varphi\colon \mathbb{C} \to A, \quad \varphi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

определяет изоморфизм поля $\mathbb{C}$ с полем матриц указанного вида. Более подробно, проверьте, что φ биективно и сохраняет операции, то есть $\varphi((a+bi)+(c+di)) = \varphi(a+bi)+\varphi(c+di)$ и $\varphi((a+bi)(c+di)) = \varphi(a+bi)\varphi(c+di)$.

Также докажите, что ограничение φ на $\{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}$ определяет изоморфизм группы из Задачи 1.37 с группой матриц поворотов (с операцией умножения). Как это связано с формулой Эйлера $e^{i\alpha} = \cos\alpha + i\sin\alpha$?

В частности, из предыдущей задачи следует, что все ненулевые матрицы вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ обратимы. Читателю предлагается получить явное выражение для обратной матрицы.

2.3 Элементарные преобразования

В этом разделе мы введем и начнем изучать элементарные преобразования строк и столбцов матриц, которые будут играть важную роль в дальнейшем.

Пусть A — произвольная матрица размера $m \times n$. Определим элементарные преобразования ее строк.

Определение 2.22. *Элементарным преобразованием типа I* строк матрицы A называется прибавление к некоторой ее строке (скажем, с номером $i,\ 1 \le i \le m$) некоторой другой ее строки (скажем, с номером $j,\ 1 \le j \le m,\ j \ne i$), умноженной на некоторое число λ (при этом остальные строки кроме i-й не меняются).

Элементарным преобразованием типа II строк матрицы A называется перестановка местами двух ее строк (скажем i-й и j-й, $1 \le i \ne j \le m$).

Элементарным преобразованием типа III строк матрицы A называется умножение некоторой ее строки (скажем, с номером $i,\ 1 \le i \le m$) на *ненулевое* число c.

Аналогично определяются три типа элементарных преобразований столбцов.

Заметим, что элементарные преобразования обратимы, то есть для каждого элементарного преобразования строк матриц с m строками существует (причем единственное) элементарное преобразование строк такое, что их композиция (последовательное выполнение) есть *тождественное преобразование* на множестве матриц с m строками (которое само является элементарным преобразованием типа I (при $\lambda = 0$) или типа III (при $c = 1$)). Например, для введенного в предыдущем Определении элементарного преобразования типа I обратным будет прибавление к i-й строке j-й, умноженной на $-\lambda$; элементарное преобразование типа II обратно самому себе; обратное к элементарному преобразованию типа III есть умножение i-й строки на c^{-1} (которое существует, поскольку $c \neq 0$).

Элементарные преобразования строк можно выполнять последовательно, получая из исходной матрицы A новые матрицы. Назовем две матрицы A и A' размера $m \times n$ *строчно эквивалентными*, если существует конечная последовательность элементарных преобразований строк, переводящая первую матрицу во вторую. Читателю предлагается провести несложную проверку того, что это — действительно отношение эквивалентности на $\mathrm{Mat}_{m\times n}(\mathbb{K})$. Оно встретится нам также при изучении систем линейных уравнений.

Естественно спросить, как можно описать множество классов строчной эквивалентности матриц данного размера? Какие свойства матриц сохраняются при элементарных преобразованиях? Каков критерий того, что две матрицы данного размера строчно эквивалентны? В общем случае ответы на эти вопросы выходят за рамки нашего курса, но вскоре мы, например, сможем многое сказать о классе эквивалентности единичной матрицы.

Определение 2.23. Квадратная матрица называется *невырожденной*, если ее строки линейно независимы. В противном случае матрица называется *вырожденной*.

Например, легко проверить, что единичная матрица невырождена, а нулевая квадратная матрица или матрица порядка $n \geq 2$ с одинаковыми строками — вырождены.

Еще пример: матрица $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ вырождена, поскольку между ее строками $\mathbf{a_1}$, $\mathbf{a_2}$, $\mathbf{a_3}$ есть линейная зависимость $\mathbf{a_1} - \mathbf{2a_2} + \mathbf{a_3} = \mathbf{0}$.

Задача 2.24. *Докажите, что квадратная матрица A вырождена тогда и только тогда, когда существует такая строка $\mathbf{c} \neq \mathbf{0}$, что $\mathbf{c}A = \mathbf{0}$ (ноль справа обозначает нулевую строку). (Указание: воспользуйтесь Предложением 2.7).*

Предложение 2.25. *Если две матрицы строчно эквивалентны, то либо обе они вырождены, либо обе невырождены.*

Доказательство. Для каждого типа элементарных преобразований проверим, что если две матрицы связаны одним элементарным преобразованием, то либо обе они вырождены,

либо обе невырождены. Для элементарных преобразований типа II это очевидно (условие линейной независимости системы векторов не зависит от порядка векторов в системе).

Рассмотрим элементарное преобразование типа III строк матрицы A, заключающееся в умножении i-й строки на $\alpha \neq 0$. То есть если $\mathbf{a}_1, \ldots, \mathbf{a}_m$ — строки матрицы A, то строки преобразованной матрицы A' удовлетворяют условиям $\mathbf{a}'_i = \alpha\mathbf{a}_i$, $\mathbf{a}'_k = \mathbf{a}_k$ при $k \neq i$. Пусть $\mathbf{c}$ — произвольная строка длины m, тогда имеем цепочку эквивалентностей:

$$\mathbf{c}A' = \mathbf{0} \;\Leftrightarrow\; c_1\mathbf{a}_1 + \ldots + c_i\alpha\mathbf{a}_i + \ldots + c_m\mathbf{a}_m = \mathbf{0} \;\Leftrightarrow\; \mathbf{c}'A = \mathbf{0},$$

где строка $\mathbf{c}'$ получена из $\mathbf{c}$ умножением i-го элемента на α. Заметим, что $\mathbf{c} \neq \mathbf{0} \Leftrightarrow \mathbf{c}' \neq \mathbf{0}$ (так как $\alpha \neq 0$). В силу предыдущей задачи это доказывает, что элементарные преобразования типа III сохраняют условие вырожденности (невырожденности) матрицы.

Наконец, рассмотрим случай преобразований типа I. Пусть $\mathbf{a}_1, \ldots, \mathbf{a}_m$ — строки матрицы A, и матрица A' получена из A прибавлением к i-й строке умноженной на λ j-й строки, то есть $\mathbf{a}'_k = \mathbf{a}_k$ при $k \neq i$ и $\mathbf{a}'_i = \mathbf{a}_i + \lambda\mathbf{a}_j$. Тогда мы имеем цепочку эквивалентностей[17]:

$$\mathbf{c}A' = \mathbf{0} \;\Leftrightarrow\; c_1\mathbf{a}_1 + \ldots + c_i\mathbf{a}'_i + \ldots + c_m\mathbf{a}_m = \mathbf{0} \;\Leftrightarrow$$

$$\Leftrightarrow\; c_1\mathbf{a}_1 + \ldots + c_i\mathbf{a}_i + \ldots + (c_j + \lambda c_i)\mathbf{a}_j + \ldots + c_m\mathbf{a}_m = \mathbf{0} \;\Leftrightarrow\; \mathbf{c}'A = \mathbf{0},$$

где $\mathbf{c}'$ получена из $\mathbf{c}$ прибавлением к j-му элементу умноженного на λ i-го элемента[18]. Причем заметим, что $\mathbf{c} \neq \mathbf{0} \Leftrightarrow \mathbf{c}' \neq \mathbf{0}$. Таким образом, в силу предыдущей задачи элементарные преобразования типа I также сохраняют условие вырожденности (невырожденности) матриц.

В итоге мы убедились, что каждый из трех типов элементарных преобразований по отдельности обладает требуемым свойством, а значит оно выполнено и для их произвольной конечной композиции. ■

Вскоре мы докажем, что все невырожденные матрицы данного порядка образуют один класс строчной эквивалентности.

Определение 2.26. *Ведущим элементом* некоторой ненулевой строки матрицы A называется первый слева среди ее ненулевых элементов. То есть a_{ij} — ведущий элемент i-й строки матрицы A, если $a_{i1} = a_{i2} = \ldots = a_{ij-1} = 0$, но $a_{ij} \neq 0$.

Определение 2.27. Говорят, что матрица A размера $m \times n$ является *ступенчатой* (или что она "имеет *ступенчатый вид*"), если в каждой следующей ее строке сверху вниз как минимум на один нуль слева больше, чем в предыдущей. Иначе говоря, если a_{1j_1}, a_{2j_2}, …, a_{rj_r} $(r \leq m)$ — последовательность из ведущих элементов ее ненулевых строк, то последовательность j_1, j_2, …, j_r номеров их столбцов строго возрастает.

[17] ниже мы предполагаем $j > i$, аналогично рассматривается второй случай.

[18] Заметим, что это некоторое элементарное преобразование столбцов. Общий случай станет ясен после прочтения раздела 2.5.

Ступенчатая квадратная матрица называется *строго верхнетреугольной*, если на главной диагонали стоят ненулевые элементы. Другими словами, если $m = n$ и $a_{11}, a_{22}, \ldots, a_{mm}$ — ее ведущие элементы.

Нетрудно видеть, что (квадратная) ступенчатая матрица невырождена тогда и только тогда, когда она строго верхнетреугольная.

Предложение 2.28. *Любой класс строчной эквивалентности матриц содержит ступенчатую матрицу.*

Доказательство. Нам нужно доказать, что для любой матрицы A существует последовательность элементарных преобразований ее строк, приводящая ее к ступенчатому виду. Мы предъявим алгоритм построения такой последовательности.

Если матрица A нулевая, то она уже имеет ступенчатый вид. Пусть это не так, и пусть j_1 — номер ее первого слева ненулевого столбца. Если $a_{1j_1} \neq 0$, то, вычитая из строк, начиная со второй, нужную кратность первой строки, мы обнуляем все элементы j_1-го столбца, кроме первого. Если $a_{1j_1} = 0$, но $a_{ij_1} \neq 0$ (ненулевой элемент в j_1-м столбце существует по условию), мы меняем местами 1-ю и i-ю строки и приходим к описанной ситуации. Тем самым мы получаем матрицу, у которой ненулевые элементы второй и последующих строк стоят в столбцах с номерами, бóльшими j_1.

Далее мы применяем описанную процедуру к подматрице, образованной строками, начиная со второй, и т.д. В итоге получаем ступенчатую матрицу. ■

В частности, любая невырожденная матрица строчно эквивалентна строго верхнетреугольной.

Алгоритм приведения матрицы к ступенчатому виду, описанный в предыдущем Предложении, называется *методом Гаусса*.

Чтобы описать дальнейшую процедуру "упрощения" матрицы, введем еще одно понятие.

Определение 2.29. *Главным столбцом* ступенчатой матрицы A называется любой столбец, в котором стоит ведущий элемент некоторой строки A.

Определение 2.30. Ступенчатая матрица называется *упрощенной*, если после отбрасывания ее нулевых строк (которые, если они есть, стоят на последних местах) главные столбцы составляют единичную подматрицу некоторого порядка $r \leq m$.

Предложение 2.31. *Любая матрица строчно эквивалентна упрощенной.*

Доказательство. К полученной на предыдущем шаге ступенчатой матрице применим процедуру, называемую *обратным ходом* метода Гаусса. Пусть $j_1 < j_2 < \ldots < j_r$ — номера всех ее главных столбцов (тогда строки с номерами, бóльшими r, равны нулю). Тогда $a_{rj_r} \neq 0$, и вычитая нужную кратность r-й строки из предыдущих, можно обнулить все

элементы j_r-го столбца кроме a_{rj_r}. Это не испортит ступенчатого вида матрицы, поскольку $a_{ij_r} = 0$ при $i < r$. Далее повторяем указанную процедуру с главным столбцом с номером j_{r-1} и т.д. В конце концов мы получим матрицу, у которой (после отбрасывания нулевых строк) главные столбцы образуют диагональную подматрицу с ненулевыми элементами на главной диагонали. Деление строк на эти элементы (т. е. применение элементарных преобразований типа III) завершает доказательство. ■

Замечание 2.32. Можно доказать, что каждый класс строчной эквивалентности матриц содержит единственную упрощенную матрицу.

Пример 2.33. Приведем, например, к упрощенному виду матрицу $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. Имеем

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

(первая стрелка отвечает композиции двух элементарных преобразований типа I: вычитанию из второй строки первой, умноженной на 4 и вычитанию из третьей строки первой, умноженной на 7; вторая стрелка отвечает умножению второй строки на $-1/3$, третьей на $-1/6$ и последующему вычитанию из третьей строки второй; третья стрелка — вычитанию из первой строки второй, умноженной на 2).

Пример 2.34. Рассмотрим еще один пример приведения матрицы к упрощенному виду. Пусть дана матрица

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 3 & 2 & -1 \\ 2 & 1 & -1 & 3 \\ 2 & 0 & -2 & 3 \end{pmatrix},$$

приведем ее сначала к ступенчатому виду по нашему алгоритму. Для этого из 2-й, 3-й и 4-й строк вычитаем 1-ю строку, умноженную на 1, 2 и 2 соответственно. В результате получаем матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & -3 & -3 & 3 \\ 0 & -4 & -4 & 3 \end{pmatrix}.$$

Далее, прибавляя к 3-й и 4-й строкам 2-ю строку, умноженную на 3 и 4 соответственно, получаем матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Наконец, переставляя 3-ю и 4-ю строки, получаем ступенчатую матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Приведем ее теперь к упрощенному виду, используя обратный ход метода Гаусса. Вычитая из 2-й строки 3-ю, получаем

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Наконец, вычитая из 1-й строки удвоенную 2-ю и умножая 3-ю строку на -1, получим упрощенную матрицу

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

У нее главные столбцы имеют номера 1, 2 и 4.

Выше уже было замечено, что ступенчатая матрица невырождена тогда и только тогда, когда она является строго верхнетреугольной. У строго верхнетреугольной матрицы все столбцы являются главными. Поэтому применение к ней обратного хода метода Гаусса дает единичную матрицу. Тогда с учетом предыдущего Предложения получаем половину следующего важного утверждения.

Предложение 2.35. *Матрица невырождена $\Leftrightarrow$ она строчно эквивалентна единичной.*

Доказательство. Как уже говорилось, импликация "$\Rightarrow$" следует из Предложения 2.31.

Обратная импликация вытекает из того, что единичная матрица, очевидно, невырождена. ■

2.4 Системы линейных уравнений I

В данном параграфе мы начнем знакомство с системами линейных уравнений; более серьезная их теория будет изложена в следующих параграфах.

Линейным уравнением от n неизвестных $x_1, \ldots, x_n$ называется уравнение вида

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

где $a_1, \ldots, a_n, b$ — заданные элементы поля $\mathbb{K}$. Линейное уравнение называется *однородным*, если $b = 0$.

Системой m линейных уравнений от n неизвестных $x_1, \ldots, x_n$ (коротко СЛУ) называется система вида

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{cases} \tag{9}$$

Система линейных уравнений (9) называется *однородной* (коротко СЛОУ), если $b_1 = b_2 = \ldots = b_m = 0$.

Решением СЛУ (9) называется любой упорядоченный набор $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n$, такой что при подстановке α_i вместо x_i, $i = 1, \ldots, n$ каждое уравнение системы превращается в верное равенство.

Решить систему — значит найти множество всех ее решений. Это — некоторое подмножество $\mathbb{K}^n$.

Системы делятся на *совместные* (множества решений которых непусты) и *несовместные*. Однородная система всегда совместна, поскольку всегда имеет *тривиальное решение* $(0, 0, \ldots, 0)$.

Две СЛУ называются *эквивалентными*, если их множества решений совпадают, то есть каждое решение первой системы является решением второй, и наоборот. В частности, если две системы эквивалентны, то число неизвестных у них одинаковое, в то же время количество уравнений в них может быть разным.

Матрицей коэффициентов системы (9) называется матрица

$$A := \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix},$$

а расширенной матрицей системы (9) — матрица

$$\tilde{A} := \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}.$$

Столбец $\mathbf{b} := (b_1, \ldots, b_m)^T$ называется *столбцом правых частей* системы (9). С использованием матричного умножения систему (9) можно записать в виде $A\mathbf{x} = \mathbf{b}$, где $\mathbf{x} := (x_1, \ldots, x_n)^T$ — столбец неизвестных (ср. (2.2)).

Заметим, что и наоборот, по расширенной матрице однозначно восстанавливается СЛУ.

Элементарные преобразования строк расширенной матрицы отвечают соответствующим преобразованиям СЛУ: прибавлению к некоторому уравнению системы некоторого другого ее уравнения, умноженного на число, перестановке двух уравнений местами или умножению некоторого уравнения системы (его правой и левой частей) на ненулевое число.

Предложение 2.36. *Элементарные преобразования строк расширенной матрицы не меняют класса эквивалентности СЛУ.*

Доказательство. Ясно, что каждое решение исходной системы будет решением и системы, полученной после элементарного преобразования. Так как элементарные преобразования обратимы, то верно и обратное. ■

Замечание 2.37. Внимательный читатель мог заметить, что на множестве систем из m уравнений от n неизвестных фактически определены два отношения эквивалентности: во-первых, системы эквивалентны, если имеют одинаковые множества решений, и во-вторых, системы эквивалентны, если могут быть получены одна из другой последовательностью элементарных преобразований. Можно показать, что на множестве *совместных* систем эти два отношения эквивалентности совпадают, то есть для двух совместных систем с одним и тем же множеством решений существует последовательность элементарных преобразований, преобразующая первую систему во вторую. Случай однородных систем будет рассмотрен в Задаче 6.45.

Теперь заметим, что произвольное решение $(\alpha_1, \ldots, \alpha_n)$ системы (9) — то же самое, что представление столбца правых частей $\mathbf{b}$ в виде линейной комбинации столбцов матрицы A с коэффициентами $\alpha_1, \ldots, \alpha_n$. В частности, решение однородной системы с матрицей коэффициентов A — то же, что некоторая конкретная линейная зависимость между столбцами матрицы A. Поэтому предыдущее Предложение может быть переформулировано в виде такого важного Следствия.

Следствие 2.38. *Строчно эквивалентные матрицы имеют одинаковые линейные зависимости между столбцами.*

Доказательство. Интерпретируем нашу матрицу A как матрицу коэффициентов СЛОУ. Линейная зависимость $(\alpha_1, \ldots, \alpha_n)$ между столбцами A — то же, что решение этой СЛОУ. При элементарном преобразовании СЛОУ перейдет в систему с тем же множеством решений, то есть данное решение $(\alpha_1, \ldots, \alpha_n)$ будет также решением преобразованной СЛОУ и определит линейную зависимость между столбцами преобразованной матрицы, которая является ее матрицей коэффициентов. То, что при этом не возникает новых линейных зависимостей, следует из обратимости элементарных преобразований. ■

Например, столбцы исходной и полученной упрощенной матриц из примера 2.33 связаны линейной зависимостью $\mathbf{a_1} - \mathbf{2a_2} + \mathbf{a_3} = \mathbf{0}$.

Следствие 2.39. *Квадратная матрица невырождена тогда и только тогда, когда ее столбцы линейно независимы.*

Доказательство. $\Rightarrow$: невырожденная матрица эквивалентна единичной, а у последней столбцы, очевидно, линейно независимы.

$\Leftarrow$: пусть столбцы A л.н.з., то есть строки A^T л.н.з., это означает, что A^T невырождена; по уже доказанному тогда столбцы A^T л.н.з., то есть строки A л.н.з., то есть A невырождена. ■

Следствие 2.40. *Матрица A невырождена $\Leftrightarrow$ A^T невырождена.*

2.5 Элементарные матрицы

Элементарные преобразования строк из Определения 2.22 естественно рассматривать одновременно для всех матриц с m строками (и произвольным конечным числом столбцов). Размер таких матриц мы будем обозначать $m \times *$. Матрицу, полученную из матрицы A применением некоторого элементарного преобразования строк ς, мы будем обозначать $\varsigma(A)$.

Следующее Предложение показывает, что действие элементарного преобразования строк сводится к умножению слева на некоторую квадратную матрицу.

Предложение 2.41. *Для произвольного элементарного преобразования ς матриц с m строками существует единственная $m \times m$-матрица S такая, что $\varsigma(A) = SA \ \forall A \in \mathrm{Mat}_{m\times *}(\mathbb{K})$ (в частности, S не зависит от A, а зависит только от ς).*

Доказательство. Докажем вначале единственность. Так как в качестве A можно взять произвольную матрицу с m строками, то возьмем в качестве A единичную матрицу E порядка m. Тогда $\varsigma(E) = SE = S$. То есть условию доказываемого Предложения может удовлетворять только матрица, полученная применением данного элементарного преобразования ς к строкам единичной матрицы E порядка m. Для элементарных преобразований из Определения 2.22 это дает матрицы

$$P_{ij}(\lambda) = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \dots & 1 & \dots & \lambda & \dots \\ & \vdots & \ddots & \vdots & \\ \dots & 0 & \dots & 1 & \dots \\ & \vdots & & \vdots & \ddots \end{pmatrix} = E + \lambda E_{ij}, \qquad Q_{ij} = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \dots & 0 & \dots & 1 & \dots \\ & \vdots & \ddots & \vdots & \\ \dots & 1 & \dots & 0 & \dots \\ & \vdots & & \vdots & \ddots \end{pmatrix} \tag{10}$$

и

$$R_i(c) = \begin{pmatrix} \ddots & \vdots & \\ \dots & c & \dots \\ & \vdots & \ddots \end{pmatrix}$$

(у первых двух матриц выделены i-я и j-я строки, у третьей — i-я строка; при этом подразумевается, что в местах главной диагонали, отмеченных многоточием, стоят единицы).

Теперь проверим, что умножение произвольной матрицы A слева на $P_{ij}(\lambda)$, Q_{ij} или $R_i(c)$ эквивалентно применению к строкам матрицы A соответствующего элементарного преобразования. Сделаем это для случая матриц $P_{ij}(\lambda)$, для двух других типов элементарных матриц доказательство аналогично. Итак, рассмотрим $P_{ij}(\lambda)A$. Согласно Предложению 2.7, k-я строка матрицы $P_{ij}(\lambda)A$ — линейная комбинация строк матрицы A с коэффициентами из k-й строки матрицы $P_{ij}(\lambda)$. При $k \neq i$ k-я строка матрицы $P_{ij}(\lambda)$ содержит единственный ненулевой элемент — единицу на k-м месте, поэтому k-я строка матрицы $P_{ij}(\lambda)A$ совпадает с k-й строкой A. При $k = i$ i-я строка $P_{ij}(\lambda)$ помимо единицы на i-м месте содержит также λ на j-м, поэтому i-я строка матрицы $P_{ij}(\lambda)A$ совпадает с суммой i-й и умноженной на λ j-й строк матрицы A. ∎

Замечание 2.42. Более концептуальное доказательство второй части предыдущего Предложения можно получить, заметив, что для любого элементарного преобразования строк ς

$$\varsigma(AB) = \varsigma(A)B \tag{11}$$

для любой матрицы B, для которой произведение имеет смысл. Тогда из (11) получаем, что $\varsigma(B) = \varsigma(EB) = \varsigma(E)B$ для любой матрицы B с m строками, где E — единичная матрица порядка m.

Для доказательства (11) можно воспользоваться Предложением 2.7, согласно которому i-я строка матрицы AB — линейная комбинация строк матрицы B с коэффициентами из i-й строки $(a_{i1}\, a_{i2}\, \dots\, a_{im})$ матрицы A. Пусть, например, ς — прибавление к i-й строке j-й строки, умноженной на λ. Согласно упомянутому Предложению, i-я строка $\varsigma(A)B$ есть линейная комбинация строк матрицы B с коэффициентами из i-й строки матрицы $\varsigma(A)$, то есть из $(a_{i1} + \lambda a_{j1},\, a_{i2} + \lambda a_{j2},\, \dots,\, a_{im} + \lambda a_{jm})$. В то же время i-я строка матрицы $\varsigma(AB)$ есть сумма i-й строки матрицы AB плюс λ умножить на j-ю строку той же матрицы, что, как легко видеть, совпадает с i-й строкой матрицы $\varsigma(A)B$. При этом остальные строки матриц $\varsigma(A)B$ и $\varsigma(AB)$ такие же как у матрицы AB. Для элементарных преобразований двух других типов равенство (11) проверяется аналогично.

Матрицы, отвечающие элементарным преобразованиям, также называются *элементарными*. Поскольку они получаются из единичной матрицы применением элементарного преобразования строк, они невырождены.

Читателю предлагается показать, что элементарные преобразования столбцов аналогично связаны с умножением на элементарные матрицы справа.

Следующее Предложение практически очевидно.

Предложение 2.43. *Композиции элементарных преобразований ς_1, ς_2 отвечает произведение элементарных матриц S_1, S_2, то есть $\varsigma_2(\varsigma_1(A)) = S_2(S_1A) = (S_2S_1)A \quad \forall\, A \in \mathrm{Mat}_{m\times *}(\mathbb{K})$.*

Заметим, что композиция элементарных преобразований (произведение элементарных матриц), вообще говоря, не является элементарным преобразованием (соответственно, элементарной матрицей).

Следствие 2.44. *Матрицы $P_{ij}(-\lambda)$, Q_{ij}, $R_i(c^{-1})$ обратны соответственно к матрицам $P_{ij}(\lambda)$, Q_{ij} и $R_i(c)$. В частности, матрица, обратная элементарной, сама элементарна.*

Доказательство. Заметим, что указанные пары матриц отвечают взаимно обратным элементарным преобразованиям. То есть таким ς_1, ς_2, что $\varsigma_2(\varsigma_1(A)) = A$, $\varsigma_1(\varsigma_2(A)) = A \ \ \forall\, A \in \mathrm{Mat}_{m\times *}(\mathbb{K})$. В частности, $\varsigma_2(\varsigma_1(E)) = S_2S_1 = E$, $\varsigma_1(\varsigma_2(E)) = S_1S_2 = E$. ∎

Следствие 2.45. *Матрица невырождена ⇔ она является произведением элементарных.*

Доказательство. Из Предложения 2.35 мы знаем, что если матрица A невырождена, то она строчно эквивалентна единичной матрице. Другими словами, существует конечная последовательность элементарных преобразований строк, преобразующая единичную матрицу в A. То есть существует конечная последовательность элементарных матриц $S_1, \ldots, S_p$ такая, что $A = S_p \ldots S_1 E = S_p \ldots S_1$.

Обратно, произведение элементарных матриц получается из единичной матрицы композицией элементарных преобразований строк и поэтому строчно эквивалентно единичной матрице, которая невырождена. ∎

Конечно, представление невырожденной матрицы в виде произведения элементарных неоднозначно.

Задача 2.46. *Разложите матрицу* $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ *в произведение элементарных.*

Ответ: например,

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Следующее Предложение непостредственно вытекает из предыдущего Следствия.

Предложение 2.47. *Произведение невырожденных матриц невырождено.*

Задача 2.48. *Пусть S_n — множество всех $n!$ перестановок*[19] *на n элементах. Каждой перестановке $\sigma \in S_n$ сопоставим матрицу A_σ порядка n, полученную из единичной матрицы перестановкой строк σ. Покажите что A_σ является произведением элементарных матриц Q_{ij} типа 2, а также что $A_\tau A_\sigma = A_{\tau\circ\sigma}$, $A_\sigma^{-1} = A_{\sigma^{-1}}$, где $\tau \circ \sigma$ — композиция перестановок, а σ^{-1} — обратная к σ перестановка.*

2.6 Связь невырожденности с обратимостью

Теорема 2.49. *Матрица обратима ⇔ она невырождена.*

Доказательство. Если матрица A невырождена, то существует последовательность элементарных преобразований строк $\tau_1, \ldots, \tau_p$, преобразующая ее в единичную матрицу.

[19] см. Определение 3.7 и далее.

Пусть $T_1, \ldots, T_p$ — соответствующая последовательность элементарных матриц. Тогда $E = T_p \ldots T_1 A$. Положим $B := T_p \ldots T_1$. Тогда $E = BA$.

Матрица B, будучи произведением элементарных матриц, невырождена, поэтому к ней применимы те же соображения, то есть существует матрица C, являющаяся произведением некоторых элементарных матриц, такая, что $E = CB$. Имеем $A = (CB)A = C(BA) = C$, то есть B является обратной для A. (По-другому, в этом месте можно рассуждать так: для невырожденной матрицы A существует последовательность элементарных преобразований столбцов, преобразующая ее в единичную матрицу, что дает матрицу D такую, что $AD = E$. Дальше снова используем ассоциативность произведения BAD чтобы доказать равенство $B = D$).

Обратно, пусть квадратная матрица A вырождена. Тогда ее столбцы линейно зависимы, то есть существует ненулевой столбец $\mathbf{c}$ такой, что $A\mathbf{c} = \mathbf{0}$. Предположим, что обратная матрица A^{-1} существует, тогда, умножая обе части последнего равенства на нее, получаем $\mathbf{c} = A^{-1}\mathbf{0} = \mathbf{0}$ — противоречие. ∎

Замечание 2.50. Удобный критерий обратимости (=невырожденности) матрицы мы получим ниже в терминах определителя.

Задача 2.51. *Пусть A и B — две матрицы порядка m такие, что $AB = E$. Докажите, что тогда и $BA = E$ (то есть обе матрицы A и B обратимы и $B = A^{-1}$ (а значит и $A = B^{-1}$)).*

Решение. Если A — вырождена, то существует ненулевая строка $\mathbf{c}$ такая, что $\mathbf{c}A = \mathbf{0}$. Следовательно, $\mathbf{0} = (\mathbf{c}A)B = \mathbf{c}(AB) = \mathbf{c}E = \mathbf{c}$ — противоречие, значит, A невырождена. Тогда существует последовательность элементарных матриц $S_1, \ldots, S_k$ такая, что $S_k \ldots S_1 A = E$. Пусть $C := S_k \ldots S_1$, тогда $CA = E$. Откуда $B = EB = (CA)B = C(AB) = CE = C$, поэтому в самом деле $BA = E$. ∎

Замечание 2.52. На множестве $\mathrm{Mat}_{m\times n}(\mathbb{K})$ рассмотрим следующее отношение эквивалентности: $B \sim C \Leftrightarrow \exists$ невырожденная $m \times m$-матрица A такая, что $C = AB$. Легко видеть, что это отношение эквивалентности совпадает с отношением строчной эквивалентности на $\mathrm{Mat}_{m\times n}(\mathbb{K})$. Отношение, связанное с умножением на невырожденные матрицы справа, совпадает с отношением столбцовой эквивалентности, которое определяется с помощью элементарных преобразований столбцов.

Пусть матрица A невырождена и $\tau_1, \ldots, \tau_p$ — последовательность элементарных преобразований строк, преобразующая ее в единичную матрицу; пусть $T_1, \ldots, T_p$ — соответствующий набор элементарных матриц. Тогда $E = T_p \ldots T_1 A$ и $T_p \ldots T_1 = A^{-1}$. Отсюда $T_p \ldots T_1(A \mid E) = (E \mid A^{-1})$. То есть если к строкам матрицы $(A \mid E)$ применить последовательность элементарных преобразований, преобразующую A в единичную матрицу, то справа будет стоять обратная к A матрица (поскольку применение той же последовательности элементарных преобразований к строкам единичной матрицы E дает матрицу, обратную к A). Это дает удобный на практике способ нахождения обратной матрицы.

Теорема 2.53. *Невырожденные матрицы данного порядка m образуют группу по умножению.*

Доказательство. Действительно, умножение — бинарная ассоциативная операция на множестве $\mathrm{Mat}_m(\mathbb{K})$, причем произведение невырожденных матриц невырождено, единичная матрица невырождена и для любой невырожденной матрицы существует обратная, которая тоже невырождена. ■

Эта группа обозначается $\mathrm{GL}_m(\mathbb{K})$ и называется *полной линейной группой* порядка m. При $m = 1$ она совпадает с *мультипликативной группой* поля $\mathbb{K}$ (то есть с группой его ненулевых элементов относительно операции умножения); при $m \geq 2$ она некоммутативна.

2.7 Системы линейных уравнений II

Теперь мы собираемся применить результаты раздела 2.3 к теории систем линейных уравнений. Мы получим условия, при которых система несовместна, совместна и имеет единственное решение, и имеет более одного решения.

Определение 2.54. Совместная система уравнений называется *определенной* (соотв. *неопределенной*), если она имеет единственное решение (соотв. более одного решения).

Определение 2.55. Система линейных уравнений называется *ступенчатой*, если ее расширенная матрица $\tilde{A}$ ступенчатая. Система линейных уравнений называется *треугольной* (соотв. *строго треугольной*), если ее матрица коэффициентов является треугольной (соотв. строго треугольной).

Заметим, что у треугольной системы число уравнений равно числу неизвестных.

Так как элементарные преобразования системы заменяют ее на эквивалентную, из Предложения 2.28 следует, что достаточно исследовать (и научиться решать) ступенчатые системы.

Итак, рассмотрим произвольную ступенчатую СЛУ; пусть A (соотв. $\tilde{A}$) — ее матрица коэффициентов (соотв. расширенная матрица). Через r (соотв. $\tilde{r}$) обозначим число ненулевых строк матрицы A (соотв. $\tilde{A}$).

Ясно, что возможно два случая: (I) $\tilde{r} = r$ или (II) $\tilde{r} = r + 1$.

В случае (II) система содержит уравнение вида $0x_1 + \ldots + 0x_n = b,\ b \neq 0$ и поэтому является несовместной.

Рассмотрим теперь случай (I). Из того, что матрица A по предположению является ступенчатой следует, что число ее ступенек r не превосходит числа ее столбцов n, то есть числа неизвестных $x_1, \ldots, x_n$ системы. Выделим в качестве подслучая (I) случай (Ia), когда $\tilde{r} = r = n$, то есть система является строго треугольной. Легко понять, что в этом случае система имеет единственное решение. Действительно, из последнего уравнения находим единственное x_n, тогда из предпоследнего — единственное x_{n-1} и т.д.

Осталось рассмотреть случай (Ib), когда $\tilde{r} = r < n$. При анализе этого случая нам пригодится дополнительная терминология.

Определение 2.56. Неизвестные $x_{j_1}, x_{j_2}, \ldots, x_{j_r}$ $1 \leq j_1 < j_2 < \ldots < j_r \leq n$, отвечающие главным столбцам матрицы A, называются главными, а остальные — свободными.

Другими словами, главные неизвестные — в точности те, которые отвечают ведущим элементам какой-либо строки. Их в точности r штук (соответственно свободных $n - r$).

Перенося все члены со свободными неизвестными в правую часть, мы получаем строго треугольную систему относительно главных неизвестных. Если мы присвоим всем свободным неизвестным какие-то значения, то значения главных неизвестных определяются из этой системы однозначно. Так как свободные неизвестные могут пробегать произвольные наборы из $\mathbb{K}^{n-r}$, то в случае бесконечного поля $\mathbb{K}$ система при $n > r$ имеет бесконечно много решений.

Еще очевидней становится анализ случая (I), если воспользоваться Предложением 2.31 о том, что любая матрица строчно эквивалентна упрощенной. Тогда, предполагая что матрица коэффициентов системы упрощенная и перенося все члены со свободными неизвестными в правую часть, мы получаем систему, разрешенную относительно главных неизвестных (это рассуждение включает в себя также случай (Ia), когда все переменные являются главными а свободные неизвестные отсутствуют). Например, если номера главных неизвестных образуют последовательность $1, 2, \ldots, r$ (общий случай сводится к этому перенумерацией неизвестных), то система имеет вид

$$\begin{cases} x_1 + c_{11}x_{r+1} + c_{12}x_{r+2} + \ldots + c_{1n-r}x_n = d_1 \\ x_2 + c_{21}x_{r+1} + c_{22}x_{r+2} + \ldots + c_{2n-r}x_n = d_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r + c_{r1}x_{r+1} + c_{r2}x_{r+2} + \ldots + c_{rn-r}x_n = d_r. \end{cases} \tag{12}$$

Результат проведенного исследования сформулируем в виде теоремы.

Теорема 2.57. *СЛУ несовместна тогда и только тогда, когда для любой ступенчатой матрицы, полученной из ее расширенной матрицы с помощью элементарных преобразований строк, $\tilde{r} > r$. СЛУ определенна тогда и только тогда, когда $\tilde{r} = r = n$, где n — число неизвестных. СЛУ неопределенна тогда и только тогда, когда $\tilde{r} = r < n$.*

Напомним, что СЛОУ всегда совместна.

Следствие 2.58. *Всякая однородная система, у которой число уравнений меньше числа неизвестных, имеет нетривиальное (то есть ненулевое) решение.*

Доказательство. Рассмотрим однородную систему из m уравнений от n неизвестных. Приведем ее к ступенчатому виду. Число r ненулевых строк полученной ступенчатой системы не превосходит m, причем $m < n$ по условию. То есть $r < n$, что и влечет, в силу предыдущего обсуждения, неопределенность системы. ∎

Предыдущее Следствие можно переформулировать так: любая система из n столбцов высоты m линейно зависима при $n > m$. Мы этим воспользуемся ниже (см. Предложение 6.4).

Заодно мы получили следующий простой и общий алгоритм решения СЛУ. Запишем расширенную матрицу системы и с помощью элементарных преобразований строк приведем ее к ступенчатому виду. Если при этом получим $\tilde{r} > r$, то делаем вывод, что система несовместна. Если же $\tilde{r} = r$, то с помощью обратного хода метода Гаусса приводим ее ступенчатую расширенную матрицу к упрощенному виду и выписываем общее решение в виде выражения главных неизвестных через свободные.

В качестве примера решим систему уравнений

$$\begin{cases} x_1 + 2x_2 + x_3 = 2 \\ x_1 + 3x_2 + 2x_3 - x_4 = 4 \\ 2x_1 + x_2 - x_3 + 3x_4 = -2 \\ 2x_1 - 2x_3 + 3x_4 = 1 \end{cases}$$

над полем $\mathbb{R}$. Выписываем расширенную матрицу

$$\tilde{A} = \begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 1 & 3 & 2 & -1 & 4 \\ 2 & 1 & -1 & 3 & -2 \\ 2 & 0 & -2 & 3 & 1 \end{pmatrix}$$

и приводим ее к ступенчатому виду по нашему алгоритму. Для этого из 2-й, 3-й и 4-й строк вычитаем 1-ю строку, умноженную на 1, 2 и 2 соответственно. В результате получаем матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & -3 & -3 & 3 & -6 \\ 0 & -4 & -4 & 3 & -3 \end{pmatrix}.$$

Далее, прибавляя к 3-й и 4-й строкам 2-ю строку, умноженную на 3 и 4 соответственно, получаем матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 5 \end{pmatrix}.$$

Наконец, переставляя 3-ю и 4-ю строки, получаем ступенчатую матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & 0 & 0 & -1 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Для нее $\tilde{r} = r = 3 < n = 4$, то есть система неопределенна. Главные переменные x_1, x_2 и x_4, а x_3 — свободная переменная. Приведем теперь матрицу к упрощенному виду, используя обратный ход метода Гаусса. Отбросив нулевую строку и вычтя из 2-й строки 3-ю, получим матрицу

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & -3 \\ 0 & 0 & 0 & -1 & 5 \end{pmatrix}.$$

Вычтя из 1-й строки удвоенную 2-ю и умножив 3-ю строку на -1, получим матрицу

$$\begin{pmatrix} 1 & 0 & -1 & 0 & 8 \\ 0 & 1 & 1 & 0 & -3 \\ 0 & 0 & 0 & 1 & -5 \end{pmatrix},$$

имеющую упрощенный вид (главные столбцы составляют единичную матрицу). Таким образом, исходная система уравнений эквивалентна системе

$$\begin{cases} x_1 & & - & x_3 & & = & 8 \\ & x_2 & + & x_3 & & = & -3 \\ & & & & x_4 & = & -5. \end{cases}$$

Перенося члены со свободной неизвестной x_3 в правую часть, получаем общее решение

$$\begin{cases} x_1 & = & x_3 & + & 8 \\ x_2 & = & -x_3 & - & 3 \\ x_4 & = & & & -5. \end{cases}$$

Чтобы подчеркнуть, что свободная переменная x_3 играет роль параметра, ее можно обозначить через t и переписать полученное решение в виде

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} t+8 \\ -t-3 \\ t \\ -5 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} t + \begin{pmatrix} 8 \\ -3 \\ 0 \\ -5 \end{pmatrix}.$$

Это — параметрическое уравнение прямой в четырехмерном пространстве $\mathbb{K}^4$ с направляющим вектором $(1, -1, 1, 0)^T$ и проходящей через точку $(8, -3, 0, -5)$.

Заметим, что на некоторые естественные вопросы о системах уравнений (и о матрицах) мы пока не дали ответы. Например, зависит ли количество свободных неизвестных СЛУ от выбора последовательности элементарных преобразований, с помощью которых мы приводили матрицу системы к ступенчатому виду? Этот вопрос, очевидно, эквивалентен вопросу о том, могут ли две ступенчатые матрицы с разным числом r ненулевых строк принадлежать одному классу строчной эквивалентности матриц? На эти вопросы мы ответим немного позже, после изучения понятий размерности векторного пространства и ранга матрицы.

3 Определители

Данная глава организована следующим образом. В первом параграфе мы приходим к понятию определителя, опираясь на понятия ориентированных площади и объема из курса аналитической геометрии. Он написан чтобы облегчить читателю переход на более абстрактный язык, который используется во втором параграфе. В частности, Теоремы 3.2, 3.4 и 3.10 являются специальными случаями Теоремы 3.23, что должно помочь читателю лучше осознать этот важный результат.

3.1 n-мерный ориентированный объем

Все пространства в данном параграфе рассматриваются над полем $\mathbb{R}$.

Читатель, вероятно, в курсе аналитической геометрии встречался с понятиями ориентированной длины на ориентированной прямой, ориентированной площади на ориентированной плоскости и ориентированного объема в ориентированном трехмерном пространстве. У этих понятий есть естественное обобщение на случай n-мерного ориентированного пространства, называемое *n-мерным ориентированным объемом*. В этом параграфе мы опишем, как можно к нему прийти, но вначале напомним определения ориентированных площадей и объемов. Данный параграф также можно рассматривать как неформальное "геометрическое" введение в теорию определителей.

Напомним, что в вещественном векторном пространстве базисы делятся на два класса: между базисами из одного класса матрицы перехода имеют положительный определитель, а между базисами из разных классов — отрицательный определитель. Ориентированной плоскостью (пространством) называется плоскость (пространство), в котором выбран один из двух классов базисов, базисы из него называются "положительными". В качестве положительных базисов обычно выбираются правые базисы (определяемые в курсе аналитической геометрии), что мы также сделаем.

Определение 3.1. *Ориентированной площадью* на ориентированной плоскости V называется функция $f\colon V \times V \to \mathbb{R}$, обладающая следующими свойствами:

1) функция f линейна по каждому из своих двух аргументов (то есть *билинейна*);

2) функция f меняет знак при перестановке аргументов (то есть *кососимметрична*);

3) если $\{e_1, e_2\}$ — правый ортонормированный базис, то $f(e_1, e_2) = 1$.

Значение $f(u, v)$ на упорядоченной паре $\{u, v\}$ векторов плоскости V — ориентированная площадь параллелограмма, построенного на данной паре векторов (иногда называемая *псевдоскалярным произведением* векторов u и v). Заметим, что из кососимметричности f сразу следует, что $f(u, u) = 0$ для произвольного $u \in V$. Более общо, из билинейности и кососимметричности f следует, что $f(u, v) = 0$, если u и v коллинеарны (нетрудно проверить, что верно и обратное).

Теорема 3.2. *Существует единственная функция f, удовлетворяющая Определению 3.1.*

Доказательство. Если функция f обладает свойствами 1), 2) из предыдущего определения и $\{e_1, e_2\}$ — некоторый базис на плоскости V, то для произвольной пары векторов $u, v \in V$ имеем

$$f(u,v) = f(u_1e_1+u_2e_2, v_1e_1+v_2e_2) = u_1v_2f(e_1,e_2)+u_2v_1f(e_2,e_1) = (u_1v_2-u_2v_1)f(e_1,e_2). \quad (13)$$

Таким образом, f однозначно в данном базисе определяется одним числом $f(e_1, e_2)$.

Обратно, легко проверить, что функция f, заданная формулой (13), полилинейна и кососимметрична. В самом деле (обозначая для простоты $c := f(e_1, e_2)$), линейность, например, по первому аргументу u вытекает из следующей выкладки: если $u = u' + u''$, то

$$f(u,v) = (u_1v_2 - u_2v_1)c = ((u'_1 + u''_1)v_2 - (u'_2 + u''_2)v_1)c =$$
$$= (u'_1v_2 - u'_2v_1)c + (u''_1v_2 - u''_2v_1)c = f(u',v) + f(u'',v),$$

и аналогично для умножения на скаляр. (Фактически, все следует из того, что в каждое слагаемое выражения $(u_1v_2 - u_2v_1)$ координаты u входят в первой степени). Кососимметричность также очевидна: если поменять местами u и v, то выражение $(u_1v_2 - u_2v_1)c$ изменит знак. ■

Коэффициент $u_1v_2 - u_2v_1$ перед $f(e_1, e_2)$ в формуле (13) называется *определителем матрицы* $\begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}$. Свойства 1) и 2) предыдущего определения означают, что он линеен и кососимметричен по строкам. Кроме того, на единичной матрице порядка 2 он принимает значение 1 и свойство 3) означает, что ориентированная площадь параллелограмма, построенного на паре векторов u, v равна определителю матрицы, составленной из координатных строк этих векторов в правом ортонормированном базисе.

Определение 3.3. *Ориентированным объемом* в ориентированном трехмерном пространстве V называется функция $f\colon V \times V \times V \to \mathbb{R}$, обладающая следующими свойствами:

1) функция f линейна по каждому из своих трех аргументов (то есть *трилинейна*);

2) функция f меняет знак при перестановке любых двух аргументов (то есть *кососимметрична*);

3) если $\{e_1, e_2, e_3\}$ — правый ортонормированный базис, то $f(e_1, e_2, e_3) = 1$.

Значение $f(u, v, w)$ на упорядоченной тройке $\{u, v, w\}$ векторов пространства V — ориентированный объем параллелепипеда, построенного на данной тройке векторов (то есть

смешанное произведение (u, v, w) векторов u, v, w). Заметим, что из полилинейности и кососимметричности f сразу следует, что $f(u, v, w) = 0$, если векторы u, v и w компланарны (верно и обратное).

Теорема 3.4. *Существует единственная функция f, удовлетворяющая Определению 3.3.*

Доказательство. Если функция f линейна по каждому аргументу и $\{e_1, e_2, e_3\}$ — некоторый базис в пространстве V, то для произвольной тройки векторов $\{u, v, w\}$ из V имеем

$$f(u, v, w) = f(u_1e_1 + u_2e_2 + u_3e_3, v_1e_1 + v_2e_2 + v_3e_3, w_1e_1 + w_2e_2 + w_3e_3) =$$

$$= \sum_{i,j,k=1}^{3} u_i v_j w_k f(e_i, e_j, e_k)$$

(правая часть содержит $3^3 = 27$ слагаемых). Если f к тому же кососимметрична, то $f(e_i, e_j, e_k) = 0$ всякий раз, когда среди индексов i, j, k есть совпадающие. Если же индексы i, j, k образуют перестановку чисел $1, 2, 3$, то

$$f(e_i, e_j, e_k) = \pm f(e_1, e_2, e_3),$$

причем знак "+" нужно взять в том случае, когда (i, j, k) получается из $(1, 2, 3)$ четным числом транспозиций (перестановок двух каких-то аргументов), а "−" — если нечетным. Соответствующий множитель ± 1 называется *знаком* перестановки (i, j, k) и обозначается $\operatorname{sgn}(i, j, k)$. Читателю предлагается выписать 6 перестановок (i, j, k) и указать их знаки (должно получиться по 3 положительных и отрицательных перестановки).

Таким образом,

$$f(u, v, w) = \sum u_i v_j w_k \operatorname{sgn}(i, j, k)\, f(e_1, e_2, e_3), \tag{14}$$

причем суммирование справа происходит по перестановкам множества $1, 2, 3$ (то есть правая часть содержит 6 слагаемых). Окончательная формула выглядит так (читателю предлагается в этом убедиться):

$$f(u, v, w) = (u_1v_2w_3 + u_2v_3w_1 + u_3v_1w_2 - u_1v_3w_2 - u_2v_1w_3 - u_3v_2w_1) f(e_1, e_2, e_3). \tag{15}$$

В частности, f однозначно в данном базисе определяется одним числом $f(e_1, e_2, e_3)$.

Обратно, легко проверить, что функция f, заданная формулой (14), полилинейна и кососимметрична. В самом деле, линейность следует из того, что в каждое слагаемое в правой части координаты каждого из векторов u, v и w входят в первой степени. Точнее, выражение

$$u_1(v_2w_3 - v_3w_2) + u_2(v_3w_1 - v_1w_3) + u_3(v_1w_2 - v_2w_1),$$

являющееся коэффициентом перед $f(e_1, e_2, e_3)$ в (14), линейно по строке (u_1, u_2, u_3), то же верно для двух других строк.

Проверим кососимметричность. Переставим, например, векторы u и v в выражении $f(u,v,w)$ (чтобы упростить формулы, мы полагаем в (14) $c := f(e_1,e_2,e_3)$):

$$f(v,u,w) = \sum \operatorname{sgn}(i,j,k)\, v_i u_j w_k c =$$

$$= \sum \operatorname{sgn}(i,j,k)\, u_j v_i w_k c = -\sum \operatorname{sgn}(j,i,k)\, u_j v_i w_k c = -f(u,v,w),$$

поскольку, очевидно, $\operatorname{sgn}(i,j,k) = -\operatorname{sgn}(j,i,k)$. ■

Коэффициент

$$u_1v_2w_3 + u_2v_3w_1 + u_3v_1w_2 - u_1v_3w_2 - u_2v_1w_3 - u_3v_2w_1$$

перед $f(e_1,e_2,e_3)$ в формуле (15) называется *определителем матрицы* $\begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}$. Свойства 1) и 2) Определения 3.3 означают, что он линеен и кососимметричен по строкам, а свойство 3) означает, что ориентированный объем параллелепипеда, построенного на упорядоченной тройке векторов u, v, w равен определителю матрицы, составленной из координатных строк этих векторов в правом ортонормированном базисе.[20]

Задача 3.5. *Докажите, что для любых векторов u, v, w, x, y, z трехмерного ориентированного евклидова пространства V выполнено тождество*

$$f(u,v,w)\, f(x,y,z) = \begin{vmatrix} (u,x) & (u,y) & (u,z) \\ (v,x) & (v,y) & (v,z) \\ (w,x) & (w,y) & (w,z) \end{vmatrix}. \tag{16}$$

Решение. Заметим, что слева и справа стоят полилинейные функции $V^{\times 6} \to \mathbb{R}$, кососимметричные по $1,2,3$ и $4,5$ и 6 аргументам. Из полилинейности следует, что это тождество достаточно проверить на наборах векторов, когда u, v, w, x, y, z пробегают элементы некоторого ортонормированного базиса $\{e_1, e_2, e_3\}$ в V, а из кососимметричности — что его достаточно проверить на наборе $u = x = e_1,\ v = y = e_2,\ w = z = e_3$, после чего в его справедливости легко убедиться. ■

Полагая $\{u,v,w\} = \{x,y,z\}$ в доказанном тождестве, получаем интересный результат: квадрат объема параллелепипеда, построенного на базисе, равен определителю его матрицы Грама.

Рассмотренные случаи $n = 2$ и $n = 3$ подсказывают, как n-мерный ориентированный объем определяется для произвольного конечного n. Во-первых, в вещественном n-мерном пространстве нужно задать ориентацию — то есть выбрать один из двух классов базисов, объявив базисы из него “положительными”. Мы будем пользоваться существованием двух классов базисов без доказательства.[21]

[20] Конечно, этот результат известен читателю из курса аналитической геометрии.

[21] Заметим, что и в общем n-мерном случае матрицы перехода между базисами из одного класса имеют положительный, а между разными классами — отрицательный определитель.

Определение 3.6. *Ориентированным объемом* в ориентированном n-мерном пространстве V называется функция $f\colon V \times V \times \ldots \times V \to \mathbb{R}$ (слева произведение n экземпляров пространства V), обладающая следующими свойствами:

1) функция f линейна по каждому из своих n аргументов (то есть *полилинейна*);

2) функция f меняет знак при перестановке любых двух аргументов (то есть *кососимметрична*);

3) если $\{e_1, e_2, \ldots, e_n\}$ — правый ортонормированный базис, то $f(e_1, e_2, \ldots, e_n) = 1$.

(В предыдущем определении мы предполагаем, что ортонормированные базисы в n-мерном пространстве существуют. Это действительно так и будет доказано в этом курсе).

Значение $f(v_1, v_2, \ldots, v_n)$ на упорядоченном наборе (системе) $v_1, v_2, \ldots, v_n$ векторов пространства V — ориентированный n-мерный объем параллелепипеда, построенного на данном наборе векторов. Заметим, что из полилинейности и кососимметричности f сразу следует, что $f(v_1, v_2, \ldots, v_n) = 0$ если система $v_1, v_2, \ldots, v_n$ линейно зависима (верно и обратное).

Для того, чтобы получить формулу для n-мерного ориентированного объема, нам понадобятся понятие и свойства перестановок.

Определение 3.7. *Перестановкой* из n элементов называется последовательность $(k_1, \ldots, k_n)$ чисел $1, 2, \ldots, n$, расположенных в некотором фиксированном порядке.

Так как k_1 может принимать n различных значений, k_2 при фиксированном k_1 — $(n-1)$ значение, k_3 при фиксированных k_1 и k_2 — $(n-2)$ значений и т.д., то всего имеется

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$$

перестановок из n элементов. Перестановка $(1, 2, \ldots, n)$ называется *тривиальной*.

Множество всех $n!$ перестановок из n элементов обозначается S_n. (В действительности, это множество очевидным образом отождествляется с множеством всех биекций множества $1, 2, \ldots, n$ на себя; при этом, в частности, тождественная биекция соответствует тривиальной перестановке. Последнее множество, очевидно, является группой относительно операции композиции. Мы не будем останавливаться на этом более подробно).

Перемена местами двух (не обязательно соседних) элементов в перестановке называется *транспозицией* этих элементов.

Определение 3.8. Знак перестановки — это такая функция

$$\operatorname{sgn}\colon S_n \to \{\pm 1\},$$

что $\operatorname{sgn}(1, 2, \ldots, n) = 1$ и которая меняет знак при любой транспозиции (то есть если перестановки $(k_1, \ldots, k_n)$ и $(j_1, \ldots, j_n)$ отличаются друг от друга одной транспозицией (не обязательно соседних элементов), то $\operatorname{sgn}(k_1, \ldots, k_n) = -\operatorname{sgn}(j_1, \ldots, j_n)$).

Задача 3.9. *Покажите, что если* $f\colon V \times \ldots \times V \to \mathbb{K}$ *— кососимметрическая функция, то*

$$f(v_{k_1}, \ldots, v_{k_n}) = \operatorname{sgn}(k_1, \ldots, k_n) f(v_1, \ldots, v_n).$$

Теорема 3.10. *Для любого* n *функция* $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ *существует и единственна.*

Доказательство. То, что существует не более одной такой функции, следует из того, что любую перестановку из n элементов можно получить из тривиальной $(1, 2, \ldots, n)$ последовательностью транспозиций.

Однако при таком подходе *существование* функции sgn не очевидно: одну и ту же перестановку можно получить из тривиальной разными последовательностями транспозиций; идея в том, что *чётность* числа транспозиций не зависит от выбора такой последовательности. На время отложим доказательство существования sgn и введем понятие *инверсии.*

Определение 3.11. Говорят, что пара (не обязательно соседних) чисел в перестановке $(k_1, \ldots, k_n)$ образуют *инверсию*, если большее из них стоит левее меньшего.

Например, тривиальная перестановка содержит 0 инверсий, а в перестановке $(n, n-1, n-2, \ldots, 2, 1)$ любая пара чисел образует инверсию, то есть число инверсий в ней равно биномиальному коэффициенту $\binom{n}{2}$ (числу 2-элементных подмножеств в множестве из n элементов).

Предложение 3.12. *При любой транспозиции четность числа инверсий в перестановке* $(k_1, \ldots, k_n)$ *меняется.*

Доказательство. При транспозиции соседних элементов меняется взаимное расположение только этих элементов, так что число инверсий меняется (увеличивается или уменьшается) на 1, следовательно, четность числа инверсий меняется. При транспозиции двух элементов i и j, разделенных s промежуточными элементами, можно сначала переставить i со всеми промежуточными элементами и с j, сделав $s+1$ соседних транспозиций, а затем j со всеми промежуточными элементами, произведя еще s соседних транспозиций. В итоге мы проделаем нечетное число $2s+1$ соседних транспозиций, каждая из которых меняет четность числа инверсий в перестановке. ∎

Вернемся теперь к существованию sgn. Пусть $i(\sigma)$ обозначает число инверсий в перестановке $\sigma := (k_1, k_2, \ldots, k_n)$. Покажем, что функция

$$s(\sigma) := (-1)^{i(\sigma)} \quad \forall \sigma \in S_n$$

обладает всеми свойствами sgn из предыдущего определения.

Действительно, если $\sigma = (1, 2, \ldots, n)$, то $i(\sigma) = 0$ и $s(\sigma) = (-1)^{i(\sigma)} = 1$. С другой стороны, из Предложения 3.12 следует, что при любой транспозиции элементов σ четность $i(\sigma)$ меняется, и значит $s(\sigma) = (-1)^{i(\sigma)}$ меняет знак. ∎

Замечание 3.13. Другое доказательство существования функции sgn можно получить, предъявив произвольную ненулевую кососимметрическую функцию от n аргументов, например $\Delta_n(x_1, x_2, \ldots, x_n) = \prod_{1 \le j < i \le n}(x_i - x_j)$ (определитель Вандермонда). Тогда $\Delta_n(x_{k_1}, x_{k_2}, \ldots, x_{k_n}) = \operatorname{sgn}(k_1, k_2, \ldots, k_n)\, \Delta_n(x_1, x_2, \ldots, x_n)$ (ср. Задачу 3.9).

Определение 3.14. Перестановки $\sigma \in S_n$ такие, что $\operatorname{sgn}\sigma = 1$, называются *четными*, а остальные — *нечетными* (для них $\operatorname{sgn}\sigma = -1$).

Таким образом, перестановка является четной, если число инверсий в ней четно и нечетной в противном случае. Например,

$$\operatorname{sgn}(n, n-1, n-2, \ldots, 2, 1) = (-1)^{\frac{n(n-1)}{2}}, \tag{17}$$

таким образом, данная перестановка четная при $n \equiv 0, 1 (\mathrm{mod}\, 4)$ и нечетная при $n \equiv 2, 3 (\mathrm{mod}\, 4)$.

Следствие 3.15. *При $n > 1$ количество четных перестановок из n элементов равно количеству нечетных.*

Доказательство. Выпишем в первый столбец все четные, а во второй — все нечетные перестановки из n элементов. Тогда, согласно Предложению 3.12, при транспозиции первого и второго элемента первый столбец биективно отображается на второй, и наоборот. ■

Задача 3.16. *Докажите, что четность числа транспозиций, в виде произведения (композиции) которых можно представить данную перестановку, зависит только от самой перестановки.*

Теорема 3.17. *Существует единственная функция f, удовлетворяющая Определению 3.6 ориентированного n-мерного объема.*

Набросок доказательства. Если функция f линейна по каждому из своих n аргументов и $\{e_1, e_2, \ldots, e_n\}$ — некоторый базис в пространстве V, то для произвольной системы из n векторов $\{v_1, v_2, \ldots, v_n\}$ в V имеем[22]

$$f(v_1, v_2, \ldots, v_n) = \sum_{i_1, i_2, \ldots, i_n = 1}^{n} v_{1 i_1} v_{2 i_2} \ldots v_{n i_n} f(e_{i_1}, e_{i_2}, \ldots, e_{i_n})$$

(сумма справа содержит n^n слагаемых). Если f к тому же кососимметрична, то $f(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) = 0$ всякий раз, когда среди индексов $i_1, i_2, \ldots, i_n$ есть совпадающие. Если же индексы $i_1, i_2, \ldots, i_n$ образуют перестановку чисел $1, 2, \ldots, n$, то

$$f(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) = \operatorname{sgn}(i_1, i_2, \ldots, i_n)\, f(e_1, e_2, \ldots, e_n)$$

[22]Ниже мы обозначаем набор координат вектора $v_k \in V$ в базисе $\{e_1, e_2, \ldots, e_n\}$ через $(v_{k1}, v_{k2}, \ldots, v_{kn})$, то есть первый индекс — номер вектора, второй — номер координаты.

(см. Задачу 3.9).

Таким образом,

$$f(v_1, v_2, \ldots, v_n) = \sum_{(i_1,i_2,\ldots,i_n)\in S_n} v_{1i_1} v_{2i_2} \ldots v_{ni_n} \operatorname{sgn}(i_1, i_2, \ldots, i_n)\, f(e_1, e_2, \ldots, e_n) \qquad (18)$$

(правая часть содержит $n!$ слагаемых).

В частности, полилинейная кососимметричная f однозначно в данном базисе определяется одним числом $f(e_1, e_2, \ldots, e_n)$.

С другой стороны, функция f, заданная формулой (18), полилинейна и кососимметрична. В самом деле, полилинейность следует из того, что каждое слагаемое в правой части (18) содержит ровно по одной координате каждого вектора v_k, $1 \le k \le n$ (в первой степени).

Проверим кососимметричность правой части (18) по векторам $v_1, \ldots, v_n$. Переставим, например, местами v_1 и v_2 (чтобы упростить вид формул, мы полагаем $f(e_1, e_2, \ldots, e_n) = 1$):

$$f(v_2, v_1, \ldots, v_n) = \sum_{(i_1,i_2,\ldots,i_n)\in S_n} \operatorname{sgn}(i_1, i_2, \ldots, i_n)\, v_{2i_1} v_{1i_2} \ldots v_{ni_n} =$$

$$= \sum_{(i_1,i_2,\ldots,i_n)\in S_n} \operatorname{sgn}(i_1, i_2, \ldots, i_n)\, v_{1i_2} v_{2i_1} \ldots v_{ni_n} =$$

$$= - \sum_{(i_2,i_1,\ldots,i_n)\in S_n} \operatorname{sgn}(i_2, i_1, \ldots, i_n)\, v_{1i_2} v_{2i_1} \ldots v_{ni_n} = -f(v_1, v_2, \ldots, v_n),$$

поскольку при любой транспозиции знак перестановки меняется. ∎

Коэффициент

$$\sum_{(i_1,i_2,\ldots,i_n)\in S_n} \operatorname{sgn}(i_1, i_2, \ldots, i_n)\, v_{1i_1} v_{2i_2} \ldots v_{ni_n}$$

перед $f(e_1, e_2, \ldots, e_n)$ в формуле (18) называется *определителем матрицы*

$$\begin{vmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{vmatrix}.$$

Свойства 1) и 2) предыдущего определения означают, что он линеен и кососимметричен по строкам. Матрица, составленная из координатных строк базисных векторов, является единичной, откуда видно, что свойство 3) означает, что на единичной матрице порядка n определитель принимает значение 1.

3.2 Основные теоремы об определителях

В предыдущем параграфе мы показали, что если зафиксировать правый ортонормированный базис в пространстве (на плоскости), то ориентированный объем параллелепипеда (ориентированная площадь параллелограмма), построенного на упорядоченной тройке (упорядоченной паре) векторов равна определителю матрицы, составленной из координатных строк этих векторов, записанных в данном порядке.

Поэтому свойства определителей (по крайней мере порядков 2 и 3) вполне аналогичны свойствам ориентированных площадей или объемов. А именно, смешанное произведение линейно по каждому аргументу, меняет знак при перестановке любых двух аргументов и смешанное произведение базисных векторов правого ортонормированного базиса равно 1. Это дает соответственно свойства линейности определителя матрицы по строкам, кососимметричности определителя по строкам (при перестановке любых двух строк определитель меняет знак) и условие нормировки: определитель единичной матрицы равен единице. Те же свойства определитель имеет и по столбцам.

С точки зрения алгебры значение определителей, в частности, в том, что они дают удобный критерий невырожденности матрицы, с помощью них можно получить явные формулы для обратной матрицы и т.д.

Хотя понятие определителя n-го порядка можно определить над любым полем, мы в этом параграфе будем считать, что $\mathbb{K}$ — произвольное поле характеристики $\neq 2$ (в частности, подходит любое поле $\mathbb{K}$, содержащее поле рациональных чисел $\mathbb{Q}$ — например $\mathbb{R}$ или $\mathbb{C}$).

Пусть V — векторное пространство над полем $\mathbb{K}$.

Определение 3.18. Функция $f\colon V \to \mathbb{K}$ называется *линейной*, если

$$\forall\, u,\, v \in V \quad f(u+v) = f(u) + f(v)$$

и

$$\forall\, v \in V,\ \lambda \in \mathbb{K} \quad f(\lambda v) = \lambda f(v).$$

Если f линейна, то для любой конечной линейной комбинации $\sum_i \lambda_i v_i$ векторов пространства V имеем

$$f\left(\sum_i \lambda_i v_i\right) = \sum_i \lambda_i f(v_i).$$

Пусть теперь $f\colon V \times V \times \ldots \times V \to \mathbb{K}$ (m сомножителей слева) — $\mathbb{K}$-значная функция от m аргументов (упорядоченных наборов из m векторов пространства V).

Определение 3.19. Функция $f\colon V \times V \times \ldots \times V \to \mathbb{K}$ называется *полилинейной* (точнее, *m-линейной*), если она линейна по каждому из m аргументов при фиксированных остальных.

Например, линейность по первому аргументу означает, что

$$f(v_1' + v_1'', v_2, \ldots, v_m) = f(v_1', v_2, \ldots, v_m) + f(v_1'', v_2, \ldots, v_m) \;\; \forall\, v_1', v_1'', v_2, \ldots, v_m \in V$$

и

$$f(\lambda v_1, v_2, \ldots, v_m) = \lambda f(v_1, v_2, \ldots, v_m) \;\; \forall v_1, v_2, \ldots, v_m \in V \;\text{ и }\; \lambda \in \mathbb{K}.$$

Предложение 3.20. *Следующие условия на полилинейную функцию* $f\colon V \times V \times \ldots \times V \to \mathbb{K}$ *эквивалентны:*

1) при перестановке любых двух аргументов значение f *меняет знак;*

2) если для некоторой пары $i \neq j$ $v_i = v_j$, *то* $f(v_1, \ldots, v_m) = 0$.

Доказательство. 1) $\Rightarrow$ 2) : при перестановке двух совпадающих аргументов значение функции одновременно меняет знак и не меняется, значит, это такой элемент $a \in \mathbb{K}$, что $a = -a \;\Leftrightarrow\; 2a = 0 \;\Leftrightarrow a = 0$ (напомним, что мы предположили, что $\operatorname{char}\mathbb{K} \neq 2$).

2) $\Rightarrow$ 1) : $\quad 0 = f(v_1, \ldots, v_i + v_j, \ldots, v_i + v_j, \ldots, v_m) =$

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_m) + f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_m)$$

(напомним, что f по предположению полилинейна). ∎

Определение 3.21. Полилинейная функция называется *кососимметрической*, если она удовлетворяет любому из эквивалентных условий из предыдущего Предложения.

В качестве векторного пространства V возьмем пространство $\mathbb{K}^n$ строк длины n с элементами из $\mathbb{K}$. Заметим, что множество матриц $\mathrm{Mat}_n(\mathbb{K})$ можно отождествить с множеством $V \times \ldots \times V$ наборов из n строк длины n (при этом отождествлении матрице сопоставляется набор ее строк).

Определение 3.22. *Определителем порядка* n называется полилинейная кососимметричная функция $f\colon \mathrm{Mat}_n(\mathbb{K}) \to \mathbb{K}$ строк матриц, принимающая на единичной матрице $E \in \mathrm{Mat}_n(\mathbb{K})$ значение 1.

Определитель матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$ обозначается $\det(A)$ или просто $|A|$.

Следующая теорема играет ключевую роль в нашем подходе к теории определителей.

Теорема 3.23. *Определитель* n*-го порядка существует и единственен. Более того, для любой полилинейной кососимметричной функции строк матриц* $f\colon \mathrm{Mat}_n(\mathbb{K}) \to \mathbb{K}$ *верно равенство* $f(A) = \det(A) f(E) \;\; \forall\, A \in \mathrm{Mat}_n(\mathbb{K})$.

Последнее равенство означает, что любая полилинейная кососимметричная функция строк матриц порядка n пропорциональна определителю с коэффициентом, равным ее значению на единичной матрице.

Читателю рекомендуется связать приведенное ниже доказательство с доказательствами Теорем 3.2, 3.4 и 3.10 (поскольку первые две из них — частные случаи, а третья — по-существу, эквивалентна доказываемой теореме).

Доказательство. Докажем сначала единственность определителя. Итак, пусть f — полилинейная кососимметричная функция строк матриц порядка n. Для матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$ пусть $a_1, \ldots, a_n$ обозначают ее строки. То есть $a_i = (a_{i1}, a_{i2}, \ldots, a_{in}),\ i = 1, \ldots, n$. Введем *единичные строки* $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 стоит на i-м месте) длины n, $i = 1, \ldots, n$. Они образуют базис в пространстве строк длины n. В частности, i-я строка матрицы A по ним раскладывается (единственным образом) как

$$a_i = \sum_{k=1}^{n} a_{ik} e_k.$$

В силу полилинейности f имеем

$$f(A) = f(a_1, \ldots, a_n) = \sum_{k_1, k_2, \ldots, k_n} a_{1k_1} a_{2k_2} \ldots a_{nk_n} f(e_{k_1}, e_{k_2}, \ldots, e_{k_n})$$

(справа стоит сумма n^n слагаемых, так как k_j независимо пробегают натуральные числа от 1 до n). В частности, полилинейная функция однозначно задается своими значениями на наборах векторов из некоторого базиса.

Теперь воспользуемся кососимметричностью f. Очевидно, что

$$f(e_{k_1}, e_{k_2}, \ldots, e_{k_n}) = 0 \quad \text{если } k_i = k_j \text{ для некоторой пары } i \neq j,$$

иначе

$$f(e_{k_1}, e_{k_2}, \ldots, e_{k_n}) = \mathrm{sgn}(k_1, \ldots, k_n) f(e_1, \ldots, e_n).$$

Для доказательства последнего равенства во-первых заметим, что при любой транспозиции левая и правая части меняют знак; во-вторых, любая перестановка приводится к тривиальной с помощью последовательности транспозиций, и в-третьих, оно верно для тривиальной перестановки.

В итоге, для произвольной полилинейной кососимметрической функции строк матрицы мы получаем формулу

$$f(A) = f(a_1, \ldots, a_n) =$$
$$= \sum_{(k_1, k_2, \ldots, k_n) \in S_n} \mathrm{sgn}(k_1, k_2, \ldots, k_n)\, a_{1k_1} a_{2k_2} \ldots a_{nk_n} f(e_1, e_2, \ldots, e_n)$$

(в правой части последней формулы $n!$ слагаемых). Поскольку $f(E) = f(e_1, \ldots, e_n)$, определитель матрицы A, если он существует, через ее матричные элементы выражается следующим образом:

$$\det(A) = \sum_{(k_1, k_2, \ldots, k_n) \in S_n} \mathrm{sgn}(k_1, k_2, \ldots, k_n)\, a_{1k_1} a_{2k_2} \ldots a_{nk_n} \tag{19}$$

(ср. (18)).

Таким образом, нам осталось доказать, что формула (19) определяет полилинейную кососимметричную функцию (поскольку любая функция, пропорциональная полилинейной кососимметрической, также является таковой).

Для этого посмотрим внимательно на правую часть (19). Она содержит $n!$ слагаемых, каждое из которых является произведением, в которое входит по одному элементу из каждой строки и каждого столбца матрицы A (последнее потому что $(k_1, k_2, \dots, k_n)$ — перестановка чисел $1, 2, \dots n$). Таким образом, если мы выбираем i-ю строку, то (19) можно записать в виде

$$\det A = \sum_{j=1}^{n} a_{ij} u_j,$$

где u_j (позднее мы отождествим их с алгебраическими дополнениями, ср. Теорему 3.40) не зависят от элементов i-й строки матрицы A. Например, для $i = 1$ имеем:

$$\det(A) = \sum_{(k_1,k_2,\dots,k_n)\in S_n} \operatorname{sgn}(k_1, k_2, \dots, k_n)\, a_{1k_1} a_{2k_2} \dots a_{nk_n} =$$

$$= a_{11} \sum_{(1,k_2,\dots,k_n)\in S_n} \operatorname{sgn}(1, k_2, \dots, k_n) a_{2k_2} \dots a_{nk_n} + a_{12} \sum_{(2,k_2,\dots,k_n)\in S_n} \operatorname{sgn}(2, k_2, \dots, k_n) a_{2k_2} \dots a_{nk_n} + \dots$$

$$+ a_{1n} \sum_{(n,k_2,\dots,k_n)\in S_n} \operatorname{sgn}(n, k_2, \dots, k_n) a_{2k_2} \dots a_{nk_n}$$

(каждая из n сумм в правой части содержит $(n-1)!$ слагаемых, то есть всего слагаемых $n!$).

Осталось доказать, что функция, определяемая формулой (19) — кососимметричная функция строк матрицы A. В силу Предложения 3.20 достаточно убедиться в том, что она принимает нулевое значение на матрице, у которой две строки, скажем, i-я и j-я, совпадают.

Разобьем множество всех перестановок на пары, получаемые друг из друга транспозицией k_i и k_j. Согласно Предложению 3.12, равные в силу $a_{ik} = a_{jk}$ произведения $a_{1k_1} a_{2k_2} \dots a_{nk_n}$, соответствующие перестановкам из одной такой пары, входят в выражение (19) с противоположными знаками. Значит, вся сумма равна нулю. ■

В доказательстве Теоремы нами получена важная формула (19), называемая *формулой полного разложения* определителя n-го порядка.

Задача 3.24. *Убедитесь, что при $n = 2, 3$ формула (19) дает известные выражения для определителей второго и третьего порядков.*

Задача 3.25. *1) Имеются ли в формуле полного разложения определителя матрицы $A = (a_{ij})$ пятого порядка слагаемые $a_{15}a_{12}a_{34}a_{21}a_{43}$, $a_{55}a_{12}a_{34}a_{21}a_{43}$? 2) С какими знаками входят в формулу полного разложения определителя матрицы пятого порядка слагаемые $a_{12}a_{21}a_{34}a_{45}a_{53}$, $a_{15}a_{23}a_{34}a_{41}a_{52}$?*

Задача 3.26. *Докажите, что если в определителе порядка n на пересечении некоторых k строк и l столбцов стоят элементы, равные нулю, причем $k+l>n$, то определитель равен нулю.*

Пример 3.27. Из (17) легко получить, что

$$\det\begin{pmatrix} 0 & 0 & \dots & 0 & \lambda_1 \\ 0 & 0 & \dots & \lambda_2 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \lambda_n & 0 & \dots & 0 & 0 \end{pmatrix} = (-1)^{\frac{n(n-1)}{2}}\lambda_1\dots\lambda_n.$$

Задача 3.28. *Докажите, что для любой квадратной вещественной матрицы A верно равенство $\det(E+hA) = 1 + h\operatorname{tr}A + O(h^2)$*[23] *при $h\to 0$. Какой геометрический смысл (с точки зрения ориентированных объемов) имеет эта формула?*

Предложение 3.29. *При элементарных преобразованиях строк, введенных в Определении 2.22, определитель меняется следующим образом. При элементарных преобразованиях типа I от не меняется, при преобразованиях типа II — умножается на -1, при преобразованиях типа III — умножается на c.*

Доказательство. В случае элементарного преобразования типа I i-я строка преобразованной матрицы A' равна $a_i+\lambda a_j$ (при этом остальные строки такие же как у исходной матрицы A). Используя линейность определителя по i-й строке, получаем, что $\det A'$ равен сумме $\det A$ и λ, умноженной на определитель матрицы, у которой две одинаковые строки (а именно i-я и j-я, равные a_j). В силу кососимметричности определителя по строкам последний определитель равен нулю.

Поведение определителя при элементарных преобразованиях типа II и III следует непосредственно из его кососимметричности и линейности по строкам. ■

Задача 3.30. *Покажите, что $\det A_\sigma = \operatorname{sgn}\sigma$, где A_σ — матрица из Задачи 2.48.*

Следствие 3.31. *Для любой матрицы $A\in \mathrm{Mat}_n(\mathbb{K})$ и элементарной матрицы S имеем*

$$\det(SA) = \det(S)\det(A).$$

В частности, определитель невырожденной матрицы равен произведению определителей элементарных матриц, в произведение которых она раскладывается.

Доказательство. Напомним, что если элементарная матрица S отвечает элементарному преобразованию строк ς, то $\forall\, A\in\mathrm{Mat}_n(\mathbb{K})$ имеем $\varsigma A = SA$. Отсюда $\det(\varsigma A) = \det(SA)$. В частности, полагая $A=E$, из Предложения 3.29 получаем, что $\det S$ равно 1, -1 и c, если ς — элементарное преобразование из Определения 2.22 типа I, II и III соответственно. Осталось еще раз применить Предложение 3.29. ■

Предложение 3.29 дает эффективный метод вычисления определителей. А именно, мы знаем, что любую квадратную матрицу с помощью элементарных преобразований строк

[23] здесь $\operatorname{tr}A$ обозначает *след* квадратой матрицы A, который просто равен сумме ее диагональных элементов.

можно привести к верхней треугольной матрице, причем при каждом элементарном преобразовании Предложение 3.29 позволяет контролировать изменение определителя. То есть достаточно научиться считать определители верхних треугольных матриц.

Предложение 3.32. *Определитель верхней треугольной матрицы равен произведению элементов, стоящих на главной диагонали.*

Доказательство. Согласно формуле (19) каждое слагаемое в разложении определителя является произведением, в которое входит по одному элементу из каждой строки и каждого столбца. В первом столбце единственный элемент, который может быть ненулевым у верхней треугольной матрицы это a_{11}; если мы его выбираем, то из второго столбца мы должны взять элемент не из первой строки; единственный такой элемент, который может быть отличен от нуля, это a_{22} и т.д. ∎

Задача 3.33. *Вычислите определитель из Примера 3.27 с помощью перестановок строк.*

Следующая теорема дает обещанный ранее критерий невырожденности матрицы.

Теорема 3.34. *Матрица A невырождена тогда и только тогда, когда* $\det A \neq 0$.

Доказательство. Если для какой-то матрицы определитель отличен от нуля (равен нулю), то поскольку максимум что с ним может произойти при элементарных преобразованиях строк — умножение на ненулевое число, он также отличен от нуля (соотв. равен нулю) на всем классе строчно эквивалентных ей матриц.

Из предыдущего мы знаем, что матрица невырождена тогда и только тогда, когда ее класс строчной эквивалентности содержит строгую верхнетреугольную матрицу (т.е. такую верхнетреугольную матрицу, у которой на главной диагонали стоят ненулевые элементы), определитель которой согласно предыдущему Предложению отличен от нуля.

Если же исходная матрица вырождена, то она строчно эквивалентна такой верхнетреугольной матрице, у которой на главной диагонали обязательно есть нули, и значит ее определитель опять же в силу предыдущего Предложения равен нулю. ∎

Следующая наша цель — доказательство того, что свойства определителя (полилинейность, кососимметричность) относительно столбцов такие же как относительно строк.

Мы знаем, что в выражение (19) входят все произведения матричных элементов по одному из каждой строки и из каждого столбца. Как определить знак, с которым произведение $a_{i_1j_1}a_{i_2j_2}\dots a_{i_nj_n}$ входит в (19), не упорядочивая его по возрастанию номеров строк?

Лемма 3.35. Пусть $(i_1, i_2, \dots, i_n)$ и $(j_1, j_2, \dots, j_n)$ — две произвольные перестановки. Тогда произведение $a_{i_1j_1}a_{i_2j_2}\dots a_{i_nj_n}$ входит в выражение (19) со знаком, равным произведению их знаков $\operatorname{sgn}(i_1, i_2, \dots, i_n)\operatorname{sgn}(j_1, j_2, \dots, j_n)$.

Доказательство. Для того, чтобы выяснить, с каким знаком входит в (19) рассматриваемое произведение, нужно расположить его сомножители в порядке возрастания номеров строк. Этого можно добиться, последовательно меняя местами два сомножителя. При каждой такой перемене в перестановках, образуемых номерами строк и столбцов, происходят транспозиции, так что произведение их знаков не меняется. Таким образом, если полученное в результате произведение будет иметь вид $a_{1k_1}a_{2k_2}\dots a_{nk_n}$, то

$$\operatorname{sgn}(k_1,k_2,\dots,k_n)=\operatorname{sgn}(1,2,\dots,n)\operatorname{sgn}(k_1,k_2,\dots,k_n)=$$

$$\operatorname{sgn}(i_1,i_2,\dots,i_n)\operatorname{sgn}(j_1,j_2,\dots,j_n),$$

а это и означает, что рассматриваемое произведение входит в (19) с указанным знаком. ∎

Теорема 3.36. $\det A^T=\det A$.

Доказательство. Определитель матрицы A^T, как и определитель матрицы A, есть алгебраическая сумма всевозможных произведений n элементов матрицы A, взятых по одному из каждой строки и из каждого столбца. Единственное, за чем надо проследить — это то, что одинаковые произведения входят в $\det A$ и $\det A^T$ с одинаковыми знаками.

В силу предыдущей Леммы для перестановок $(i_1,i_2,\dots,i_n)$ и $(j_1,j_2,\dots,j_n)$ произведение $a_{i_1j_1}a_{i_2j_2}\dots a_{i_nj_n}$ входит в разложение определителя матрицы A со знаком $\operatorname{sgn}(i_1,i_2,\dots,i_n)\operatorname{sgn}(j_1,j_2,\dots,j_n)$. В разложение определителя $\det A^T$ это же произведение $a_{i_1j_1}a_{i_2j_2}\dots a_{i_nj_n}=a^T_{j_1i_1}a^T_{j_2i_2}\dots a^T_{j_ni_n}$ в силу предыдущей Леммы входит с тем же знаком. ∎

Заметим, что из доказанной Теоремы снова легко вывести Следствие 2.40.

Следствие 3.37. *Определитель есть полилинейная кососимметрическая функция столбцов матрицы. Любая такая функция пропорциональна определителю с коэффициентом, равным ее значению на единичной матрице.*

Теорема 3.38. (об определителе матрицы с углом нулей). *Пусть матрица A имеет вид*

$$A=\begin{pmatrix}B & D\\ 0 & C\end{pmatrix},$$

где B и C — квадратные матрицы порядков k и $n-k$ соответственно. Тогда $\det A=\det B\cdot\det C$.

Доказательство. Для фиксированных матриц $C\in\operatorname{Mat}_{n-k}(\mathbb{K})$ и $D\in\operatorname{Mat}_{k\times(n-k)}(\mathbb{K})$ определим функцию $f_{D,C}\colon\operatorname{Mat}_k(\mathbb{K})\to\mathbb{K}$ формулой

$$f_{D,C}(B):=\det\begin{pmatrix}B & D\\ 0 & C\end{pmatrix}\quad\forall\,B\in\operatorname{Mat}_k(\mathbb{K}).$$

Функция $f_{D,C}$ является полилинейной и кососимметричной функцией столбцов матрицы B, поэтому по Теореме 3.23 $f_{D,C}(B) = \det(B) f_{D,C}(E)$. Аналогично, для фиксированной матрицы $D \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{K})$ определим функцию $g_D\colon \mathrm{Mat}_{n-k}(\mathbb{K}) \to \mathbb{K}$ формулой

$$g_D(C) := \det \begin{pmatrix} E & D \\ 0 & C \end{pmatrix} \quad \forall\, C \in \mathrm{Mat}_{n-k}(\mathbb{K}).$$

Функция g_D является полилинейной и кососимметричной функцией строк матрицы C, поэтому $g_D(C) = \det(C) g_D(E)$. Собирая все вместе, с учетом того, что $f_{D,C}(E) = g_D(C)$ и $g_D(E) = 1$, получаем требуемое. ∎

Пусть A — произвольная (не обязательно квадратная) матрица. Всякая матрица, составленная из элементов матрицы A, находящихся на пересечении каких-то выбранных строк и каких-то выбранных столбцов, называется *подматрицей* матрицы A. Подчеркнем, что выбираемые строки и столбцы не обязаны идти подряд.

Определитель квадратной подматрицы порядка k называется *минором* порядка k матрицы A. Иногда, допуская вольность речи, саму квадратную подматрицу также называют минором. В частности, если A — квадратная матрица порядка n, то минор порядка $n-1$, получаемый вычеркиванием i-й строки и j-го столбца, называется *дополнительным минором* элемента a_{ij} и обозначается через M_{ij}. Число

$$A_{ij} := (-1)^{i+j} M_{ij}$$

называется *алгебраическим дополнением* элемента a_{ij}. Смысл алгебраического дополнения ясен из следующей леммы.

Лемма 3.39.

$$\begin{vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & a_{ij} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix} = a_{ij} A_{ij}.$$

(В левой части стоит определитель матрицы, полученной из матрицы $A = (a_{ij})$ заменой нулями всех элементов i-й строки, кроме a_{ij}.)

Доказательство. Поменяем местами i-ю строку со всеми предыдущими строками и j-й столбец со всеми предыдущими столбцами. При этом мы будем $i-1$ раз менять местами строки и $j-1$ раз столбцы, так что определитель умножится на $(-1)^{i-1+j-1} = (-1)^{i+j}$. В результате получится определитель вида

$$\begin{vmatrix} a_{ij} & 0 & \dots & 0 \\ a_{1j} & a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{nj} & a_{n1} & \dots & a_{nn} \end{vmatrix},$$

где в правом нижнем углу стоит дополнительный минор элемента a_{ij}. По теореме об определителе матрицы с углом нулей этот определитель равен $a_{ij}M_{ij}$. С учетом предыдущего знака отсюда и получается доказываемое равенство. ■

Теорема 3.40. *Для любой квадратной матрицы A*

$$\det A = \sum_j a_{ij}A_{ij} = \sum_i a_{ij}A_{ij}.$$

Первая из этих формул называется *формулой разложения определителя по i-й стоке*, вторая — *формулой разложения определителя по j-му столбцу.*

Доказательство. Представим i-ю строку $(a_{i1}, a_{i2}, \ldots, a_{in})$ матрицы A в виде суммы строк

$$(a_{i1}, 0, 0, \ldots, 0, 0) + (0, a_{i2}, 0, \ldots, 0, 0) + \ldots + (0, 0, 0, \ldots, 0, a_{in})$$

и воспользуемся линейностью определителя по строкам и предыдущей Леммой. Аналогично для столбца. ■

Теорема 3.41. *Для любых квадратных матриц A и B одного порядка* $\det(AB) = \det A \cdot \det B$.

Доказательство. При фиксированной матрице $B \in \mathrm{Mat}_n(\mathbb{K})$ определим функцию

$$f_B \colon \mathrm{Mat}_n(\mathbb{K}) \to \mathbb{K}, \qquad f_B(A) := \det(AB).$$

Мы утверждаем, что она полилинейна и кососимметрична как функция строк матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$. Для этого заметим, что строки $c_1, \ldots, c_n$ матрицы $C := AB$ получаются из строк $a_1, \ldots, a_n$ матрицы A умножением на B:

$$c_i = a_i B \quad (i = 1, \ldots, n).$$

Пусть например $a_1 = a_1' + a_1''$, где a_1', a_1'' — какие-то строки; тогда, рассматривая матрицу A как совокупность ее строк, имеем

$$\det(AB) = f_B(A) = f_B(a_1' + a_1'', a_2, \ldots, a_n) = \det((a_1' + a_1'')B, a_2B, \ldots, a_nB) =$$

$$= \det(a_1'B + a_1''B, a_2B, \ldots, a_nB) = \det(a_1'B, a_2B, \ldots, a_nB) + \det(a_1''B, a_2B, \ldots, a_nB) =$$

$$= f_B(a_1', a_2, \ldots, a_n) + f_B(a_1'', a_2, \ldots, a_n).$$

Остальные свойства проверяются аналогично. Тогда согласно Теореме 3.23 $f_B(A) = \det A \cdot f_B(E)$, что равносильно требуемому. ■.

Замечание 3.42. Наметим также другое доказательство предыдущей Теоремы, использующее свойства элементарных матриц. Во-первых, предположим что матрица A вырождена. Последнее равносильно существованию ненулевой строки c такой, что $cA = 0$. Тогда и $0 = (cA)B = c(AB)$, значит, произведение AB тоже вырождено. Так как определитель вырожденной матрицы равен нулю, то Теорема в этом случае верна.

Пусть теперь A невырождена. Тогда она представляется в виде произведения элементарных матриц. Теперь требуемое легко вывести из Следствия 3.31.

Задача 3.43. *Докажите, что следующие условия равносильны:*

1) $\det A = 1$;

2) матрицу A можно привести к единичной матрице используя только преобразования типа I;

3) матрица A является произведением элементарных матриц типа I.

3.3 Некоторые приложения определителей

Рассмотрим квадратную систему линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= b_n. \end{cases} \tag{20}$$

Обозначим через A ее матрицу коэффициентов и через A_i $(i = 1, 2, \ldots, n)$ матрицу, полученную из A заменой ее i-го столбца столбцом свободных членов.

Теорема 3.44. *Если* $\det A \neq 0$, *то система (20) имеет единственное решение* $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, *которое может быть найдено по формулам*

$$\alpha_i = \frac{\det A_i}{\det A} \qquad (i = 1, 2, \ldots, n). \tag{21}$$

Эти формулы называются *формулами Крамера.*

Доказательство. Будем производить элементарные преобразования строк расширенной матрицы системы (20) с целью привести ее матрицу коэффициентов к единичной матрице (это возможно, поскольку по условию A невырождена). При этом система будет заменяться эквивалентной. Кроме того, правая часть (21) также не меняется при элементарных преобразованиях (при элементарных преобразованиях типа I числитель и знаменатель не меняются, при преобразованиях типа II числитель и знаменатель меняют знак, при преобразованиях типа III умножаются на одно и то же ненулевое число).

Таким образом, формулы Крамера достаточно проверить для системы с единичной матрицей коэффициентов, то есть вида

$$\begin{cases} x_1 &= b_1 \\ x_2 &= b_2 \\ \ldots\ldots\ldots\ldots\ldots \\ x_n &= b_n. \end{cases}$$

Она, очевидно, имеет единственное решение $\alpha_i = b_i$ $(i = 1, \ldots, n)$. С другой стороны,

$$\det A = \det E = 1, \qquad \det A_i = \begin{vmatrix} 1 & 0 & \ldots & 0 & b_1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & b_2 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 & b_n & 0 & \ldots & 1 \end{vmatrix} = b_i,$$

так что формулы Крамера в этом случае действительно верны. ■

Из только что доказанной теоремы следует, что если определитель квадратной матрицы порядка n отличен от нуля, то ее столбцы образуют базис в линейном пространстве $\mathbb{K}^n$ столбцов высоты n, поскольку любой столбец $(b_1, \dots, b_n)$ по ним однозначно раскладывается.

Заметим, что если система (20) имеет единственное решение, то столбцы матрицы A линейно независимы (ср. Лемму 6.3 ниже), что согласно Следствию 2.39 равносильно тому, что матрица невырождена, что, в свою очередь по Теореме 3.34 равносильно условию $\det A \neq 0$.

Применим теперь формулы Крамера для явного нахождения обратной матрицы.

Теорема 3.45. *Пусть $A = (a_{ij})$ — невырожденная матрица. Тогда*

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}$$

(напомним, что A_{ij} обозначает алгебраическое дополнение элемента a_{ij}).

Доказательство. Матрица A^{-1} является решением матричного уравнения $AX = E$. Это уравнение распадается на n уравнений относительно столбцов X_1, X_2, …, X_n матрицы X:

$$AX_j = E_j, \tag{22}$$

где E_j — j-й столбец матрицы E.

В координатной записи уравнение (22) представляет собой систему n линейных уравнений относительно элементов $x_{1j}, x_{2j}, \dots, x_{nj}$ столбца X_j. Матрицей коэффициентов этой системы служит матрица A, а столбцом свободных членов — столбец E_j. По формулам Крамера i-я компонента решения равна

$$x_{ij} = \frac{\det A_i}{\det A} = \frac{1}{\det A} \begin{vmatrix} a_{11} & \dots & 0 & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{j1} & \dots & 1 & \dots & a_{jn} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & 0 & \dots & a_{nn} \end{vmatrix} = \frac{A_{ji}}{\det A}$$

(в определителе 1 стоит в i-м столбце), что и требовалось доказать ■.

Задача 3.46. *Решите Задачу 3.5, используя свойства определителей. Предложите ее обобщение на n-мерный случай. (Указание: выберем ортонормированный базис и запишем координаты векторов $\{u, v, w\}$ и $\{x, y, z\}$ в нем в строки матриц A и B соответственно. Тогда произведение AB^T будет равно правой части формулы (16)).*

3.4 Присоединенная матрица

Пусть A — матрица порядка n. Ее *присоединенной матрицей* $\widehat{A}$ называется транспонированная к матрице, составленной из алгебраических дополнений матрицы A. Иными словами, если $\widehat{A} = (\widehat{a}_{ij})$, то $\widehat{a}_{ij} = A_{ji}$, где A_{ij} — алгебраическое дополнение элемента a_{ij} матрицы A. Из Теоремы 3.45 немедленно следует, что для обратимой матрицы A верно равенство

$$A\widehat{A} = \widehat{A}A = (\det A)\, E, \tag{23}$$

где E — единичная матрица порядка n.

Предложение 3.47. *Формула (23) верна для произвольной квадратной матрицы A.*

Доказательство. Докажем, например, $A\widehat{A} = (\det A)\, E$. Произведение i-й строки A на i-й столбец $\widehat{A}$ совпадает с разложением определителя A по i-й строке, то есть равно $\det A$. То есть все диагональные элементы матрицы $A\widehat{A}$ равны $\det A$.

Произведение i-й строки A на j-й столбец $\widehat{A}$ при $i \neq j$ равно, как легко убедится читатель, разложению по j-й строке определителя матрицы, которая получается из A заменой j-й строки на i-ю строку (все остальные строки кроме j-й у нее такие же как у A). Так как у такой матрицы две одинаковые строки, то в силу кососимметричности по строкам, ее определитель равен нулю. Это показывает, что в матрице $A\widehat{A}$ все элементы вне главной диагонали равны нулю. ■

Заметим, что из доказанного Предложения снова вытекает Теорема 3.45.

4 Группы

В этом разделе мы продолжаем изучение групп, начатое в параграфах 1.4 и 1.5.

4.1 Гомоморфизмы и изоморфизмы групп

Сравним таблицы умножения групп $(\mathbb{Z}_3, +)$ и $(\mu_3, \cdot)$, где $\mu_n \subset \mathbb{C}^*$ — группа комплексных корней n-й степени из 1. Обозначим $\varepsilon := \exp(2\pi i/3)$, тогда

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	1	ε	ε^2
1	1	ε	ε^2
ε	ε	ε^2	1
ε^2	ε^2	1	ε

Мы видим, что таблицы умножения двух указанных групп с точностью до переобозначений элементов совпадают. Поскольку таблица умножения содержит всю информацию о бинарной операции, эти две группы устроены одинаково как множества с операцией. В этом случае говорят, что рассматриваемые группы *изоморфны*.

Дадим формальное определение.

Определение 4.1. Пусть $(G, \cdot)$ и $(H, *)$ — две группы. Биективное отображение

$$\varphi\colon G \to H$$

называется *изоморфизмом* между $(G, \cdot)$ и $(H, *)$, если для любых $g_1, g_2 \in G$

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2). \tag{24}$$

Группы $(G, \cdot)$ и $(H, *)$ называются *изоморфными* (что обозначается как $(G, \cdot) \cong (H, *)$ или просто $G \cong H$), если из $(G, \cdot)$ в $(H, *)$ существует хотя бы один изоморфизм.

Предложение 4.2. *1) Композиция изоморфизмов изоморфизм.*

2) Отображение, обратное к изоморфизму[24]*, изоморфизм.*

3) Тождественное отображение является изоморфизмом.

Доказательство. 1) Пусть $\varphi\colon (G, \cdot) \to (H, *)$ и $\psi\colon (H, *) \to (K, \circ)$ — изоморфизмы. Тогда $\psi\varphi\colon (G, \cdot) \to (K, \circ)$ — биекция и мы имеем

$$(\psi\varphi)(g_1 \cdot g_2) = \psi(\varphi(g_1 \cdot g_2)) = \psi(\varphi(g_1) * \varphi(g_2)) =$$

$$= \psi(\varphi(g_1)) \circ \psi(\varphi(g_2)) = (\psi\varphi)(g_1) \circ (\psi\varphi)(g_2).$$

2) Пусть $\varphi\colon (G, \cdot) \to (H, *)$ — изоморфизм и $\varphi^{-1}\colon H \to G$ — теоретико-множественно обратное к φ. Нужно проверить, что $\forall\, h_1, h_2 \in H\ \varphi^{-1}(h_1 * h_2) = \varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2)$.

Пусть $h_i = \varphi(g_i)$, $i = 1, 2$ (такие g_1 и g_2 существуют и единственны в силу биективности φ). Тогда $h_1 * h_2 = \varphi(g_1 \circ g_2)$ в силу (24), а значит

$$\varphi^{-1}(h_1 * h_2) = g_1 \circ g_2 = \varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2).$$

Пункт 3) очевиден. ■

Следствие 4.3. *На "множестве" групп отношение "быть изоморфными" является отношением эквивалентности.*

Задача 4.4. *Найдите изоморфизм $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$. Проверьте, что обратное отображение к найденному также является изоморфизмом.*

Задача 4.5. *Для поля $\mathbb{K}$ постройте изоморфизм между группой $(\mathbb{K}, +)$ и группой матриц вида*

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K})$$

с операцией умножения.

Задача 4.6. *Пусть $\mathrm{U}(1) \subset \mathbb{C}^*$ — группа комплексных чисел, равных по модулю единице, с операцией умножения. Постройте изоморфизм между $\mathrm{U}(1)$ и группой вещественных матриц вида*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

с единичным определителем, с операцией умножения.

Таким образом, возникает естественная задача классификации всех групп с точностью до изоморфизма, то есть описание классов изоморфизма групп. В такой общности эта задача безнадёжна, хотя некоторые типы групп могут быть полностью классифицированы (ниже мы это сделаем для циклических групп, также это несложная задача для конечнопорождённых абелевых групп).

Для решения задачи классификации объектов некоторого типа в математике используют инварианты, которые одинаковы для всех объектов из одного класса. Очевидным инвариантом класса изоморфизма групп является мощность множества её элементов: если две группы $(G, \cdot)$ и $(H, *)$ изоморфны, то мощности множеств их элементов совпадают. Если мощность множества элементов группы $(G, \cdot)$ конечна, то ее называют *порядком* группы G и обозначают $|G|$.

[24] Оно существует, поскольку изоморфизм по определению биективен.

Назовём *структурой группы* на данном множестве X задание бинарной операции, которая удовлетворяет аксиомам группы.

Даже на конечных множествах, как правило, существуют операции, удовлетворяющие аксиомам группы, которые задают неизоморфные группы (например, с точностью до изоморфизма, существует 5 различных групп порядка 12, одна порядка 15[25] и 51 порядка 32). На пустом множестве нельзя задать структуру группы (поскольку по определению группы в ней есть хотя бы один элемент — нейтральный), на множестве из одного элемента или на множествах, мощность которых равна простому числу любые групповые операции задают изоморфные структуры группы (см. Следствие 4.77 и Теорему 4.41).

Задача 4.7. *Классифицируйте с точностью до изоморфизма группы порядка* 4.

Ещё одним инвариантом изоморфизма является такое свойство операции как коммутативность (или некоммутативность).

Задача 4.8. *Докажите, что если группа* $(G, \cdot)$ *коммутативна (некоммутативна), то и любая изоморфная ей группа коммутативна (некоммутативна).*

Классификация с точностью до изоморфизма абелевых групп данного конечного порядка n — несложная задача (при условии, что известно разложение n на простые), которая решается в более полных курсах алгебры.

В следующем параграфе мы познакомимся с определением циклической группы. Группа, изоморфная циклической, сама является циклической. Также мы определим порядки элементов группы и докажем, что при изоморфизме элемент порядка n отображается в элемент порядка n. Из этого следует, что если две группы изоморфны, то для любого n мощности множеств элементов порядка n в них равны. В несложных ситуациях этих соображений бывает достаточно, чтобы доказать неизоморфность конкретных групп.

Вообще, “абстрактная” теория групп интересуется только теми свойствами групп, которые сохраняются при изоморфизмах. Пример “свойства”, которое не сохраняется при изоморфизме — выбор конкретной реализации циклической группы порядка 3 в виде группы классов вычетов по модулю 3 либо как группы комплексных корней 3-й степени из 1 (см. пример в начале этого параграфа).

Задача 4.9. *Для данной группы* $(G, \cdot)$ *обозначим через* $(G^{op}, *)$ *то же самое множество элементов, но с (вообще говоря, другой) операцией* $*$*, задаваемой условием*

$$g_1 * g_2 := g_2 \cdot g_1 \ \forall g_1, g_2 \in G.$$

Докажите, что

1) $(G^{op}, *)$ *является группой;*

2) *отображение* $\varphi(g) = g^{-1}$ *является изоморфизмом* $(G, \cdot) \to (G, *)$.

Если в Определении 4.1 отказаться от условия биективности φ, мы придём к определению гомоморфизма групп.

Определение 4.10. Пусть $(G, \cdot)$ и $(H, *)$ — две группы. Отображение

$$\varphi \colon G \to H$$

называется *гомоморфизмом* между $(G, \cdot)$ и $(H, *)$, если для любых $g_1, g_2 \in G$

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2). \tag{25}$$

[25] Существует единственная с точностью до изоморфизма группа порядка n тогда и только тогда, когда $(n, \phi(n)) = 1$, где ϕ — функция Эйлера.

Задача 4.11. *Если $\varphi\colon G \to H$ — гомоморфизм групп, то*

1) $\varphi(e_G) = e_H$;

2) $\varphi(g^{-1}) = \varphi(g)^{-1}\ \forall\, g \in G$.

Задача 4.12. *1) Композиция гомоморфизмов групп — гомоморфизм групп.*

2) Тождественное отображение — гомоморфизм групп.

3) Изоморфизмы групп — в точности обратимые гомоморфизмы. Другими словами, гомоморфизм $\varphi\colon G \to H$ является изоморфизмом тогда и только тогда, когда существует гомоморфизм $\psi\colon H \to G$ такой, что $\psi\varphi = \mathrm{id}_G$, $\varphi\psi = \mathrm{id}_H$.

Заметим, что между любыми двумя группами G и H существует гомоморфизм, а именно *тривиальный гомоморфизм*, который все элементы группы G переводит в нейтральный элемент в H.

Приведем теперь примеры гомоморфизмов.

Пример 4.13. Отображение $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$, заданное формулой $\varphi(k) = [k]$, является гомоморфизмом групп.

Пример 4.14. Пусть $\mathrm{U}(1) \subset \mathbb{C}^*$ — группа комплексных чисел, равных по модулю единице, с операцией умножения. Отображение $\varphi\colon (\mathbb{R}, +) \to \mathrm{U}(1)$, заданное формулой $\varphi(x) = \exp(2\pi i x)$, является гомоморфизмом групп.

Пример 4.15. Отображение $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$, ставящее в соответствие обратимой матрице A ее определитель, является гомоморфизмом групп.

Пример 4.16. Пусть $m, n \in \mathbb{N}$, $m \mid n$. Отображение $\varphi\colon (\mathbb{Z}_n, +) \to (\mathbb{Z}_m, +)$, заданное формулой $\varphi([k]_n) = [k]_m$, является гомоморфизмом групп. Читателю, в частности, необходимо убедиться в корректности определения отображения φ.

Пример 4.17. Пусть D_3 — группа симметрий правильного треугольника. Рассмотрим отображение $\varphi\colon D_3 \to \{\pm 1\}$, заданное условием, что $\varphi(g) = -1$ если $g \in D_3$ меняет ориентацию плоскости и $\varphi(g) = 1$ если сохраняет. Тогда φ — гомоморфизм групп.

Пример 4.18. Зафиксируем натуральное n. Пусть отображение $\varphi_n\colon \mathbb{C}^* \to \mathbb{C}^*$ задано формулой $\varphi_n(z) = z^n$. Тогда φ_n — гомоморфизм групп.

Пример 4.19. Пусть $z \in \mathbb{C}^*$ — произвольное ненулевое комплексное число. Тогда отображение $\varphi\colon (\mathbb{Z}, +) \to \mathbb{C}^*$, заданное формулой $\varphi(n) = z^n$, является гомоморфизмом групп.

С каждым гомоморфизмом $\varphi\colon G \to H$ связаны две подгруппы — одна в G, называемая *ядром* φ, другая в H, называемая *образом* φ.

Определение 4.20. Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Тогда его *ядром* (обозначение: $\ker\varphi$) называется подгруппа

$$\{g \in G \mid \varphi(g) = e\} \subset G,$$

состоящая из элементов группы G, которые φ отображает в нейтральный элемент в H.

Определение 4.21. Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Тогда его *образом* (обозначение: $\mathrm{Im}\,\varphi$) называется подгруппа

$$\{h \in H \mid \exists\, g \in G \quad \text{такой, что} \quad \varphi(g) = h\} \subset H,$$

состоящая из элементов группы H, в которые отображаются элементы группы G.

Задача 4.22. *Убедитесь, что* $\ker\varphi \subset G$ *и* $\mathrm{Im}\,\varphi \subset H$ *в самом деле являются подгруппами.*

Предложение 4.23. *Гомоморфизм групп $\varphi\colon G \to H$ является*

1) инъективным $\Leftrightarrow \ \ker\varphi = \{e\}$;

2) сюръективным $\Leftrightarrow \ \operatorname{Im}\varphi = H$.

Доказательство. 1) В одну сторону утверждение тривиально: если $\ker\varphi \neq \{e\}$, то в нейтральный элемент группы H помимо нейтрального элемента группы G переходит еще какой-то элемент, и поэтому φ не инъективен.

Обратно, пусть φ не инъективен, тогда $\exists\, g_1 \neq g_2 \in G$ такие, что $\varphi(g_1) = \varphi(g_2)$. Но тогда и $e \neq g_1 g_2^{-1} \in \ker\varphi$, поскольку

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e.$$

Пункт 2) тривиален. ■

Пункт 1) из предыдущего Предложения весьма полезен: он утверждает, что для проверки инъективности гомоморфизма достаточно убедиться что прообраз нейтрального элемента состоит только из одного (нейтрального) элемента, тогда и прообразы всех элементов из образа одноэлементны. Ниже мы получим обобщение этого результата: в общем случае полные прообразы всех элементов из образа равномощны ядру.

Следствие 4.24. *Гомоморфизм групп $\varphi\colon G \to H$ является изоморфизмом* $\Leftrightarrow \ \ker\varphi = \{e\}$ *и* $\operatorname{Im}\varphi = H$.

Задача 4.25. *Найдите ядра и образы гомоморфизмов из приведённых выше примеров. Выясните, являются ли гомоморфизмы инъективными, сюръективными, изоморфизмами.*

4.2 Циклические группы

Пусть G — произвольная группа, а $g \in G$ — некоторый ее элемент. Определим целые степени элемента g следующими формулами:

$$g^k = \begin{cases} \underbrace{gg\dots g}_{k \text{ сомножителей}}, & \text{если } k > 0, \\ e, & \text{если } k = 0, \\ \underbrace{g^{-1}g^{-1}\dots g^{-1}}_{k \text{ сомножителей}}, & \text{если } k < 0. \end{cases} \tag{26}$$

Задача 4.26. *Докажите, что $g^k g^l = g^{k+l}$ для любых целых k, l. (Указание: рассмотрите отдельно несколько случаев).*

Из (26) следует, что $(g^k)^{-1} = g^{-k}$. Кроме того, $e = g^0$ по определению. Таким образом, степени элемента g образуют подгруппу в группе G. Она называется *циклической подгруппой, порожденной элементом* g, и обозначается $\langle g\rangle$.

Итак,

$$\langle g\rangle := \{g^k \mid k \in \mathbb{Z}\} \subset G$$

и результат Задачи 4.26 означает, что сопоставление $k \mapsto g^k$ задает гомоморфизм групп

$$\varphi_g\colon \mathbb{Z} \to G,$$

образом которого является подгруппа $\langle g\rangle \subset G$.

Для гомоморфизма φ_g возможны два варианта: либо он инъективен, либо нет. В первом случае все степени g различны и, в частности, группа $\langle g\rangle$ бесконечна. В этом случае говорят, что элемент $g \in G$ *имеет бесконечный порядок.*

Поскольку во втором случае по предположению гомоморфизм φ_g не инъективен, его ядро ненулевое. Из описания подгрупп группы $\mathbb{Z}$ (см. Пример 1.38) следует, что тогда $\ker \varphi_g = n\mathbb{Z} \subset \mathbb{Z}$, где $n \in \mathbb{N}$. Легко видеть, что n — наименьшее натуральное число такое, что $g^n = e$. Такое n называется *порядком* элемента $g \in G$ и обозначается $\operatorname{ord}(g)$.

Предложение 4.27. *Если* $\operatorname{ord}(g) = n$, *то*

1) $g^m = e \Leftrightarrow n|m$;

2) $g^k = g^l \Leftrightarrow n|(l-k)$.

Доказательство. 1) Разделим m на n с остатком:

$$m = qn + r, \quad 0 \leq r < n.$$

Тогда в силу определения порядка элемента $g^m = (g^n)^q \cdot g^r = g^r = e \Leftrightarrow r = 0$.

2) В силу предыдущего

$$g^k = g^l \Leftrightarrow g^{l-k} = e \Leftrightarrow n|(l-k). \quad \blacksquare$$

Мы видим, что если $\operatorname{ord}(g) = n$, то можно корректно определить $g^{[k]}$, где $[k] \in \mathbb{Z}_n$ — класс вычетов по модулю n.

Следствие 4.28. *Если* $\operatorname{ord}(g) = n$, *то подгруппа* $\langle g \rangle$ *содержит* n *элементов.*

Доказательство. Действительно, $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, причем все перечисленные элементы различны и исчерпывают $\langle g \rangle$. $\blacksquare$

Предложение 4.29. *Пусть* $\varphi\colon G \to H$ — *гомоморфизм групп и* $g \in G$ — *элемент конечного порядка. Тогда* $\operatorname{ord}(\varphi(g)) \mid \operatorname{ord}(g)$.

Доказательство. Пусть $\operatorname{ord} g = n$. Тогда $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$ и по пункту 1) Предложения 4.27 $\operatorname{ord}(\varphi(g)) \mid n$. $\blacksquare$

Следствие 4.30. *При изоморфизме групп элемент порядка* n *переходит в элемент порядка* n.

Доказательство.

$$n = \operatorname{ord}(\varphi^{-1}(\varphi(g))) \mid \operatorname{ord}(\varphi(g)) \mid \operatorname{ord}(g) = n. \quad \blacksquare$$

Задача 4.31. *Докажите, что* $\forall\, g \in G$ $\operatorname{ord}(g) = \operatorname{ord}(g^{-1})$. *(Указание: воспользуйтесь тем, что для любой абелевой группы* H *сопоставление* $h \mapsto h^{-1}$ *задает изоморфизм группы* H *на себя и тем, что группа* $\langle g \rangle$, *очевидно, абелева).*

Задача 4.32. *Докажите, что группы* $\mathbb{R}^*$ *и* $\mathbb{C}^*$ *не изоморфны.*

Задача 4.33. *Докажите, что для любой группы* G *и любых ее элементов* $g, h \in G$ $\operatorname{ord} g = \operatorname{ord}(hgh^{-1})$.

Чему равен порядок элемента g^k, если $\operatorname{ord}(g) = n$? Для пары натуральных чисел k, n их наиboord$(g) = n$,льший общий делитель обозначим (k, n).

Предложение 4.34. *Если* $\operatorname{ord}(g) = n$, *то*

$$\operatorname{ord}(g^k) = \frac{n}{(n,k)}.$$

Доказательство. Пусть

$$(n,k)=d,\ n=n_1d,\ k=k_1d,$$

так что $(n_1,k_1)=1$. Имеем

$$(g^k)^m=e\ \Leftrightarrow\ n\mid km\ \Leftrightarrow n_1\mid k_1m\ \Leftrightarrow\ n_1\mid m.$$

Следовательно, $\operatorname{ord}(g^k)=n_1$. ■

Определение 4.35. Группа G называется *циклической*, если существует такой элемент $g\in G$, что $G=\langle g\rangle$. Всякий такой элемент называется *порождающим* элементом группы G.

Пример 4.36. Группа $\mathbb{Z}$ циклическая, так как порождается элементом 1. С тем же успехом она порождается элементом -1. (С точки зрения *группы* $\mathbb{Z}$ свойства элементов 1 и -1 аналогичны; только когда мы рассматриваем $\mathbb{Z}$ как кольцо, появляется разница между ними). Других порождающих в $\mathbb{Z}$ кроме ±1 нет.

Пример 4.37. Группа $(\mathbb{Z}_n,+)$ (см. Пример 1.40) классов вычетов по модулю n циклическая, поскольку порождается своим элементом [1]. Описать другие порождающие помогает Предложение 4.34 (см. ниже).

Пример 4.38. Группа комплексных корней n-й степени из 1

$$\mu_n:=\{z\in\mathbb{C}\mid z^n=1\}\subset\mathbb{C}^*$$

является циклической, поскольку порождается корнем $\varepsilon:=\exp(\frac{2\pi i}{n})$.

Напомним, что число элементов конечной группы G называется ее *порядком* и обозначается через $|G|$. Порядок конечной циклической группы равен порядку ее порождающего элемента. Поэтому из Предложения 4.34 следует

Предложение 4.39. *Элемент g^k циклической группы $G=\langle g\rangle$ порядка n является порождающим тогда и только тогда, когда $(n,k)=1$.*

Число натуральных чисел среди $1,2,\dots,n$, взаимно простых с n, называется *функцией Эйлера* и обозначается $\phi(n)$.

Задача 4.40. *Докажите, что для простого p $\phi(p)=p-1$. Более общо, $\phi(p^k)=p^k-p^{k-1}$.*

Циклические группы представляют собой простейший класс групп и легко классифицируются с точностью до изоморфизма. (Также нетрудно классифицировать более широкий класс конечно порожденных абелевых групп, но это выходит за рамки нашего рассмотрения).

Теорема 4.41. *Всякая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$. Всякая конечная циклическая группа порядка n изоморфна группе $\mathbb{Z}_n$.*

Доказательство. Если $G=\langle g\rangle$ — бесконечная циклическая группа, то в силу формулы (26) отображение $\varphi\colon\mathbb{Z}\to G,\ k\mapsto g^k$, является гомоморфизмом, который сюръективен, поскольку элемент g является порождающим для G. Если бы φ не был инъективным, то элемент g имел бы конечный порядок, что противоречило бы бесконечности группы G.

Пусть теперь $G=\langle g\rangle$ — конечная циклическая группа порядка n. Рассмотрим отображение

$$\varphi\colon\mathbb{Z}_n\to G,\ \ [k]\mapsto g^k\ \ (k\in\mathbb{Z}).$$

Так как

$$[k]=[l]\ \Leftrightarrow\ n\mid(l-k)\ \Leftrightarrow\ g^k=g^l,$$

отображение φ корректно определено и биективно. Свойство

$$\varphi([k]+[l]) = \varphi([k])\varphi([l])$$

следует из формулы (26). Таким образом, φ — изоморфизм. ■

Таким образом, все циклические группы порядка n изоморфны, и, в частности, группа классов вычетов $\mathbb{Z}_n$ изоморфна группе корней из единицы μ_n. В каждой из них ровно $\phi(n)$ порождающих элементов.

Задача 4.42. *Докажите, что всякая конечная подгруппа мультипликативной группы $\mathbb{C}^*$ поля комплексных чисел является циклической. (Указание: воспользуйтесь тем, что количество корней ненулевого многочлена в поле не превосходит его степени).*

Задача 4.43. *Пусть μ_∞ — множество всех комплексных корней (всевозможных степеней) из 1. Докажите, что μ_∞ является подгруппой группы $\mathbb{C}^*$. Будет ли группа μ_∞ циклической?*

Задача 4.44. *Опишите все бесконечные циклические подгруппы в $\mathbb{C}^*$.*

Опишем теперь подгруппы циклических групп. (В случае бесконечной циклической группы мы это уже сделали в Примере 1.38).

Теорема 4.45. *1) Всякая подгруппа циклической группы сама является циклической.*

2) В циклической группе порядка n порядок любой подгруппы делит n и для любого делителя d числа n существует, и притом только одна подгруппа порядка d.

Доказательство. 1) Пусть $G = \langle g\rangle$ — циклическая группа и H — ее подгруппа, отличная от $\{e\}$. (Единичная подгруппа, очевидно, является циклической). Заметим, что если $g^{-m} \in H$ для какого-либо $m \in \mathbb{N}$, то и $g^m \in H$. Пусть m — наименьшее из натуральных чисел, для которых $g^m \in H$. Докажем, что $H = \langle g^m\rangle$. Пусть $g^k \in H$. Разделим k на m с остатком:

$$k = qm + r, \quad 0 \le r < m.$$

Имеем

$$g^r = g^k(g^m)^{-q} \in H,$$

откуда в силу определения числа m следует, что $r = 0$ и, значит, $g^k = (g^m)^q$.

2) Пусть H — подгруппа циклической группы $G = \langle g\rangle$, $|G| = n$. Выше мы видели, что $H = \langle g^m\rangle$ для некоторого натурального m. Очевидно, что порядок элемента g^m делит $\operatorname{ord}(g) = n$; то же верно и для $|H|$. Пусть $d \mid n$; тогда

$$\langle g^{n/d}\rangle = \{e, g^{n/d}, g^{2n/d}, \dots, g^{(d-1)n/d}\} \tag{27}$$

является подгруппой порядка d в G.

Пусть в группе G есть произвольная подгруппа H' порядка d. Поскольку H' является циклической, она порождается некоторым элементом $g^k \in G$. Докажем, что $\langle g^k\rangle = \langle g^{(k,n)}\rangle$. В самом деле, поскольку $(k,n) \mid k$, то $g^k \in \langle g^{(k,n)}\rangle$ и, значит, $\langle g^k\rangle \subseteq \langle g^{(k,n)}\rangle$. С другой стороны, из Предложения 4.34 следует, что $\operatorname{ord}(g^k) = \operatorname{ord}(g^{(k,n)})$, откуда и следует $\langle g^k\rangle = \langle g^{(k,n)}\rangle$.

Таким образом, $H' = \langle g^{(k,n)}\rangle$. Но $(k,n) \mid n$ и $d = \operatorname{ord}(g^{(k,n)}) = \frac{n}{(k,n)}$ согласно все тому же Предложению 4.34. Значит, $(k,n) = n/d$ и H' совпадает с подгруппой (27). ■

Следствие 4.46. *В циклической группе простого порядка любая неединичная подгруппа совпадает со всей группой.*

Циклическую группу порядка n будем обозначать C_n.

Порядок любого элемента циклической группы C_n делит порядок группы n. Пусть $\Phi(d) \subset C_n$ — множество элементов порядка $d|n$. (Например, $\Phi(1)$ состоит из единственного элемента e, а $\Phi(n)$ — из порождающих элементов для C_n, которых, как мы знаем, $\phi(n)$ штук). Тогда

$$C_n = \coprod_{d|n} \Phi(d).$$

Каждый элемент порядка $d \mid n$ порождает единственную подгруппу $C_d \subset C_n$ порядка d. Как мы знаем, в C_d ровно $\phi(d)$ порождающих элементов, поэтому $|\Phi(d)| = \phi(d)$.

Таким образом, мы доказали такое

Следствие 4.47.

$$n = \sum_{d|n} \phi(d).$$

Задача 4.48. *Докажите, что максимальный порядок образа гомоморфизма $\varphi\colon C_n \to C_m$ равен (m, n). В частности, если $(m, n) = 1$, то существует только один гомоморфизм $\varphi\colon C_n \to C_m$ (он все элементы C_n переводит в нейтральный элемент группы C_m).*

Задача 4.49. *Пусть G — произвольная группа. 1) Постройте биекцию между множеством гомоморфизмов $\mathbb{Z} \to G$ и множеством элементов группы G. 2) Постройте биекцию между множеством гомоморфизмов $C_n \to G$ и множеством таких элементов группы G, порядок которых делит n.*

4.3 Симметрические группы

Совокупность $S(X)$ всех биективных преобразований множества X является группой относительно операции композиции. В самом деле, композиция преобразований ассоциативна; композиция биекций — биекция, обратное преобразование к биекции — биекция, тождественное преобразование (нейтральный элемент относительно композиции) — биекция.

Если множество X конечно (что мы будем предполагать в дальнейшем), то можно считать, что $X = \{1, 2, \ldots, n\}$; в этом случае группа $S(X)$ называется *группой подстановок* или *симметрической группой* степени n и обозначается S_n. Подстановка $\sigma \in S_n$ может быть записана в виде таблицы

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix},$$

в первой строке которой выписаны в каком-то порядке числа $1, 2, \ldots, n$, а во второй строке — их образы, т.е. $j_k = \sigma(i_k)$. Фиксируя расположение чисел в первой строке (например, располагая их в порядке возрастания), мы видим, что число подстановок равно числу перестановок, т.е. $n!$. При этом каждая подстановка может быть записана $n!$ способами.

Произведение подстановок — сложная функция $(\tau\sigma)(i) = \tau(\sigma(i))$, $1 \leq i \leq n$. Приведем пример на умножение подстановок в табличной форме записи:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

(Здесь мы сначала для удобства переписали первую подстановку таким образом, чтобы первая строка в ее записи совпала со второй строкой в записи второй подстановки).

Симметрические группы S_n, $n \in \mathbb{N}$ образуют интересный класс конечных групп, неабелевых при $n > 2$. Достаточно сказать, что любая конечная группа изоморфна подгруппе группы S_n для некоторого

натурального n (теорема Кэли). Мы, однако, познакомимся только с самыми простейшими свойствами симметрических групп.

Назовем *знаком* подстановки $\sigma \in S_n$ и обозначим через $\operatorname{sgn}\sigma$ произведение знаков верхней и нижней перестановки в ее записи

$$\operatorname{sgn}\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \operatorname{sgn}(i_1, i_2, \dots, i_n) \cdot \operatorname{sgn}(j_1, j_2, \dots, j_n)$$

(см. Определение 3.8). Это произведение не зависит от способа записи подстановки σ, поскольку от любого способа записи можно перейти к любому другому последовательными транспозициями столбиков, а при каждой такой транспозиции одновременно меняются знаки верхней и нижней перестановок, так что их произведение сохраняется. Основное свойство знака описывает следующее

Предложение 4.50. *Отображение*

$$\operatorname{sgn}\colon S_n \to C_2 = \{\pm 1\}, \quad \sigma \mapsto \operatorname{sgn}(\sigma)$$

является гомоморфизмом групп.

Доказательство. Перемножая подстановки σ и τ, мы можем считать, что верхняя перестановка в записи σ совпадает с нижней перестановкой в записи τ:

$$\sigma = \begin{pmatrix} j_1 & j_2 & \dots & J_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}, \quad \tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Тогда

$$\sigma\tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

так что

$$\operatorname{sgn}\sigma\tau = \operatorname{sgn}(i_1, i_2, \dots, i_n) \cdot \operatorname{sgn}(k_1, k_2, \dots, k_n) =$$

$$= [\operatorname{sgn}(i_1, i_2, \dots, i_n) \operatorname{sgn}(j_1, j_2, \dots, j_n)] \times [\operatorname{sgn}(j_1, j_2, \dots, j_n) \operatorname{sgn}(k_1, k_2, \dots, k_n)] =$$

$$= \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau. \quad \blacksquare$$

Ядро гомоморфизма sgn называется *знакопеременной группой* и обозначается A_n. Подстановки σ, для которых $\operatorname{sgn}\sigma = 1$ (соответственно $\operatorname{sgn}\sigma = -1$) называются *четными* (соответственно *нечетными*). Таким образом, A_n — это подгруппа четных перестановок в S_n.

Задача 4.51. *Докажите, что в любой подгруппе $G \subseteq S_n$, содержащей нечетную перестановку, количество четных перестановок равно количеству нечетных (в частности, ее порядок четен). (Указание: если $\sigma \in G$ — нечетная перестановка, то умножение на нее задает взаимно-обратные биекции между подмножествами четных и нечетных перестановок в G).*

Задача 4.52. *Докажите, что порядок нечетной перестановки $\sigma \in G$ является четным числом.*

Покажем теперь, как вычисляются порядки элементов группы S_n.

Подстановка $\tau \in S_n$ называется *циклом* длины k и обозначается $(i_1 i_2 \dots i_k)$ (не следует путать это обозначение с похожим обозначением перестановок), если она циклически переставляет $i_1, i_2, \dots, i_k$, то есть $\tau(i_1) = i_2$, $\tau(i_2) = i_3, \dots, \tau(i_k) = i_1$, а все остальные числа оставляет на месте. Очевидно, что порядок цикла длины k равен k.

Заметим, что запись $(i_1 i_2 \dots i_k)$ цикла неоднозначна: с тем же успехом этот же цикл можно было бы обозначить $(i_2 i_3 \dots i_k i_1)$.

Циклы τ_1 и τ_2 называются *независимыми*, если среди фактически переставляемых ими чисел нет общих; в этом случае $\tau_1\tau_2 = \tau_2\tau_1$.

Всякая подстановка σ однозначно (с точностью до порядка сомножителей) разлагается в произведение независимых циклов. В самом деле, рассмотрим последовательность $1, \sigma(1), \sigma^2(1), \ldots$. Поскольку порядок σ конечен, то существует такое натуральное k, что $\sigma^k(1) = 1$. Выберем такое k наименьшим. Тогда среди чисел $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)$ нет совпадающих (если $\sigma^i(1) = \sigma^j(1)$, где $j > i$, то $\sigma^{j-i}(1) = 1$), и мы получили цикл длины k (записав эти числа по порядку в вершины правильного k-угольника, заметим, что применение σ поворачивает его на угол $\frac{2\pi}{k}$). Далее выберем $i \notin \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}$ и рассмотрим цикл, получаемый применением к нему степеней σ. Легко проверить, что он будет независим от первого цикла (если $\sigma^r(i) = \sigma^s(1)$, то $i = \sigma^{s-r}(1)$ в противоречии с предположением). Продолжая в том же духе, получим разложение σ в произведение независимых циклов. Проверку единственности такого разложения оставим читателю. Например,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 4 & 8 & 3 & 2 & 1 \end{pmatrix} = (2637)(158)(4)$$

(последнюю неподвижную четверку можно не писать, поскольку (4) — тождественная подстановка).

Если подстановка σ раскладывается в произведение независимых циклов длин $k_1, k_2, \ldots, k_s$, то

$$\operatorname{ord}\sigma = \text{НОК}\{k_1, k_2, \ldots, k_s\}.$$

Например, порядок приведенной выше подстановки σ равен 12.

Замечание 4.53. Заметим, что разложение подстановки $\sigma \in S_n$ на независимые циклы приводит к разбиению множества $\{1, 2, \ldots, n\}$, отвечающему следующему отношению эквивалентности:

$$i \sim j \;\Leftrightarrow\; \exists\, r \text{ такое, что } j = \sigma^r(i).$$

Также разложение на независимые циклы дает быстрый способ вычислять знак подстановки.

Предложение 4.54. $\operatorname{sgn}(i_1 i_2 \ldots i_k) = (-1)^{k-1}$. *Словами: цикл четной длины — нечетная подстановка и наоборот.*

Доказательство. Легко проверить, что цикл длины k раскладывается в произведение $k-1$-й транспозиций (= цикла длины 2) следующим образом:

$$(i_1 i_2 \ldots i_k) = (i_1 i_k) \ldots (i_1 i_4)(i_1 i_3)(i_1 i_2).$$

Поскольку транспозиция, очевидно, нечетная подстановка, то требуемое следует из Предложения 4.50. ■

Следствие 4.55. *Подстановка четная тогда и только тогда, когда ее разложение на независимые циклы содержит четное количество циклов четной длины.*

Читателю предлагается используя полученный результат предложить новое решение Задачи 4.52.

Задача 4.56. *Чему равен максимальный порядок элемента в S_{10}? Будут ли элементы максимального порядка в S_{10} лежать в подгруппе A_{10}?*

После того, как мы определили разложение перестановки на независимые циклы, трудно удержаться чтобы не применить эту конструкцию к описанию классов сопряженных элементов в группе S_n.

Пусть G — произвольная группа. Рассмотрим на множестве элементов G следующее отношение эквивалентности:

$$g \sim g' \;\Leftrightarrow\; \exists\, h \in G\colon g' = hgh^{-1}.$$

Классы эквивалентности для этого отношения называются *классами сопряженных элементов* группы G (а про элементы, принадлежащие одному классу говорят, что они *сопряжены*).

Например, один из классов сопряженных элементов состоит из нейтрального элемента. Если бы мы изучали действия групп на множествах, то смогли бы легко доказать, что для конечной группы мощность любого класса сопряженных элементов делит порядок группы (впрочем, читатель все равно может попытаться это доказать).

Назовем *цикловым типом* подстановки $\sigma \in S_n$ неупорядоченный набор длин независимых циклов, на которые она раскладывается

Предложение 4.57. *Две подстановки $\sigma, \sigma' \in S_n$ принадлежат к одному классу сопряженных элементов в $S_n \Leftrightarrow$ они имеют одинаковый цикловой тип.*

Доказательство. Легко проверить, что

$$\sigma(i) = j \quad \Leftrightarrow \quad (\tau\sigma\tau^{-1})(\tau(i)) = \tau(j). \tag{28}$$

Поэтому в разложение подстановки σ в произведение независимых циклов входит цикл $(i_1 i_2 \dots i_k)$ тогда и только тогда, когда в аналогичное разложение для $\tau\sigma\tau^{-1}$ входит цикл $(\tau(i_1)\tau(i_2)\dots\tau(i_k))$. Отсюда следует, что если подстановки сопряжены, то они имеют одинаковый цикловой тип.

Обратное следует из той же формулы (28). Точнее, она позволяет находить по двум подстановкам $\sigma, \sigma' \in S_n$, имеющим одинаковый цикловой тип, соответствующие τ. В частности, она показывает, что такие τ в этом случае существуют. ■

Симметрические и знакопеременные группы малых порядков часто встречаются как группы симметрий известных геометрических объектов.

Для решения некоторых приведенных ниже задач будет полезна следующая

Лемма 4.58. Если образ гомоморфизма групп $\varphi\colon G \to S_n$ содержит все транспозиции в S_n, то $\operatorname{Im}\varphi = S_n$, то есть φ сюръективен.

Доказательство. Заметим, что любую подстановку $\sigma \in S_n$ можно представить в виде произведения (зависимых) транспозиций. В самом деле, σ можно разложить в произведение независимых циклов, а каждый цикл можно разложить в произведение транспозиций как в доказательстве Предложения 4.54. Поскольку $\operatorname{Im}\varphi$ является подгруппой в S_n, то вместе с любым конечным набором элементов он содержит и их произведение (в любом порядке). ■

Задача 4.59. *Пусть D_3 — группа симметрий правильного треугольника. Постройте изоморфизм $D_3 \to S_3$. Каким симметриям отвечает подгруппа $A_3 \subset S_3$?*

Задача 4.60. *Постройте изоморфизм $\mathrm{GL}_2(\mathbb{Z}_2) \to S_3$. (Невырожденной матрице сопоставьте перестановку на множестве ненулевых столбцов, предварительно их занумеровав).*

Задача 4.61. *Пусть G — группа симметрий правильного многогранника, содержащая хотя бы одно преобразование, меняющее ориентацию пространства. Тогда G содержит подгруппу G^+ индекса 2, состоящую из поворотов.*

Задача 4.62. *Пусть T — группа симметрий тетраэдра. Постройте изоморфизм $T \to S_4$. Какой подгруппе в T соответствует подгруппа $A_4 \subset S_4$?*

Задача 4.63. *Пусть Q — группа поворотов трехмерного пространства, переводящих куб в себя. Постройте изоморфизм $Q \to S_4$. (Указание: сопоставьте вращению куба перестановку на множестве из четырех диагоналей, соединяющих диаметрально противоположные вершины).*

Задача 4.64. *Пусть D_4 — группа симметрий квадрата (ее порядок равен 8). Используя изоморфизм предыдущей задачи, найдите в S_4 3 подгруппы, изоморфные D_4.*

Задача 4.65. *Постройте сюръективный гомоморфизм $S_4 \to S_3$ и найдите его ядро. (Указание: сопоставьте вращению куба из задачи 4.63 перестановку на множестве прямых, соединяющих середины противоположных граней).*

Ясно, что двойственные правильные многогранники имеют одинаковые группы симметрий, в частности, у октаэдра она такая же как у куба. Для пары икосаэдр-додекаэдр группа поворотов пространства, переводящих их в себя, изоморфна группе A_5.

4.4 Смежные классы

Мы видели, как рассмотрение эквивалентности относительно подгруппы $n\mathbb{Z} \subset \mathbb{Z}$ приводит к определению классов вычетов. Аналогичная конструкция есть для произвольной группы и ее подгруппы $H \subset G$, только в случае неабелевой группы G она приводит, вообще говоря, к двум видам "классов вычетов", которые называются левыми и правыми смежными классами по подгруппе.

Перейдем к точным определениям. Как обычно в случае общих конструкций теории групп будем использовать мультипликативную запись групповой операции.

Итак, пусть G — группа и H — ее подгруппа. Определим отношение эквивалентности $\sim_H$ на множестве элементов G следующим образом:

$$g_1 \sim_H g_2 \;\Leftrightarrow\; g_1^{-1} g_2 \in H, \tag{29}$$

то есть $g_2 = g_1 h$, где $h \in H$. Легко видеть, что это определение обобщает определение сравнимости по модулю n, которое получается в случае $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

Задача 4.66. *Убедитесь, что $\sim_H$ в самом деле является отношением эквивалентности.*

Классы этой эквивалентности называются *левыми смежными классами* группы G по подгруппе H. Ясно, что смежный класс, содержащий элемент g, имеет вид

$$gH := \{gh \mid h \in H\} \subset G$$

(эта запись аналогична записи $k + n\mathbb{Z} \subset \mathbb{Z}$ смежного класса $[k]$ по модулю n). Одним из смежных классов является подмножество $H \subset G$.

Поскольку умножение в группе G не предполагается коммутативным, мы получим, вообще говоря, другое отношение эквивалентности $\sim'_H$, взяв вместо условия (29) аналогичное ему условие

$$g_2 g_1^{-1} \in H. \tag{30}$$

Классы эквивалентности $\sim'_H$ называются *правыми смежными классами* группы G по подгруппе H. Они имеют вид

$$Hg := \{hg \mid h \in H\}.$$

Заметим, что инверсия $g \mapsto g^{-1}$ задает биективное отображение $G \to G$, причем $g_1 \sim g_2 \;\Leftrightarrow\; g^{-1} \sim'_H g_2^{-1}$. Таким образом, инверсия устанавливает биекцию между множествами левых и правых смежных классов.

Пример 4.67. Пусть $G = \mathbb{R}$, $H = \mathbb{Z}$. Тогда для $a, b \in \mathbb{R}$

$$a \sim b \;\Leftrightarrow\; b - a \in \mathbb{Z}$$

и смежные классы — подмножества в $\mathbb{R}$ вида $a + \mathbb{Z} = \{a + n \mid n \in \mathbb{Z}\}$.

Пример 4.68. Пусть $G = \mathbb{C}$, $H = \mathbb{R}$. Тогда для z_1, $z_2 \in \mathbb{C}$

$$z_1 \sim z_2 \;\Leftrightarrow\; z_2 - z_1 \in \mathbb{R}$$

и смежные классы — подмножества в $\mathbb{C}$ вида $z + \mathbb{R}$, то есть прямые, параллельные вещественной оси.

Пример 4.69. Пусть $G = \mathbb{C}^*$, $H = \mathbb{R}^*_{>0}$. Для $z \in \mathbb{C}^*$ смежный класс есть подмножество $z\,\mathbb{R}^*_{>0} = \{zr \mid r \in \mathbb{R}^*_{>0}\}$ в $\mathbb{C}^*$, то есть луч, исходящий из нуля.

Пример 4.70. Смежные классы группы $\mathbb{C}^*$ по подгруппе $\mathrm{U}(1) := \{z \in \mathbb{C}^* \mid |z| = 1\}$ — это концентрические окружности с центром в нуле.

Пример 4.71. Пусть $G = \mathrm{GL_n}(\mathbb{K})$, $H = \mathrm{SL}_n(\mathbb{K}$. Тогда условие (29) равно как и (30) означает, что $\det g_1 = \det g_2$. Поэтому левые смежные классы совпадают в данном случае с правыми смежными классами, хотя группа $\mathrm{GL}_n(\mathbb{K})$ не абелева; каждый из них представляет собой совокупность всех матриц с определителем, равным некоторому ненулевому элементу из $\mathbb{K}$.

Пример 4.72. В группе $G = S_n$ рассмотрим подгруппу H, состоящую из подстановок, оставляющих на месте число n. Подстановки σ_1, $\sigma_2 \in S_n$ принадлежат одному левому смежному классу по H, если $\sigma_1^{-1}\sigma_2(n) = n$, то есть если

$$\sigma_1(n) = \sigma_2(n).$$

Следовательно, имеется n левых смежных классов P_1, $P_2, \ldots, P_n$, где

$$P_k = \{\sigma \in S_n \mid \sigma(n) = k\} \subset S_n.$$

В то же время подстановки $\sigma_1, \sigma_2 \in S_n$ принадлежат одному правому смежному классу, если $\sigma_2\sigma_1^{-1}(n) = n$, то есть если

$$\sigma_1^{-1}(n) = \sigma_2^{-1}(n).$$

Следовательно, имеется n правых смежных классов Q_1, $Q_2, \ldots, Q_n$, где

$$Q_k = \{\sigma \in S_n \mid \sigma(k) = n\} \subset S_n.$$

Мы видим, что при $n > 2$ правые смежные классы отличны от левых, за исключением класса $Q_n = P_n = H$.

Множество левых смежных классов группы G по подгруппе H обозначается через G/H. Число смежных классов группы G по H, если оно конечно, называется *индексом* подгруппы H в G и обозначается через $[G\colon H]$.

Теорема 4.73. *(теорема Лагранжа) Пусть G — конечная группа и H — любая ее подгруппа, тогда*

$$|G| = [G\colon H]|H|. \tag{31}$$

Доказательство. Все смежные классы gH содержат одно и то же число элементов, равное $|H|$. Поскольку они образуют разбиение группы G (как классы эквивалентности), порядок группы G равен произведению их числа на $|H|$. ■

Пример 4.74. В примере 4.72 мы видели, что $[S_n\colon H] = n$, где H — подгруппа в S_n, состоящая из подстановок, которые оставляют n на месте. Ясно, что $H \cong S_{n-1}$. Поэтому формула (31) позволяет вычислить порядок группы S_n индуктивно.

Следствие 4.75. *Порядок любой подгруппы конечной группы делит порядок группы.*

Мы уже видели это в случае циклических групп (Теорема 4.45).

Следствие 4.76. *Порядок любого элемента конечной группы делит порядок группы.*

Доказательство. Порядок элемента равен порядку порождаемой им циклической подгруппы. ■

Следствие 4.77. *Всякая конечная группа простого порядка является циклической.*

Доказательство. Возьмем произвольный элемент $g \neq e$ группы G, $|G| = p$. Тогда по Следствию 4.76 $\operatorname{ord} g$ делит p и $\neq 1$; значит, такой элемент имеет порядок p и является порождающим для G. ■

Задача 4.78. *Пусть p — простое число. Найдите в симметрической группе S_p количество подгрупп порядка p.*

Следствие 4.79. *Если $|G| = n$, то $g^n = e$ для любого $g \in G$.*

Доказательство. Пусть $\operatorname{ord} g = m$. Тогда по Следствию 4.76 $m \mid n$, следовательно, $g^n = e$. ■

Следствие 4.80. *(теорема Эйлера) Для любого $a \in \mathbb{Z}$, взаимно простого с натуральным $n \in \mathbb{N}$, имеет место сравнение*

$$a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

Доказательство. Рассмотрим кольцо $\mathbb{Z}_n$ классов вычетов по модулю n. Порядок его мультипликативной группы $\mathbb{Z}_n^*$ равен количеству чисел в ряде $1, 2, \ldots, n$, взаимно простых с n, то есть $\phi(n)$. По условию $[a] \in \mathbb{Z}_n^*$ и тогда по предыдущему Следствию $[a]^{\phi(n)} = [1]$ в кольце $\mathbb{Z}_n$. Последнее равенство равносильно $[a^{\phi(n)} - 1] = [0]$, что, в свою очередь равносильно доказываемому сравнению. ■

Частным случаем предыдущего Следствия является *малая теорема Ферма*, которая утверждает, что если $a \in \mathbb{Z}$ не делится на простое p, то

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Задача 4.81. *Пусть $H := S_k \times S_{n-k} \subset S_n =: G$ — подгруппа группы подстановок (она состоит в точности из тех подстановок, которые подмножество $\{1, 2, \ldots, k\} \subset \{1, 2, \ldots, n\}$ переводят в себя). Постройте биекцию между множествами левых смежных классов G по H и k-элементных подмножеств в $\{1, 2, \ldots, n\}$.*

4.5 Факторгруппа и теорема о гомоморфизме

Пусть $\varphi\colon G \to H$ — гомоморфизм групп и $K := \ker \varphi$ — его ядро. Любая ли подгруппа в G может быть ядром гомоморфизма? Оказывается, что если G — неабелева группа, то, вообще говоря, нет. Попробуем разобраться в этом вопросе.

Пусть $g_1 \sim g_2 \Leftrightarrow \varphi(g_1) = \varphi(g_2)$ — отношение эквивалентности, связанное с отображением φ (см. абзац после Примера 1.22). Имеем:

$$\varphi(g_1) = \varphi(g_2) \Leftrightarrow \varphi(g_2 g_1^{-1}) = e \Leftrightarrow g_2 g_1^{-1} \in K \Leftrightarrow g_2 \in K g_1.$$

С другой стороны,

$$\varphi(g_1) = \varphi(g_2) \Leftrightarrow \varphi(g_1^{-1} g_2) = e \Leftrightarrow g_1^{-1} g_2 \in K \Leftrightarrow g_2 \in g_1 K.$$

Это означает, что если $K \subset G$ — ядро гомоморфизма $\varphi\colon G \to H$, то разбиения G на левые и правые смежные классы по K совпадают: $\forall\, g \in G\ gK = Kg$.

Определение 4.82. Подгруппа $K \subset G$ называется *нормальной* (обозначение: $K \lhd G$), если $\forall\, g \in G\ gK = Kg$. Последнее эквивалентно также условию $\forall\, g \in G\ K = gKg^{-1}$.

Тем самым мы доказали такое

Предложение 4.83. *Ядро гомоморфизма групп $\varphi\colon G \to H$ — нормальная подгруппа в G.*

В абелевой группе любая подгруппа является нормальной. Пример не нормальной подгруппы в S_n был приведен в Примере 4.72.

Предложение 4.84. *В введенных выше обозначениях пусть $h \in \operatorname{Im}\varphi$. Тогда $\varphi^{-1}(h) = gK$ для произвольного $g \in G$ такого, что $\varphi(g) = h$.*

Доказательство.

$$g' \in \varphi^{-1}(h) \Leftrightarrow \varphi(g') = h = \varphi(g) \Leftrightarrow g' \in gK. \quad \blacksquare$$

То есть полные прообразы элементов из образа при гомоморфизме групп являются смежными классами по ядру. В частности, каждый такой прообраз равномощен множеству элементов K. Среди таких прообразов подгруппой в G является только прообраз единичного элемента — это K.

Покажем, что наоборот, любая нормальная подгруппа в G является ядром некоторого гомоморфизма $G \to H$.

Предложение 4.85. *Разбиение группы на левые смежные классы по подгруппе K согласовано с операцией в G (см. Определение 1.39) тогда и только тогда, когда $K \lhd G$.*

Доказательство. Поскольку в нашем случае $g \sim g' \Leftrightarrow g' = gk$ для $k \in K$, нужно доказать, что

$$\{g_1 g_2 \sim g_1 k_1 g_2 k_2 \ \ \forall\, g_1,\, g_2 \in G,\ \forall\, k_1,\, k_2 \in K\} \Leftrightarrow K \lhd G.$$

Имеем

$$g_1 g_2 \sim g_1 k_1 g_2 k_2 \Leftrightarrow (g_1 g_2)^{-1} g_1 k_1 g_2 k_2 \in K \Leftrightarrow g_2^{-1} k_1 g_2 k_2 \in K \Leftrightarrow$$
$$\Leftrightarrow g_2^{-1} k_1 g_2 \in K \Leftrightarrow K = gKg^{-1}\ \forall g \in G \Leftrightarrow K \lhd G. \quad \blacksquare$$

Следствие 4.86. *Если $K \lhd G$, то*

$$g_1 K \cdot g_2 K = (g_1 g_2) K$$

задает корректно определенную операцию на множестве смежных классов G по K.

Доказательство. См. абзац после Определения 1.39. $\blacksquare$

Легко видеть, что операция на множестве левых смежных классов, определённая в предыдущем Следствии, задает на этом множестве структуру группы (обратным к gK является $g^{-1}K$, нейтральным элементом eK; ассоциативность следует из ассоциативности операции в G). Эта группа называется *факторгруппой* группы G по подгруппе K и обозначается G/K (как и множество левых смежных классов, но это обычно не приводит к путанице). Данная конструкция обобщает конструкцию группы классов вычетов $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ на случай произвольной группы G и её нормальной подгруппы K.

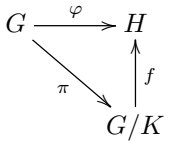
Из определения операции в факторгруппе непосредственно следует, что факторотображение

$$\pi\colon G \to G/K, \quad g \mapsto gK$$

является гомоморфизмом групп. Он называется *каноническим гомоморфизмом* на факторгруппу.

Следующая теорема показывает, что, по-существу, других сюръективных гомоморфизмов групп кроме канонических, нет.

Теорема 4.87. *(Основная теорема о гомоморфизмах групп) Пусть $\varphi\colon G \to H$ — сюръективный гомоморфизм групп с ядром K. Тогда $H \cong G/K$. Более точно, отображение $f\colon G/K \to H$ заданное формулой $f(gK) = h$, где $h = \varphi(g)$, задаёт изоморфизм групп $G/K \to H$ такой, что диаграмма*



коммутативна.

Доказательство. 1. Проверим, что отображение f корректно определено. В самом деле, $g'K = gK \Leftrightarrow \varphi(g) = \varphi(g')$.

2. Проверим, что f является гомоморфизмом групп. В самом деле, поскольку если $\varphi(g_i) = h_i$, $i = 1, 2$, то $\varphi(g_1 g_2) = h_1 h_2$, и мы имеем

$$f(g_1K \cdot g_2K) = f((g_1g_2)K) = h_1h_2 = f(g_1K)f(g_2K).$$

3. Из определения f очевидно, что f сюръективен. Проверим, что f инъективен: если $f(gK) = e$, то $\varphi(g) = e$, то есть $g \in \ker\varphi = K$, откуда $gK = eK$. Значит, f — изоморфизм.

4. Наконец, проверим коммутативность диаграммы. Имеем

$$f(\pi(g)) = f(gK) = \varphi(g). \quad \blacksquare$$

Практическое значение доказанной теоремы заключается, в частности, в том, что она позволяет находить, какой группе изоморфна факторгруппа. Всё что для этого нужно — найти сюръективный гомоморфизм с подходящим ядром (см. примеры ниже).

Заметим, что если G — конечная группа, то в предыдущих обозначениях $|G| = |H||K|$.

Заметим также, что для произвольного гомоморфизма $\varphi\colon G \to H$ его ограничение $\varphi'\colon G \to \operatorname{Im}\varphi$ на образ сюръективно, поэтому если в предыдущей теореме заменить H на $\operatorname{Im}\varphi$, то она будет верна для произвольного (не обязательно сюръективного) гомоморфизма φ.

Пример 4.88. Поскольку существует сюръективный гомоморфизм $\mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto [k]$ с ядром $n\mathbb{Z} \subset \mathbb{Z}$, то $\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}_n$.

Пример 4.89. Аналогично, сюръективный гомоморфизм $\mathbb{R} \to \mathrm{U}(1)$ с ядром $\mathbb{Z}$ из Примера 4.14 показывает, что $\mathbb{R}/\mathbb{Z} \cong \mathrm{U}(1)$.

Пример 4.90. $S_n/A_n \cong \{\pm 1\}$ (см. Предложение 4.50).

Пример 4.91. Пусть $T_n(\mathbb{K})$, $UT_n(\mathbb{K})$, $D_n(\mathbb{K})$ — группы невырожденных верхних треугольных матриц, невырожденных верхних унитреугольных матриц (т.е. верхних треугольных с единицами на главной диагонали) и невырожденных диагональных матриц соответственно над полем $\mathbb{K}$. Тогда читатель легко проверит, что сопоставление верхней треугольной матрице диагональной матрицы, диагональные элементы которой совпадают с соответствующими элементами треугольной матрицы, задает гомоморфизм групп $T_n(\mathbb{K}) \to D_n(\mathbb{K})$. Его ядром является подгруппа $UT_n(\mathbb{K})$. Значит, она нормальна в $T_n(\mathbb{K})$ и $T_n(\mathbb{K})/UT_n(\mathbb{K}) \cong D_n(\mathbb{K})$.

Вопрос читателю: будет ли подгруппа $D_n(\mathbb{K})$ нормальна в $T_n(\mathbb{K})$?

Пример 4.92. Пусть $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ — гомоморфизм, определенный в Примере 4.15. Его ядром является подгруппа в $\mathrm{GL}_n(\mathbb{K})$, состоящая из матриц с определителем 1. Она называется *специальной линейной группой* и обозначается $\mathrm{SL}_n(\mathbb{K})$. Имеем $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \cong \mathbb{K}^*$.

Пример 4.93. Читатель, решивший Задачу 4.65, построил сюръективный гомоморфизм $S_4 \to S_3$. Его ядро состоит из перестановок $\{e, (12)(34), (13)(24), (14)(23)\}$ и имеет классическое обозначение V_4. Таким образом, $S_4/V_4 \cong S_3$.

Вообще, нормальные подгруппы в S_n можно искать с помощью описания классов сопряженных элементов в S_n, данном в Предложении 4.57.

Предложение 4.94. *Если $N \lhd G$, то N либо целиком содержит класс сопряженных элементов в G, либо не пересекается с ним. (Иными словами, N является объединением некоторого множества классов сопряженных элементов в G). Наоборот, если объединение некоторых классов сопряженных элементов является подгруппой, то эта подгруппа нормальна.*

Доказательство. Если $N \lhd G$, и $n \in N$, то $gng^{-1} \in N$ $\forall g \in G$ или, эквивалентно, $[n] \subseteq N$, где $[n] := \{gng^{-1} \mid g \in G\}$ есть класс сопряженности n. Отсюда

$$N = \bigcup_{n \in N} [n]. \tag{32}$$

Обратно, если N — подгруппа в G, удовлетворяющая (32), то для любых $n \in N$ и $g \in G$ $gng^{-1} \in N$, и значит $N \lhd G$. ■

Найдем теперь все нормальные подгруппы в S_4. Пусть $N \lhd S_4$; тогда по предыдущему N является объединением каких-то классов сопряженных элементов в S_4. Перечислим эти классы, указывая по представителю:

$$1)\ e,\quad 2)\ (12),\quad 3)\ (12(34),\quad 4)\ (123),\quad 5)\ (1234).$$

Мощности этих классов соответственно 1, 6, 3, 8, 6. Таким образом, $|N| = 1 + 6\alpha + 3\beta + 8\gamma + 6\delta$, где α, β, γ, $\delta \in \{0, 1\}$. Кроме того, по теореме Лагранжа, $|N| \mid |S_4| = 24$. Легко проверить, что этому условию удовлетворяют наборы $(\alpha, \beta, \gamma, \delta) = \{(0, 0, 0, 0), (0, 1, 0, 0), (0, 1, 1, 0), (1, 1, 1, 1)\}$, причем первый и последний отвечают тривиальной подгруппе и всей группе. Третий набор приводит к знакопеременной группе, поскольку входящие в него классы состоят в точности из четных перестановок. Второй набор соответствует V_4 из предыдущей задачи: легко проверяется, что $\{e, (12)(34), (13)(24), (14)(23)\}$ — подгруппа в S_4, а значит она нормальна.

Впрочем, набор нормальных подгрупп в группах S_n весьма беден: согласно классическому результату Э. Галуа, при $n \geq 5$ в S_n помимо тривиальных подгрупп (равных $\{e\}$ или самой группе) нормальной является только подгруппа A_n.

Заметим, что есть нетривиальные ($\neq \{e\}$) группы, называемые *простыми*, у которых нет нетривиальных нормальных подгрупп. Любой гомоморфизм из такой группы является либо тривиальным (все переводит в e), либо вложением (т.е. инъективным). Среди конечных абелевых групп это в точности группы простого порядка (см. Следствие 4.75), они вообще не содержат нетривиальных подгрупп. Существует также бесконечно много неабелевых простых групп (например, группы A_n при $n \geq 5$ простые, что тесно связано с неразрешимостью в радикалах алгебраических уравнений степени ≥ 5). Многие специалисты в теории конечных групп считают, что к настоящему моменту получена полная классификация простых конечных групп.

Для полноты картины вернемся к вопросу об описании отношений эквивалентности на множестве элементов группы, согласованных с групповой операцией. Выше мы видели, что отношение сравнимости по модулю нормальной подгруппы согласовано с операцией в группе.

Предложение 4.95. *Пусть G — произвольная группа. Любое отношение эквивалентности, согласованное с операцией в G является отношением сравнимости по модулю некоторой нормальной подгруппы $K \lhd G$.*

Доказательство. Пусть $\sim$ — отношение эквивалентности на множестве G, согласованное с групповой операцией. Пусть $K \subset G$ — класс эквивалентности $e \in G$. Покажем, что K — нормальная подгруппа в G и $\sim$ совпадает с отношением сравнимости по модулю K.

1. Докажем, что K — подгруппа в G. Из согласованности отношения эквивалентности с групповой операцией

$$g_1 \sim e,\ g_2 \sim e \ \Rightarrow\ g_1 g_2 \sim ee = e,$$

поэтому K замкнуто относительно операции. Если $g \sim e$, $e = g^{-1}g \sim g^{-1}e = g^{-1}$, а значит из $g \in K$ следует $g^{-1} \in K$. Кроме того, $e \in K$. Значит, K — подгруппа в G.

2. Для любого $k \in K$ и $g \in G$ имеем $gkg^{-1} \sim geg^{-1} = e$, откуда $gKg^{-1} = K\ \forall\, g \in G$, поэтому $K \lhd G$.

3. Наконец, то, что $\sim$ совпадает с отношением сравнимости по модулю K, следует из цепочки эквивалентностей

$$g' \sim g \ \Leftrightarrow\ g^{-1}g' \sim e \ \Leftrightarrow\ g^{-1}g' \in K \ \Leftrightarrow\ g' \in gK. \quad \blacksquare$$

4.6 Прямые произведения (прямые суммы) групп

Познакомимся вкратце с простейшим способом конструирования новых групп из уже имеющихся, называемым *прямым произведением групп.*

Определение 4.96. Пусть $(G, \cdot)$ и $(H, *)$ — две группы. Их *прямым произведением* называется множество $G \times H$ с покомпонентной операцией

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \cdot g_2, h_1 * h_2).$$

Как обычно, в дальнейшем мы будем опускать явные обозначения операций. Ясно, что $G \times H$ является группой: нейтральным элементом является $e_{G\times H} = (e_G, e_H)$; обратным $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Предложение 4.97. *Если элементы $g \in G$ и $h \in H$ имеют конечные порядки, то* $\operatorname{ord}(g, h) = \operatorname{НОК}(\operatorname{ord}(g), \operatorname{ord}(h))$.

Доказательство. Упражнение. $\blacksquare$

Зададимся теперь вопросом: как понять, что данная группа P изоморфна прямому произведению двух каких-то групп G, $H \neq \{e\}$? Ведь если это так, то изучение P может быть сведено к изучению "более элементарных" групп G и H.

Заметим, что существуют инъективные гомоморфизмы

$$i_G \colon G \to G \times H,\ \ i_G(g) = (g, e_H)$$

и

$$i_H \colon H \to G \times H,\ \ i_H(h) = (e_G, h).$$

Пусть $G' := \operatorname{Im} i_G,\ H' := \operatorname{Im} i_H$. Тогда G' и H' — подгруппы группы $P := G \times H$, изоморфные G и H соответственно и обладающие следующими легко проверяемыми свойствами:

1) $\forall\, p \in P\ \ \exists\, g' \in G',\ h' \in H'$ такие, что $p = g'h'$;

2) $G' \cap H' = e_P$;

3) $g'h' = h'g'\ \ \forall\, g' \in G',\ h' \in H'$.

Заметим, что из свойств 1) и 2) следует, что для любого $p \in P$ представление в виде произведения $g'h'$, где $g' \in G'$, $h' \in H'$, единственно. (В самом деле, если $g'h' = gh$, то $g^{-1}g' = hh'^{-1} \in G' \cap H' = e$)

Пусть теперь нам дана группа P, в которой есть подгруппы G, H, удовлетворяющие приведённым выше условиям 1), 2), 3). Покажем, что тогда $P \cong G \times H$.

Зададим отображение $\varphi\colon G \times H \to P$ формулой $\varphi(g, h) = gh$ (где справа стоит произведение элементов g, h в группе P). Проверим, что φ — гомоморфизм:

$$\varphi((g_1, h_1)(g_2, h_2)) = \varphi(g_1g_2, h_1h_2) = g_1g_2h_1h_2 = g_1h_1g_2h_2 = \varphi(g_1, h_1)\varphi(g_2, h_2)$$

(где мы воспользовались условием 3)). Инъективность φ теперь следует из условия 2), в то время как сюръективность — из условия 1).

Тем самым мы доказали следующее

Предложение 4.98. *Группа P изоморфна прямому произведению своих подгрупп G' и H' тогда и только тогда, когда выполнены условия 1) — 3).*

Пример 4.99. Из существования и единственности показательной записи ненулевого комплексного числа следует, что группа $\mathbb{C}^*$ является прямым произведением групп $\mathrm{U}(1)$ и $\mathbb{R}^*_{>0}$.

Пример 4.100. В группе S_3 есть подгруппы $\langle(12)\rangle$ и $\langle(123)\rangle$ порядков 2 и 3 соответственно. Их пересечение, очевидно, тривиально, но S_3 не представляется в виде их прямого произведения, поскольку иначе она была бы абелева. Какое из условий предыдущего Предложения при этом нарушается?

Пример 4.101. Группа $T_n(\mathbb{K})$ не является прямым произведением своих подгрупп $UT_n(\mathbb{K})$ и $D_n(\mathbb{K})$ (см. Пример 4.91).

Если A, B — аддитивные абелевы группы, то их прямое произведение называется также *прямой суммой* и обозначается $A \oplus B$.

Задача 4.102. *Докажите, что группа $\mathbb{Z}$ не может быть разложена в прямую сумму двух ненулевых подгрупп.*

Задача 4.103. *Докажите, что группа $\mathbb{Z}$ не изоморфна $\mathbb{Z} \oplus \mathbb{Z}$.*

Не следует думать, что все подгруппы в $G \times H$ имеют вид $K \times L$, где $K \subset G$, $L \subset H$.

Задача 4.104. *Сколько подгрупп в группе $\mathbb{Z}_p \oplus \mathbb{Z}_p$, где p — простое число?*

Представляются ли какие-либо циклические группы нетривиальным образом в виде прямой суммы? Для бесконечной циклической группы $\mathbb{Z}$ выше мы получили отрицательный ответ.

Предложение 4.105. *Группа $\mathbb{Z}_k \oplus \mathbb{Z}_l$ является циклической тогда и только тогда, когда $(k, l) = 1$.*

Доказательство. Пусть $(k, l) = 1$. Тогда по Предложению 4.97 элемент $([1]_k, [1]_l) \in \mathbb{Z}_k \oplus \mathbb{Z}_l$ имеет порядок kl, равный порядку прямой суммы, а значит прямая сумма — циклическая группа.

Другой способ доказательства: обозначим для упрощения обозначений $n := kl$ и рассмотрим отображение

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_k \oplus \mathbb{Z}_l, \quad \varphi([a]_n) = ([a]_k, [a]_l).$$

Во-первых, φ корректно определено, поскольку если $n \mid (a' - a)$, то $k \mid (a' - a)$ и $l \mid (a' - a)$. Во-вторых, φ является гомоморфизмом:

$$\varphi([a]_n + [b]_n) = \varphi([a + b]_n) = ([a + b]_k, [a + b]_l) = ([a]_k + [b]_k, [a]_l + [b]_l) =$$

$$= ([a]_k, [a]_l) + ([b]_k, [b]_l) = \varphi([a]_n) + \varphi([b]_n).$$

В-третьих, гомоморфизм φ инъективен: если $[a]_n \in \ker\varphi$, то $k \mid a$ и $l \mid a$, а поскольку $(k,l) = 1$, то $kl = n \mid a$. Тогда, поскольку порядки групп $\mathbb{Z}_n$ и $\mathbb{Z}_k \oplus \mathbb{Z}_l$ равны, то φ является изоморфизмом, а значит $\mathbb{Z}_k \oplus \mathbb{Z}_l$ — циклическая группа.

Пусть теперь $(k,l) = d > 1$. Тогда НОК $(k,l) = \frac{kl}{d}$. Мы знаем, что порядок d_1 элемента из $\mathbb{Z}_k$ является делителем k, а порядок d_2 элемента из $\mathbb{Z}_l$ является делителем l, поэтому порядок элемента из $\mathbb{Z}_k \oplus \mathbb{Z}_l$, равный НОК (d_1, d_2), является делителем $\frac{kl}{d} < kl$. То есть в группе $\mathbb{Z}_k \oplus \mathbb{Z}_l$ нет элементов порядка kl, а значит она не является циклической. ■

Понятия прямого произведения и прямой суммы можно распространить на любое конечное число слагаемых. Сделаем это для прямой суммы.

Пусть A — аддитивная абелева группа. Она раскладывается в прямую сумму своих подгрупп $A_1, A_2, \ldots, A_s$, если любой ее элемент $a \in A$ однозначно представляется в виде $a_1 + a_2 + \ldots + a_s$, где $a_i \in A_i$, $i = 1, \ldots, s$. При этом пишут $A = A_1 \oplus A_2 \oplus \ldots \oplus A_s$. Такая группа изоморфна группе, элементами которой являются последовательности $(a_1, a_2, \ldots, a_s)$, $a_i \in A_i$, с покомпонентной операцией сложения. Если группы $A_1, A_2, \ldots, A_s$ конечны, то $|A| = |A_1||A_2|\ldots|A_s|$.

Предложение 4.106. *Пусть $n = n_1 n_2 \ldots n_s$, где натуральные числа $n_1, n_2, \ldots, n_s$ попарно взаимно просты. Тогда отображение*

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_s}, \quad [a]_n \mapsto ([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_s})$$

является изоморфизмом групп.

Доказательство. Упражнение. ■

Следствие 4.107. *Если $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ — разложение натурального n на различные простые множители, то*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

Например,

$$\mathbb{Z}_{60} \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{20} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5.$$

В то же время, например, $\mathbb{Z}_{60} \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

Примарной циклической группой называется циклическая группа, порядок которой является степенью простого числа.

Задача 4.108. *Докажите, что примарная циклическая группа не может быть разложена в прямую сумму двух ненулевых подгрупп.*

В заключении параграфа сформулируем чрезвычайно важную и полезную для приложений теорему, описывающую все конечные абелевы группы.

Теорема 4.109. *Любая конечная абелева группа раскладывается в прямую сумму примарных циклических подгрупп, причем набор порядков этих подгрупп определен однозначно.*

Например, с точностью до изоморфизма, существует ровно 3 абелевы группы порядка 24, это:

$$\mathbb{Z}_8 \oplus \mathbb{Z}_3, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3;$$

первая из них является циклической.

Существуют и другие помимо прямой суммы способы построения новых групп из уже имеющихся, например, конструкция полупрямого произведения, с которой мы встретимся при изучении группы аффинных преобразований. (Другие примеры полупрямых произведений дают примеры 4.100 и 4.101).

4.7 Несколько слов о топологических группах

В различных приложениях часто требуются группы с дополнительной структурой, такие как топологические группы или группы Ли. Попробуем коротко объяснить что это такое, отсылая читателя за подробностями к дополнительной литературе. Для этого вернемся к исходным определениям.

Напомним, что группа — множество с заданной на нем бинарной операцией, удовлетворяющей определенным аксиомам. На множествах помимо алгебраических операций могут быть заданы структуры других типов — например, мы встречались с отношениями эквивалентности. Если на одном и том же множестве заданы две такие структуры — скажем, бинарная операция и отношение эквивалентности, то возникает вопрос, что означает условие их согласования. Для бинарной операции и отношения эквивалентности мы знаем ответ.

Допустим, что на множестве G заданы структуры группы и топологического пространства. Что означает, что эти две структуры согласованы? Поскольку задание структуры группы эквивалентно заданию двух отображений

$$G \times G \to G, \;\; (g_1, g_2) \mapsto g_1 g_2 \quad \text{и} \quad G \to G, \;\; g \mapsto g^{-1} \tag{33}$$

с требуемыми свойствами, а отображения, согласованные с топологией — в точности непрерывные отображения, то естественным требованием согласования двух этих структур является условие непрерывности данных отображений (при этом, естественно, на множестве $G \times G$ рассматривается топология произведения). Это и есть определение топологической группы.

Определение 4.110. *Топологической группой* называется группа G, одновременно являющаяся топологическим пространством, такая что операции умножения и взятия обратного (33) являются непрерывными.

Соответствующим образом модифицируется и понятие гомоморфизма между топологическими группами, а именно рассматриваются только такие гомоморфизмы $\varphi\colon G \to H$, которые одновременно являются непрерывными отображениями.

Пример 4.111. Любая группа является топологической, если задать на ней дискретную топологию.

Пример 4.112. Пусть на $\mathbb{R}$ рассматривается стандартная топология. Тогда $(\mathbb{R}, +)$ — топологическая группа. То же, конечно, верно для $(\mathbb{C}, +)$.

Пример 4.113. Группу $\mathrm{U}(1) = \{z \in \mathbb{C} \mid |z| = 1\}$ рассмотрим с топологией, индуцированной вложением $\mathrm{U}(1) \subset \mathbb{C}$ (на $\mathbb{C}$ топология стандартная). Тогда $\mathrm{U}(1)$ — топологическая группа. Более того, ранее рассмотренный гомоморфизм $\varphi\colon \mathbb{R} \to \mathrm{U}(1)$, $\varphi(x) = e^{2\pi i x}$, является гомоморфизмом топологических групп.

Пример 4.114. Группа $\mathrm{GL}_n(\mathbb{R})$ (или $\mathrm{GL}_n(\mathbb{C})$) является топологической группой относительно топологии, индуцированной вложением $\mathrm{GL}_n(\mathbb{R}) \subset \mathrm{Mat}_n(\mathbb{R}) = \mathbb{R}^{n^2}$. Это следует из того, что матричные элементы произведения матриц $C = AB$ (соответственно обратной матрицы A^{-1}) непрерывно зависят от матричных элементов сомножителей A и B (соответственно от матричных элементов матрицы A). По тем же причинам топологическими группами будут также $\mathrm{O}(n)$, $\mathrm{SO}(n)$ (соотв. $\mathrm{U}(n)$, $\mathrm{SU}(n)$).

При этом, например, отображение $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ $(= \mathrm{GL}_1(\mathbb{R}))$ является гомоморфизмом топологических групп.

Любопытно, что структуру топологической группы можно ввести не на любом топологическом пространстве. Например, этого нельзя сделать на двумерной (более общо, четномерной) сфере. Это связано с тем, что ее эйлерова характеристика отлична от нуля. В то же время на одномерной сфере (как показывает пример группы $\mathrm{U}(1)$) и на трехмерной сфере (группа $\mathrm{SU}(2)$) структуру топологической группы (и даже группы Ли) ввести можно.

Определение группы Ли похоже на определение топологической группы, только вместо структуры топологического пространства на G рассматривается структура гладкого многообразия, и условие ее согласования со структурой группы заключается в том, что отображения, задающие умножение в группе и взятие обратного, должны быть гладкими. Группы Ли допускают в некотором смысле линеаризацию, называемую алгебрами Ли, что сильно облегчает их изучение по сравнению с топологическими группами. Например, известный нам пример алгебры Ли — трехмерное ориентированное евклидово пространство с операцией векторного произведения — является алгеброй Ли групп $\mathrm{SO}(3)$ и $\mathrm{SU}(2)$[26]. Группы из приведенных выше примеров имеют структуру групп Ли. Например, $\mathrm{GL}_n(\mathbb{R})$, будучи открытым подмножеством в пространстве $\mathbb{R}^{n^2}$, является гладким многообразием. Важный для физики пример группы Ли — группа Лоренца.

Как правило, в приложениях группы (в частности, группы Ли) реализуются обратимыми линейными преобразованиями, которые действуют на каком-то линейном пространстве (скажем, на пространстве состояний квантовой системы).

Определение 4.115. Вещественным (комплексным) *линейным представлением* группы G называется пара (ρ, V), где V — линейное пространство над полем $\mathbb{R}$ (соотв. $\mathbb{C}$), а $\rho\colon G \to \mathrm{GL}_n(V)$ — гомоморфизм групп (в случае топологической группы G непрерывный).

Читатель может построить вещественное линейное представление группы симметрий треугольника D_3 в двумерном евклидовом пространстве, записав симметрии треугольника матрицами относительно фиксированного базиса.

С началами теории представлений можно познакомиться по книге [6] или более полно по [11] и [20].

5 Кольца, поля

5.1 Обратимые элементы и делители нуля

В этом параграфе R — *ассоциативное кольцо с единицей.*

Элемент $a \in R$ называется *обратимым*, если существует $a^{-1} \in R$ такой, что $aa^{-1} = 1 = a^{-1}a$.

Предложение 5.1. *Пусть R — ассоциативное кольцо с единицей. Тогда множество обратимых (по умножению) элементов R^* в R образует группу по умножению.*

Доказательство. Упражнение. ■

Пример 5.2. Если $R = \mathrm{Mat}_n(\mathbb{K})$, то группа R^* обратимых матриц обозначается $\mathrm{GL}_n(\mathbb{R})$.

Пример 5.3. $\mathbb{K}[x]^* = \mathbb{K}^*$ (этот факт читатель может сейчас доказать в качестве упражнения; мы докажем его в следующем параграфе).

Пример 5.4. $\mathbb{Z}^* = \{\pm 1\}$.

Пример 5.5. Элемент $[a] \in \mathbb{Z}_n$ обратим тогда и только тогда, когда $(a, n) = 1$ (см. Предложение 5.41). Поэтому группа $\mathbb{Z}_n^*$ имеет порядок $\phi(n)$. Группа $\mathbb{Z}_n^*$ может быть как циклической (например, при $n = p^k$, $p \neq 2$), так и не циклической (например, при $n = 2^k$, $k \geq 3$).

Элемент $a \in R$, $a \neq 0$ называется *левым делителем нуля*, если существует $b \in R$, $b \neq 0$ такой, что $ab = 0$. Аналогично определяются правые делители нуля. Ясно, что в коммутативном кольце нет разницы между левыми и правыми делителями нуля.

[26] Хотя эти группы не изоморфны, они "локально изоморфны" и поэтому имеют изоморфные линеаризации.

Например, кольцо $C[0,1]$ непрерывных функций на отрезке $[0,1]$ имеет делители нуля. Пусть ненулевая функция $f\colon [0,1] \to \mathbb{R}$ равна нулю на $[1/3,1] \subset [0,1]$, другая ненулевая функция $g\colon [0,1] \to \mathbb{R}$ равна нулю на $[0,2/3]$; тогда, очевидно, $fg = 0$.

Если $a \in R$ не является левым делителем нуля, то из $ab = ac$ следует $b = c$. (В самом деле, перенося все в левую часть получаем $a(b-c) = 0$). Аналогично на элементы, не являющиеся правыми делителями нуля, можно сокращать справа.

Предложение 5.6. *Обратимый элемент не может быть делителем нуля.*

Доказательство. Пусть a обратим, тогда если $ab = 0 \;\Rightarrow\; a^{-1}ab = b = 0$. ■

Обратное неверно: например, в кольце $\mathbb{Z}$ нет делителей нуля, а обратимы только ± 1.

Поскольку в поле по определению любой ненулевой элемент обратим, в поле нет делителей нуля.

Среди делителей нуля встречаются *нильпотенты* — это такие элементы $a \in R$, $a \neq 0$, для которых существует натуральное n такое, что $a^n = 0$. Например, в кольце матриц порядка n нильпотентными являются верхние нильтреугольные матрицы — верхнетреугольные матрицы, у которых на главной диагонали стоят нули.

Задача 5.7. *Найдите обратимые элементы, делители нуля и нильпотентные элементы в кольцах: а) $\mathbb{Z}_{p^k}$; b) $\mathbb{Z}_n$; c) в кольце $\mathrm{T}_n(\mathbb{K})$ верхних треугольных матриц порядка n над полем $\mathbb{K}$.*

5.2 Кольцо многочленов над полем

Пусть $\mathbb{K}$ — произвольное поле. Рассмотрим счетномерное векторное пространство V над $\mathbb{K}$, базисом в котором являются символы $\{e_0, e_1, e_2, \ldots\} = \{e_i \mid i \in \mathbb{N} \cup 0\}$. Таким образом, элементами V являются выражения $\sum_i a_i e_i$, $a_i \in \mathbb{K}$, в которых $a_i \neq 0$ только для конечного множества индексов i.

Зададим правило умножения базисных элементов $e_k e_l = e_{k+l}$ и продолжим его по билинейности на конечные линейные комбинации:

$$\sum_i a_i e_i \sum_j b_j e_j = \sum_{i,j} a_i b_j e_{i+j} = \sum_k \left(\sum_{i+j=k} a_i b_j \right) e_k = \sum_k c_k e_k. \tag{34}$$

Тем самым мы определили некоторую алгебру над полем $\mathbb{K}$. Она ассоциативна, коммутативна и имеет единицу e_0. Первые два свойства следуют из ассоциативности $(e_k e_l)e_m = e_k(e_l e_m)(= e_{k+l+m})$ и коммутативности $e_k e_l = e_{k+l} = e_l e_k$ произведения базисных векторов.

Заметим, что $e_k = (e_1)^k$ при $k \in \mathbb{N} \cup 0$. Обозначим $x := e_1$, $1 := e_0$; тогда базис в V есть $\{1, x, x^2, \ldots\}$ и конечные линейные комбинации имеют вид обычных многочленов $\sum_i a_i x^i$ с привычным законом умножения многочленов.

Построенная нами алгебра $(V, +, \cdot)$ называется *алгеброй многочленов над полем* $\mathbb{K}$. Обычно она обозначается $\mathbb{K}[x]$ (где x — обозначение "переменной").

Заметим, что $\mathbb{K}$ можно рассматривать как подалгебру в $\mathbb{K}[x]$, состоящей из многочленов, для которых $a_1 = a_2 = \ldots = 0$ (т.е. "констант").

Замечание 5.8. Кстати, похожую конструкцию можно применить к группе. Пусть G, скажем, конечная группа. Рассмотрим линейное пространство V над $\mathbb{K}$, базис которого занумерован элементами группы, $\{e_g \mid g \in G\}$. Базисные элементы будем перемножать в соответствии с групповым законом: $e_g e_h = e_{gh}$. Продолжим по билинейности умножение базисных элементов на линейные комбинации:

$$\left(\sum_{g \in G} a_g e_g \right) \left(\sum_{h \in G} b_h e_h \right) = \sum_{g,h \in G} (a_g b_h e_{gh}) =$$

$$= \sum_{t\in G} \left(\sum_{(g,\,h)\colon\, gh=t} a_g b_h \right) e_t = \sum_{t\in G} \left(\sum_{g\in G} a_g b_{g^{-1}t} \right) e_t \tag{35}$$

(здесь мы положили $t = gh$, тогда $h = g^{-1}t$, и воспользовались тем, что когда g пробегает элементы G, пары $(g, g^{-1}t)$ пробегают пары (g, h) такие, что $gh = t$). Тогда мы получим пример ассоциативной (коммутативной если группа коммутативна) алгебры с единицей e_e, которая называется *групповой алгеброй* и обозначается $\mathbb{K}[G]$. Алгебра многочленов получается аналогичной конструкцией, если вместо группы взять полугруппу неотрицательных целых чисел по сложению.

Можно немного изменить обозначения и вместо выражений $\sum_g a_g e_g$ рассматривать соответствующие функции $a\colon G \to \mathbb{K}$, $a(g) = a_g$. Тогда групповая алгебра $\mathbb{K}[G]$ состоит из всех функций $a\colon G \to \mathbb{K}$ с операцией умножения $a * b = c$, где $c(t) = \sum_{g\in g} a(g)b(g^{-1}t)$ (ср. (5.8)), называемой *свёрткой*.

Аналогично, многочленом можно называть финитную функцию $a\colon \mathbb{Z}_{\geq 0} \to \mathbb{K}$, причем произведением многочленов a и b является свертка $a * b = c$, где $c(n) = \sum_{i+j=n} a(i)b(j)$, $n \in \mathbb{Z}_{\geq 0}$ (ср. формулу (34)).

Вернемся к многочленам. В многочлене $f(x) = \sum_i a_i x^i$ числа $a_0, a_1, a_2 \ldots$ называются *коэффициентами* многочлена. Если $f \neq 0$, то $\max\{\, k \mid a_k \neq 0\}$ называется *степенью многочлена* f и обозначается $\deg f$, а сам ненулевой коэффициент a_k с максимальным k называется *старшим коэффициентом* многочлена f. Положим степень нулевого многочлена равной $-\infty$ (что логично, поскольку $-\infty$ — точная верхняя грань пустого подмножества в $\mathbb{R}$).

Легко видеть, что

$$\deg(f+g) \leq \max\{\deg f, \deg g\},$$
$$\deg fg = \deg f + \deg g.$$

Например, второе равенство следует из того, что старший коэффициент произведения многочленов является произведением старших коэффициентов сомножителей, а в поле нет делителей нуля.

В качестве следствия получаем, что в алгебре многочленов над полем нет делителей нуля, а также что обратимыми элементами в $\mathbb{K}[x]$ являются только многочлены нулевой степени, то есть ненулевые элементы поля $\mathbb{K}$.

Аналогично алгебре многочленов от одной переменной $\mathbb{K}[x]$ можно определить *алгебру многочленов от n переменных* $\mathbb{K}[x_1, x_2, \ldots, x_n]$. Для этого рассмотрим векторное пространство V над $\mathbb{K}$ с базисом $e_{k_1 k_2 \ldots k_n}$, $k_i \geq 0$. Зададим правило умножения базисных векторов

$$e_{k_1 k_2 \ldots k_n} e_{l_1 l_2 \ldots l_n} = e_{k_1+l_1 k_2+l_2 \ldots k_n+l_n}$$

и продолжим его по билинейности на их конечные линейные комбинации. Ясно, что определенное таким образом умножение ассоциативно, коммутативно и $e_{00\ldots0}$ играет роль единицы. Обозначая $x_1 := e_{10\ldots0}$, $x_1 := e_{010\ldots0}, \ldots, x_n := e_{00,\ldots01}$, получаем $e_{k_1 k_2 \ldots k_n} = x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ и приходим к обычной записи многочлена от n переменных

$$f = \sum_{k_1, k_2, \ldots, k_n \geq 0} a_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

в которой только конечное число коэффициентов $a_{k_1 k_2 \ldots k_n}$ отлично от нуля.

Заметим, что многочлен от n переменных $x_1, x_2, \ldots, x_n$ однозначно записывается как многочлен от x_n с коэффициентами из $\mathbb{K}[x_1, x_2, \ldots, x_{n-1}]$, откуда получается изоморфизм колец

$$\mathbb{K}[x_1, x_2, \ldots, x_n] \cong \mathbb{K}[x_1, x_2, \ldots, x_{n-1}][x_n]. \tag{36}$$

Замечание 5.9. Рассуждение, с помощью которого мы доказали отсутствие делителей нуля в $\mathbb{K}[x]$ обобщается на случай, когда вместо поля $\mathbb{K}$ рассматривается произвольное коммутативное кольцо с единицей и без делителей нуля R: в этом случае кольцо $R[x]$ также не имеет делителей нуля. Используя это наблюдение вместе с изоморфизмом (36) и индукцией по числу переменных n, можно доказать, что кольцо $\mathbb{K}[x_1, x_2, \ldots, x_n]$ не имеет делителей нуля.

Каждый многочлен

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in \mathbb{K}[x]$$

определяет функцию на $\mathbb{K}$ со значениями в $\mathbb{K}$, значение которой в точке $c \in \mathbb{K}$ по определению равно

$$f(c) = a_0 + a_1 c + a_2 c^2 + \ldots + a_n c^n.$$

Легко видеть, что сопоставление $f \mapsto f(c)$ определяет гомоморфизм алгебр (в частности, колец) $\alpha_c \colon \mathbb{K}[x] \to \mathbb{K}$, то есть

$$(f+g)(c) = f(c) + g(c), \quad (fg)(c) = f(c)g(c), \quad (\lambda f)(c) = \lambda f(c).$$

В частности, для каждого $c \in \mathbb{K}$ мы получаем свой гомоморфизм α_c.

Если поле $\mathbb{K}$ бесконечно, то, как свидетельствует следующая Теорема, отождествление многочленов с определяемыми ими функциями на $\mathbb{K}$ не приводит к потере информации. Например, $\mathbb{R}[x]$ можно рассматривать как подалгебру в алгебре $C(\mathbb{R})$ вещественнозначных непрерывных функций на вещественной прямой. Но в случае конечного поля $\mathbb{K}$ разные многочлены могут задавать одну и ту же функцию, например, многочлены x и x^2 над полем $\mathbb{Z}_2$. Именно по этой причине мы в начале этого параграфа дали "алгебраическую" конструкцию алгебры многочленов $\mathbb{K}[x]$ без упоминания функций.

Теорема 5.10. *Если поле $\mathbb{K}$ бесконечно, то разные многочлены над $\mathbb{K}$ определяют разные функции.*

Доказательство. Приведем доказательство, основанное на идеях линейной алгебры; другое доказательство мы получим как следствие Теоремы 5.14.

Итак, пусть многочлены $f, g \in \mathbb{K}[x]$ определяют одну и ту же функцию. Тогда их разность $h := f - g$ определяет нулевую функцию, то есть $h(c) = 0 \; \forall\, c \in \mathbb{K}$. Предположим, что $h \neq 0$ и пусть

$$h = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \quad (a_{n-1} \neq 0).$$

Возьмем различные $c_1, c_2, \ldots, c_n \in \mathbb{K}$ (здесь используется бесконечность поля $\mathbb{K}$). Совокупность верных равенств

$$\begin{cases} a_0 + a_1 c_1 + a_2 c_1^2 + \ldots + a_{n-1} c_1^{n-1} = 0, \\ a_0 + a_1 c_2 + a_2 c_2^2 + \ldots + a_{n-1} c_2^{n-1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1 c_n + a_2 c_n^2 + \ldots + a_{n-1} c_n^{n-1} = 0 \end{cases} \tag{37}$$

будем рассматривать как квадратную систему линейных однородных уравнений относительно $a_0, a_1, a_2, \ldots, a_{n-1}$. Определитель матрицы коэффициентов этой системы есть определитель Вандермонда и потому отличен от нуля. Следовательно, система имеет только нулевое решение, что противоречит нашему предположению. ■

Замечание 5.11. Даже если поле $\mathbb{K}$ конечно, множество всех многочленов над $\mathbb{K}$ бесконечно (но счетно). Однако множество всех функций на $\mathbb{K}$ со значениями в $\mathbb{K}$ в этом случае конечно, и поэтому обязательно должны существовать разные многочлены, определяющие одну и ту же функцию. Тем не менее предыдущая Теорема и ее доказательство остаются в силе для многочленов, степень которых меньше числа элементов поля $\mathbb{K}$.

Перейдем к делению многочлена на ненулевой многочлен с остатком.

Теорема 5.12. *Пусть $f, g \in \mathbb{K}[x]$, причем $g \neq 0$. Тогда существуют такие многочлены q и r, что $f = qg + r$ и либо $r = 0$, либо $\deg r < \deg g$. Многочлены q и r определены этими условиями однозначно.*

Доказательство. 1) Докажем возможность деления с остатком. Если $\deg f < \deg g$, то можно взять $q = 0$, $r = f$. Если $\deg f \geq \deg g$, то q и r находятся обычной процедурой "деления уголком". А именно, пусть

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_0,$$

$$g = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m,$$

где a_0, $b_0 \neq 0$. Рассмотрим многочлен

$$f_1 = f - \frac{a_0}{b_0}x^{n-m}g.$$

Его степень меньше, чем степень многочлена f. Если $\deg f_1 < \deg g$, то можно взять

$$q = \frac{a_0}{b_0}x^{n-m}, \quad r = f_1.$$

В противном случае поступаем с многочленом f_1 так же, как с f. В конце концов мы получим такой многочлен

$$q = c_0x^{n-m} + c_1x^{n-m-1} + \ldots + c_{n-m},$$

что $\deg(f - qg) < \deg g$. Это и будет неполное частное от деления f на g, а многочлен $r = f - qg$ будет остатком.

2) Докажем, что многочлены q и r определены условиями теоремы однозначно. Пусть

$$f = q_1g + r_1 = q_2g + r_2,$$

где $\deg r_1 < \deg g$ и $\deg r_2 < \deg g$. Тогда

$$r_1 - r_2 = (q_2 - q_1)g$$

и, если $q_1 \neq q_2$, то

$$\deg(r_1 - r_2) = \deg(q_2 - q_1) + \deg g \geq \deg g,$$

что, очевидно, неверно. Следовательно, $q_1 = q_2$ и $r_1 = r_2$. ■

Особое значение имеет деление на линейный двучлен $x - c$. В этом случае остаток имеет степень < 1, т.е. является элементом поля $\mathbb{K}$. Таким образом, результат деления с остатком многочлена f на $x - c$ имеет вид

$$f(x) = (x - c)q(x) + r \quad (r \in \mathbb{K}).$$

Отсюда следует, что $f(c) = r$, т.е. остаток равен значению многочлена f в точке c. Это утверждение называется *теоремой Безу.*

5.3 Общие свойства корней многочленов

Элемент c поля $\mathbb{K}$ называется *корнем* многочлена $f \in \mathbb{K}[x]$ (или соответствующего алгебраического уравнения $f(x) = 0$), если $f(c) = 0$. Из Теоремы Безу (см. предыдущий параграф) следует

Теорема 5.13. *Элемент c поля $\mathbb{K}$ является корнем многочлена $f \in \mathbb{K}[x]$ тогда и только тогда, когда f делится на $x - c$.*

Этим можно воспользоваться для доказательства следующей теоремы.

Теорема 5.14. *Число корней ненулевого многочлена не превосходит его степени.*

Доказательство. Пусть c_1 — корень многочлена f. Тогда

$$f = (x - c_1)f_1 \quad (f_1 \in \mathbb{K}[x]).$$

Пусть c_2 — корень многочлена f_1. Тогда

$$f_1 = (x - c_2)f_2 \quad (f_2 \in \mathbb{K}[x])$$

и, значит,

$$f = (x - c_1)(x - c_2)f_2.$$

Продолжая так дальше, мы в конце концов представим многочлен f в виде

$$f = (x - c_1)(x - c_2)\dots(x - c_m)g, \tag{38}$$

где многочлен $g \in \mathbb{K}[x]$ не имеет корней. Числа $c_1, c_2, \dots, c_m$ — это все корни многочлена f. В самом деле, для любого $c \in \mathbb{K}$ имеем

$$f(c) = (c - c_1)(c - c_2)\dots(c - c_m)g(c)$$

и, так как $g(c) \neq 0$, то $f(c) = 0$ только если $c - c_i$ для некоторого i. Таким образом, число корней многочлена f не превосходит m (оно может быть меньше m, поскольку не исключено, что среди чисел $c_1, c_2, \dots, c_m$ есть одинаковые); но

$$m = \deg f - \deg g \leq \deg f. \quad \blacksquare$$

Заметим, что из только что доказанной Теоремы можно получить новое доказательство Теоремы 5.10. А именно, если два многочлена f и g совпадают как функции на $\mathbb{K}$, то любой элемент поля $\mathbb{K}$ является корнем их разности $h = f - g$, а ненулевой многочлен в силу доказанной Теоремы имеет конечное число корней (не превосходящее его степени).

Доказательство предыдущей теоремы наводит на мысль, что корни правильнее считать с кратностями. *Кратностью* корня c называется наибольшее из таких k, что f делится на $(x - c)^k$. *Простым* корнем называется корень кратности 1. Иногда удобно считать, что число, не являющееся корнем, — это корень кратности 0.

Лемма 5.15. *c является корнем кратности k многочлена f тогда и только тогда, когда*

$$f = (x - c)^k g, \tag{39}$$

где $g(c) \neq 0$.

Доказательство. В самом деле, если имеет место представление (39), то c — корень кратности не меньше k. Если c является корнем кратности $> k$, то $f = (x - c)^{k+1}h$, и тогда, сокращая на $(x - c)^k$ равенство $(x - c)^k g = (x - c)^{k+1}h$ (и используя то, что в $\mathbb{K}[x]$ нет делителей нуля), получаем $g = (x - c)h$, что противоречит предположению $g(c) \neq 0$.

Обратно, если k — кратность корня c многочлена f, то $f = (x - c)^k h$приведенной для некоторого $h \in \mathbb{K}[x]$. Если $h(c) = 0$, то по следствию из Теоремы Безу $h = (x - c)p$, где $p \in \mathbb{K}[x]$, и тогда $(x - c)^{k+1} \mid f$, что противоречит нашему предположению. $\blacksquare$

Теперь мы докажем уточнение Теоремы 5.14.

Теорема 5.16. *Число корней ненулевого многочлена с учётом их кратностей не превосходит степени многочлена, причём равенство имеет место тогда и только тогда, когда этот многочлен раскладывается на линейные множители.*

Доказательство. Перепишем равенство (38), объединив одинаковые множители:

$$f = (x - c_1)^{k_1}(x - c_2)^{k_2} \dots (x - c_s)^{k_s} g \tag{40}$$

($c_1, c_2, \dots, c_s$ различны). Ясно, что $c_1, c_2, \dots, c_s$ — это все корни многочлена f. Далее, выделяя в (40) множитель $(x - c_i)^{k_i}$, мы можем написать

$$f = (x - c_i)^{k_i} h, \quad \text{где} \quad h_i(c_i) \neq 0.$$

Следовательно, c_i — корень кратности k_i.

Таким образом, число корней многочлена f с учётом кратностей равно

$$k_1 + k_2 + \ldots + k_s = \deg f - \deg g,$$

откуда и вытекают все утверждения Теоремы. ■

Если многочлен

$$f = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

раскладывается на линейные множители, то это разложение может быть записано в виде

$$f = a_0(x - c_1)(x - c_2) \dots (x - c_n),$$

где $c_1, c_2, \dots, c_n$ — корни многочлена f, причём каждый из них повторен столько раз, какова его кратность. Приравнивая коэффициенты при соответствующих степенях x в этих двух представлениях многочлена f, мы получаем следующие *формулы Виета:*

$$c_1 + c_2 + \ldots + c_n = -\frac{a_1}{a_0},$$

$$c_1 c_2 + c_1 c_3 + \ldots + c_{n-1} c_n = \frac{a_2}{a_0}.$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\sum_{i_1 < i_2 < \ldots < i_k} c_{i_1} c_{i_2} \dots c_{i_k} = (-1)^k \frac{a_k}{a_0},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$c_1 c_2 \dots c_n = (-1)^n \frac{a_n}{a_0}.$$

В левой части k-й формулы Виета стоит сумма всевозможных произведений k корней многочлена f. С точностью до множителя $(-1)^k$ это коэффициент при x^{n-k} в произведении $(x - c_1)(x - c_2) \dots (x - c_n)$.

В случае $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$ существует еще одна интерпретация кратности корня многочлена из $\mathbb{K}[x]$ с использованием производной.

Сделав в многочлене $f \in \mathbb{K}[x]$ замену $x = c + y$, где $c \in \mathbb{K}$, мы можем представить его в виде многочлена (той же степени) от $y = x - c$ или, как говорят, разложить по степеням $x - c$:

$$f = b_0 + b_1(x - c) + b_2(x - c)^2 + \ldots + b_n(x - c)^n. \tag{41}$$

Очевидно, что если c —корень многочлена f, то его кратность равна номеру первого отличного от нуля коэффициента этого разложения.

Предложение 5.17. *Если $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$, то коэффициенты разложения $f \in \mathbb{K}[x]$ по степеням $x - c$ могут быть найдены по формулам*

$$b_k = \frac{f^{(k)}(c)}{k!}.$$

Доказательство. Продифференцируем равенство (41) k раз и подставим $x = c$. ■

Таким образом,

$$f = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n.$$

Эта формула называется *формулой Тейлора* для многочленов.

Из формулы Тейлора и сделанного выше замечания следует

Теорема 5.18. *Если $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$, то кратность корня c многочлена $f \in \mathbb{K}[x]$ равна наименьшему порядку производной многочлена f, не обращающейся в нуль в точке c.*

Следствие 5.19. *При том же условии всякий k-кратный корень многочлена f является $(k-1)$-кратным корнем его производной.*

5.4 Многочлены над полями $\mathbb{C}$ и $\mathbb{R}$

Над полем $\mathbb{R}$ существуют многочлены положительной степени, не имеющие ни одного вещественного корня, например $x^2 + 1$. Такие многочлены могут иметь сколь угодно большую степень, например, $\frac{x^p-1}{x-1}$, где p — простое число. Чудом кажется тот факт, что "присоединяя" к полю $\mathbb{R}$ один из корней такого многочлена, мы получаем поле $\mathbb{C}$, которое является *алгебраически замкнутым*: все многочлены над $\mathbb{C}$ (т.е. не только с вещественными, но и с комплексными коэффициентами) положительной степени имеют корень, лежащий в $\mathbb{C}$, а значит раскладываются на линейные множители над $\mathbb{C}$.

Теорема 5.20. *Всякий многочлен положительной степени над полем $\mathbb{C}$ имеет корень.*

Поле, над которым всякий многочлен положительной степени имеет хотя бы один корень, называется *алгебраически замкнутым*. Таким образом, предыдущая теорема означает, что поле $\mathbb{C}$ является алгебраически замкнутым.

Существуют различные доказательства этой теоремы. Любое из них включает элементы анализа (или топологии), в частности, одно из них обычно приводится в курсе комплексного анализа. Существует и более алгебраическое доказательство, основанное на теории Галуа. Мы в этом курсе их не приводим.

Следствие 5.21. *В кольце $\mathbb{C}[x]$ всякий ненулевой многочлен раскладывается на линейные множители.*

В самом деле, в силу предыдущей Теоремы многочлен g в разложении (38) должен иметь нулевую степень, т.е. быть просто числом.

В силу Теоремы 5.16 отсюда получаем

Следствие 5.22. *Всякий многочлен степени n над $\mathbb{C}$ имеет n корней с учетом кратностей.*

Займемся теперь многочленами с вещественными коэффициентами, т.е. элементами $\mathbb{R}[x]$. Такой многочлен степени n может иметь $< n$ (в частности, вообще не иметь) вещественных корней, но, как и всякий многочлен с комплексными коэффициентами, он всегда имеет ровно n комплексных корней (с учетом кратностей).

Теорема 5.23. *Пусть $f \in \mathbb{R}[x]$ и $c \in \mathbb{C}\backslash\mathbb{R}$ — корень f, то и комплексно сопряженное $\bar{c}$ также является корнем f, причем той же кратности что и c.*

Доказательство. Используя вещественность коэффициентов многочлена f и свойства операции комплексного сопряжения, имеем

$$f(c) = 0 \quad \Leftrightarrow \quad \overline{f(c)} = 0 \quad \Leftrightarrow \quad f(\overline{c}) = 0.$$

То есть $\overline{c}$ — также корень многочлена f. Аналогично доказывается, что

$$f^{(k)}(c) = 0 \quad \Leftrightarrow \quad f^{(k)}(\overline{c}) = 0.$$

Следовательно, кратности корней c и $\overline{c}$ одинаковые (см. Теорему 5.18). ■

Следствие 5.24. *В кольце $\mathbb{R}[x]$ всякий ненулевой многочлен раскладывается на линейные и квадратичные множители с отрицательным дискриминантом.*

Доказательство. Заметим, что если $c \in \mathbb{C}\backslash\mathbb{R}$, то квадратный трехчлен

$$(x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}$$

имеет вещественные коэффициенты; его дискриминант отрицателен.

Пусть теперь

$$c_1, \ldots, c_s, c_{s+1}, \ldots, c_{s+t}, \overline{c}_{s+1}, \ldots, \overline{c}_{s+t}$$

— все (различные) комплексные корни многочлена $f \in \mathbb{R}[x]$, причем

$$c_1, \ldots, c_s \in \mathbb{R}, \quad c_{s+1}, \ldots, c_{s+t} \notin \mathbb{R}.$$

Если кратность корня c_i равна k_i, то

$$f = a_0(x - c_1)^{k_1} \ldots (x - c_s)^{k_s}[(x - c_{s+1})(x - \overline{c}_{s+1})]^{k_{s+1}} \ldots [(x - c_{s+t})(x - \overline{c}_{s+t})]^{k_{s+t}}$$

(где a_0 — старший коэффициент многочлена f). Перемножая линейные множители в квадратных скобках, получаем искомое разложение. ■

Следствие 5.25. *Многочлен нечетной степени над $\mathbb{R}$ имеет вещественный корень.*

Пример 5.26.

$$x^5 - 1 = (x - 1)[(x - e^{\frac{2\pi i}{5}})(x - e^{\frac{8\pi i}{5}})][(x - e^{\frac{4\pi i}{5}})(x - e^{\frac{6\pi i}{5}})] =$$
$$(x - 1)\left(x^2 - \frac{\sqrt{5} - 1}{2}x + 1\right)\left(x^2 + \frac{\sqrt{5} + 1}{2}x + 1\right).$$

5.5 Евклидовы кольца

Разложение многочленов над $\mathbb{C}$ на линейные множители и многочленов над $\mathbb{R}$ на линейные и квадратичные множители аналогично разложению целых чисел на простые множители. Для многочленов над произвольным полем также имеется подобное разложение, но его множители могут иметь произвольную степень. В этом параграфе мы докажем существование и единственность (в некотором точном смысле) такого разложения, а также существование и единственность разложения целого числа на простые множители (результат, называемый “Основной теоремой арифметики”).

Для того, чтобы охватить единым рассуждением оба случая, введем некоторые общие понятия.

Определение 5.27. Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется *целостным кольцом* (или *областью целостности*).

Так, кольцо $\mathbb{Z}$ и кольцо многочленов $\mathbb{K}[x]$ над любым полем $\mathbb{K}$ являются целостными кольцами. Более того, кольцо многочленов над любым целостным кольцом является целостным (см. Замечание 5.9). Например, целостным является кольцо многочленов $\mathbb{Z}[x]$ (что, впрочем, понятно и так, так как оно является подкольцом с единицей в $\mathbb{R}[x]$). Заметим, что кольцо, состоящее из одного нуля, не считается целостным.

Пусть A — целостное кольцо. Говорят, что элемент $b \in A$ *делит* элемент $a \in A$ (обозначение: $b \mid a$), если существует элемент $q \in A$ такой, что $a = qb$. Элементы a и b называются *ассоциированными* (обозначение: $a \sim b$), если выполняется любое из следующих эквивалентных условий:

1) $b \mid a$ и $a \mid b$;

2) $a = cb$, где $c \in A$ — обратимый элемент.

В следующем определении аксиоматизируется то общее, что есть у кольца многочленов над полем и кольца целых чисел $\mathbb{Z}$ — возможность деления с остатком.

Определение 5.28. Целостное кольцо A, не являющееся полем, называется *евклидовым*, если существует функция

$$N\colon A\backslash\{0\} \to \mathbb{Z}_{>0}$$

(называемая (евклидовой) *нормой*), удовлетворяющая следующим условиям:

1) $N(ab) \geq N(a)$, причем равенство имеет место только тогда, когда элемент b обратим;

2) для любых $a, b \in A$, где $b \neq 0$, существуют такие $q, r \in A$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Основными для нас примерами евклидовых колец являются $\mathbb{Z}$ с функцией модуля в качестве нормы, и кольцо $\mathbb{K}[x]$ многочленов над полем $\mathbb{K}$, где роль евклидовой нормы играет степень многочлена. Существуют и другие примеры евклидовых колец.

Условие 2) из Определения выше означает возможность "деления с остатком". Его единственности (то есть однозначной определенности пары q, r) не требуется. Например, $5 = 1\cdot 3+2$, но также и $5 = 2\cdot 3+(-1)$.

Замечание 5.29. Заметим, что вторая часть условия 1) может быть выведена из остальных условий. В самом деле, пусть элемент b необратим. Тогда a не делится на ab (в самом деле, если $a = qab$, то $1 = qb$ и, вопреки предположению, b обратим). Разделим a на ab с остатком:

$$a = q(ab) + r, \quad r \neq 0.$$

Так как $r = a(1 - qb)$, то

$$N(a) \leq N(r) < N(ab),$$

что и требовалось.

Приведем пример евклидова кольца, отличный от упоминавшихся ранее.

Пример 5.30. Комплексные числа вида $c = a + bi$, где $a, b \in \mathbb{Z}$, называются *целыми гауссовыми числами*. Они образуют подкольцо с единицей в $\mathbb{C}$, обозначаемое $\mathbb{Z}[i]$.

Кольцо $\mathbb{Z}[i]$ является евклидовым относительно нормы

$$N(c) = |c|^2 = a^2 + b^2.$$

В самом деле, очевидно, что $N(cd) = N(c)N(d)$ и, поскольку $N(1) = 1$, обратимые элементы кольца $\mathbb{Z}[i]$ — это элементы с нормой 1, то есть ± 1 и $\pm i$. Отсюда следует, что выполнено условие 1) в определении евклидова кольца.

Докажем возможность деления с остатком. Пусть $c, d \in \mathbb{Z}[i]$, $d \neq 0$. Рассмотрим целое гауссово число q, ближайшее к $\frac{c}{d} \in \mathbb{C}$. Поскольку целые гауссовы числа расположены в вершинах решетки со стороной 1

в комплексной плоскости, то расстояние от $\frac{c}{d}$ до q не превосходит $1/\sqrt{2}$, то есть $|\frac{c}{d} - q| \leq 1/\sqrt{2}$. Положим $r := c - qd \in \mathbb{Z}[i]$. Тогда $c = qd + r$ и

$$N(r) = |c - qd|^2 = |\frac{c}{d} - q|^2 |d|^2 \leq \frac{1}{2} N(d) < N(d).$$

Определение 5.31. *Наибольшим общим делителем* элементов a и b целостного кольца называется их общий делитель, делящийся на все их общие делители. Он обозначается (a, b).

Наибольший общий делитель, если он существует, определен однозначно с точностью до ассоциированности. Однако его может не существовать. Например, элементы x^5 и x^6 в кольце $\mathbb{K}[x^2, x^3] \subset \mathbb{K}[x]$ многочленов без линейного члена не имеют наибольшего общего делителя.

Теорема 5.32. *В евклидовом кольце для любых двух элементов a, b существует наибольший общий делитель d, и он может быть представлен в виде $d = au + bv$, где u, v — какие-то элементы кольца.*

Доказательство. Если $b = 0$, то $d = a = a \cdot 1 + b \cdot 0$. Если a делится на b, то $d = b = a \cdot 0 + b \cdot 1$. В общем случае доказательство дословно повторяет доказательство Предложения 1.27. ■

Процедура нахождения наибольшео общего делителя, использованная в этом доказательстве, называется *алгоритмом Евклида.* Элементы a, $b \in A$ называются *взаимно простыми*, если $(a, b) = 1$. В этом случае, согласно доказанной Теореме, существуют такие u, $v \in A$, что

$$au + bv = 1.$$

Пример 5.33. Покажем, что кольцо $\mathbb{Z}[x]$ многочленов с целыми коэффициентами не является евклидовым. Рассмотрим пару элементов $a = 2$ и $b = x$ этого кольца. Ясно, что их наибольший общий делитель есть 1. В то же время 1 нельзя представить в виде $2g + xh$, где g, $h \in \mathbb{Z}[x]$, поскольку $2g + xh$ является многочленом, свободный член которого четен.

Перейдем теперь к вопросу о разложении на простые множители в евклидовом кольце.

Определение 5.34. Необратимый ненулевой элемент p целостного кольца называется *простым*, если его нельзя представить в виде $p = ab$, где a и b — необратимые элементы.

Иначе говоря, элемент p простой, если всякий его делитель ассоциирован либо с 1 либо с p. Простые элементы кольца $\mathbb{Z}$ в этом смысле — это числа вида $\pm p$, где p — простое число.

Простые элементы кольца $\mathbb{K}[x]$, где $\mathbb{K}$ — поле, по традиции называются *неприводимыми многочленами.* Таким образом, неприводимый многочлен — это такой многочлен положительной степени, который не может быть разложен в произведение двух многочленов положительной степени (в $\mathbb{K}[x]$).

Очевидно, что всякий многочлен первой степени неприводим. Из Следствия 5.21 мы знаем, что неприводимые многочлены над $\mathbb{C}$ — это только многочлены первой степени, а из Следствия 5.24 — что неприводимые многочлены над $\mathbb{R}$ — это многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. Можно показать, что неприводимые многочлены над полем $\mathbb{Q}$ могут иметь любую степень.

Пример 5.35. Опишем простые элементы в кольце $\mathbb{Z}[i]$. Это, с точностью до ассоциированности, простые натуральные числа вида $4k + 3$, числа вида $a + bi$ (a, $b \in \mathbb{N}$), где $a^2 + b^2$ есть простое натуральное число вида $4k + 1$ и число $1 + i$.

Пусть A — произвольное евклидово кольцо.

Лемма 5.36. Если простой элемент p кольца A делит произведение $a_1 a_2 \dots a_n$, то он делит хотя бы один из сомножителей $a_1, a_2, \dots, a_n$.

Доказательство. Докажем это утверждение индукцией по n. При $n = 2$ предположим, что p не делит a_1. Тогда $(p, a_1) = 1$ и, значит, существуют такие u, $v \in A$, что $pu + a_1 v = 1$. Умножая это равенство на a_2 получаем

$$pua_2 + a_1 a_2 v = a_2,$$

откуда следует что p делит a_2

При $n > 2$ представим произведение $a_1 a_2 \dots a_n$ в виде $a_1(a_2 \dots a_n)$. По доказанному $p \mid a_1$ или $p \mid a_2 \dots a_n$. Во втором случае по предположению индукции $p \mid a_i$ где i — один из индексов $2, \dots, n$. ■

Теорема 5.37. *В евклидовом кольце всякий необратимый ненулевой элемент может быть разложен на простые множители, причем это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы. (Говоря о разложении на простые множители мы не исключаем разложения, состоящего только из одного множителя).*

Доказательство. Назовем необратимый ненулевой элемент $a \in A$ *хорошим*, если он может быть разложен на простые множители. Предположим, что существуют *плохие* элементы. Выберем из них элемент с наименьшей нормой. Пусть это будет элемент a. Он не может быть простым. Следовательно, $a = bc$, где b и c — необратимые элементы. Имеем $N(b) < N(a)$ и $N(c) < N(a)$ и, значит, b и c — хорошие элементы; но тогда, очевидно, и a — хороший элемент, что противоречит нашему предположению. Таким образом, всякий необратимый ненулевой элемент кольца A может быть разложен на простые множители.

Докажем теперь индукцией по n, что если

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \tag{42}$$

где p_i, q_j — простые элементы, то $m = n$ и, после подходящей перенумерации множителей, $p_i \sim q_i$ при $i = 1, 2, \dots, n$.

При $n = 1$ это утверждене очевидно. При $n > 1$ имеем $p_1 \mid q_1 q_2 \dots q_m$ и по лемме 5.36 существует такой номер i, что $p_1 \mid q_i$. Тогда $p_1 \sim q_i$. Можно считать, что $i = 1$ и $p_1 = q_1$. Сокращая равенство (42) на p_1, получаем

$$p_2 \dots p_n = q_2 \dots q_m.$$

По предположению индукции отсюда следует, что $m = n$ и, после подходящей перенумерации, $p_i \sim q_i$ при $i = 2, \dots, n$. Тем самым утверждение доказано. ■

Задача 5.38. *Докажите, что в евклидовом кольце*

1) $b \mid a$, $c \mid a$ *и* $(b, c) = 1 \;\Rightarrow\; bc \mid a$;

2) $c \mid ab$ *и* $(b, c) = 1 \;\Rightarrow\; c \mid a$.

Известно, что простых чисел бесконечно много. Напомним рассуждение, которое это доказывает (оно похоже на то, которое приведено в Началах Евклида). Предположим что $p_1, p_2, \dots, p_n$ — это все простые числа. Тогда число $p_1 p_2 \dots p_n + 1$ не делится ни на одно из них, что, очевидно, невозможно.

Интересен вопрос о том, как простые числа распределены среди натуральных. Вот простейший результат в этом направлении.

Предложение 5.39. *Существуют сколь угодно длинные отрезки натурального ряда, не содержащие простых чисел.*

Доказательство. Рассмотрим n последовательных натуральных чисел

$$(n+1)! + 2,\ (n+1)! + 3, \dots, (n+1)! + n + 1.$$

Первое из них делится на 2, второе — на 3 и т.д., последнее делится на $n + 1$, т.е. все они являются составными. ■

Замечание 5.40. Обозначим через $\pi(n)$ количество простых чисел среди первых n натуральных чисел $1, 2, \ldots, n$. Еще Гаусс заметил, что

$$\pi(n) \sim \frac{n}{\ln n} \quad \text{при} \quad n \to \infty.$$

Рассуждение, аналогичное приведенному выше, показывает, что количество нормированных (т.е. со старшим коэффициентом 1) неприводимых многочленов над любым полем $\mathbb{K}$ бесконечно. Если само поле $\mathbb{K}$ бесконечно, этот результат не представляет интереса, так как в этом случае имеется бесконечно много нормированных многочленов первой степени. Однако если поле $\mathbb{K}$ конечно, то этот результат означает, что имеются неприводимые многочлены сколь угодно высокой степени. Из этого сразу следует, что любое алгебраически замкнутое поле бесконечно.

5.6 Кольца классов вычетов

Напомним, что определение кольца классов вычетов $\mathbb{Z}_n$ по модулю n дано в Примере 1.50. Это — ассоциативное коммутативное кольцо с единицей.

Предложение 5.41. *Элемент* $[k] \in \mathbb{Z}_n$ *обратим* $\Leftrightarrow (k, n) = 1$.

Доказательство. Если $(k, n) = 1$, то по тождеству Безу $\exists\, u, v \in \mathbb{Z}$ такие, что $ku + pv = 1$. Тогда $[ku + pv] = [k] \cdot [u] = [1]$, и значит $[k]^{-1} = [u]$.

Обратно, если $(k, n) = d > 1$, то пусть $n_1 := \frac{n}{d}$. Тогда $[n_1] \neq [0]$, но $[k][n_1] = [0]$, поскольку $n \mid kn_1$. Значит, $[k]$ — делитель нуля в $\mathbb{Z}_n$ и, следовательно, необратим. ■

Напомним, что $\mathbb{Z}_n^*$ — группа обратимых элементов кольца $\mathbb{Z}_n$.

Следствие 5.42. $|\mathbb{Z}_n^*| = \phi(n)$, *где* ϕ — *функция Эйлера.*

Доказательство. По определению $\phi(n)$ — количество чисел среди $1, 2, \ldots, n$ взаимно простых с n, в то время как $\mathbb{Z}_n = \{[1], [2], \ldots, [n]\}$. ■

Из доказательства предыдущего Предложения легко вывести

Следствие 5.43. *Кольцо* $\mathbb{Z}_n$ *не имеет делителей нуля* $\Leftrightarrow n$ — *простое число.*

Следствие 5.44. *Кольцо* $\mathbb{Z}_n$ *является полем* $\Leftrightarrow n$ — *простое число.*

Для натуральных k, l определим *прямую сумму* $\mathbb{Z}_k \oplus \mathbb{Z}_l$ колец как множество упорядоченных пар $\mathbb{Z}_k \times \mathbb{Z}_l$ с покомпонентными операциями. В частности, аддитивной группой кольца $\mathbb{Z}_k \oplus \mathbb{Z}_l$ является прямая сумма аддитивных групп $\mathbb{Z}_k \oplus \mathbb{Z}_l$ (для упрощения обозначений мы в данном случае используем одинаковые обозначения для групп и колец).

Определение 5.45. Отображение f кольца A в кольцо B называется *гомоморфизмом*, если оно сохраняет операции, т.е. если

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$

для любых $x, y \in A$. *Изоморфизмом* называется биективный гомоморфизм.

Очевидным образом определяются *ядро* и *образ* гомоморфизма колец $f\colon A \to B$, являющиеся подкольцами соответственно в A и в B. Про ядро гомоморфизма колец можно сказать больше: оно является т.н. *идеалом* (двусторонним) в A. Что это такое, а также про теорему о гомоморфизмах колец можно почитать в более подробных учебниках, например, в [11].

Пример 5.46. Отображение $\mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto [k]_n$ является гомоморфизмом колец с ядром $n\mathbb{Z} \subset \mathbb{Z}$.

Задача 5.47. *Опишите все гомоморфизмы*

1) групп $\mathbb{Z} \to \mathbb{Q}$;

2) колец $\mathbb{Z} \to \mathbb{Q}$.

Задача 5.48. *Опишите ядра гомоморфизмов колец*

1) $\mathbb{K}[x] \to \mathbb{K}$, $f \mapsto f(c)$, $c \in \mathbb{K}$;

2) $\mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(c)$, $c \in \mathbb{C}\backslash\mathbb{R}$.

Предложение 5.49. *Пусть* $(k, l) = 1$, $n := kl$. *Тогда отображение*

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_k \oplus \mathbb{Z}_l, \quad [a]_n \mapsto ([a]_k, [a]_l)$$

является изоморфизмом колец.

Доказательство. То, что данное отображение корректно определено и является изоморфизмом групп, мы уже проверили в доказательстве Предложения 4.105. Осталось проверить, что φ согласовано с умножением:

$$\varphi([ab]_n) = ([ab]_k, [ab]_l) = ([a]_k[b]_k, [a]_l[b]_l) = ([a]_k, [a]_l)([b]_k, [b]_l) = \varphi([a]_n)\varphi([b]_n). \quad \blacksquare$$

Следствие 5.50. *Если* $(k, l) = 1$, *то* $\phi(kl) = \phi(k)\phi(l)$.

Доказательство. Изоморфизм, доказанный в предыдущем Предложении, устанавливает изоморфизм групп обратимых элементов $\mathbb{Z}_{kl}^*$ и $(\mathbb{Z}_k \oplus \mathbb{Z}_l)^*$. Так как операции в кольце $\mathbb{Z}_k \oplus \mathbb{Z}_l$ определены покомпонентно, то элемент $([a]_k, [b]_l) \in \mathbb{Z}_k \oplus \mathbb{Z}_l$ обратим $\Leftrightarrow$ $[a]_k$ обратим в $\mathbb{Z}_k$ и $[b]_l$ обратим в $\mathbb{Z}_l$. Значит, $(\mathbb{Z}_k \oplus \mathbb{Z}_l)^* \cong \mathbb{Z}_k^* \times \mathbb{Z}_l^*$. $\blacksquare$

Следствие позволяет эффективно вычислять функцию Эйлера: если $n = p_1^{k_1} \dots p_s^{k_s}$, где $p_i \neq p_j$, то $\phi(n) = \phi(p_1^{k_1}) \dots \phi(p_s^{k_s})$; кроме того, как мы знаем (см. Задачу 4.40), $\phi(p^k) = p^k - p^{k-1}$.

5.7 Поля

Выше мы видели примеры полей, которые не содержат нетривиальных (отличных от них самих) подполей. Эти примеры — поля классов вычетов $\mathbb{Z}_p$ (где p — произвольное простое) и поле рациональных чисел $\mathbb{Q}$. Оказывается, любое поле содержит одно (и только одно) из указанных полей. Обсудим этот вопрос более подробно.

Пусть $\mathbb{K}$ — произвольное поле. Рассмотрим в $(\mathbb{K}, +)$ циклическую подгруппу, порожденную единицей $1 \in \mathbb{K}$.

Пусть эта подгруппа конечна порядка n, то есть n — такое наименьшее натуральное число, что выполнено соотношение $1 + 1 + \ldots + 1 = 0$ (n слагаемых) в $\mathbb{K}$. Если n не простое, то $n = kl$ и произведение суммы k единиц на сумму l единиц равно нулю, хотя оба слагаемых отличны от нуля. Так как в поле не может быть делителей нуля, такое невозможно и значит n обязательно простое число, $n = p$. В этом случае говорят, что поле $\mathbb{K}$ имеет *характеристику* p, $\operatorname{char}\mathbb{K} = p$. Заметим, что в поле $\mathbb{K}$ характеристики p для любого $a \in \mathbb{K}$ сумма

$$a + a + \ldots + a = (1 + 1 + \ldots + 1)a$$

(p слагаемых) равна нулю.

Если 1 порождает бесконечную циклическую подгруппу в $(\mathbb{K}, +)$, то поле $\mathbb{K}$ по определению имеет *нулевую характеристику*, $\operatorname{char}\mathbb{K} = 0$.

Предложение 5.51. *Любое поле характеристики p содержит подполе, изоморфное $\mathbb{Z}_p$. Любое поле характеристики 0 содержит подполе, изоморфное $\mathbb{Q}$.*

Доказательство. Отображение

$$f\colon \mathbb{Z} \to \mathbb{K}, \quad f(k) = k \cdot 1$$

является гомоморфизмом колец. В самом деле, $f(k+l) = (k+l)1 = k1 + l1 = f(k) + f(l)$, $f(kl) = (kl)1 = (k1)(l1) = f(k)f(l)$.

В случае характеристики p образ f является подполем поля $\mathbb{K}$, изоморфным $\mathbb{Z}_p$.

В случае характеристики 0 гомоморфизм f инъективен и образ f — подкольцо в $\mathbb{K}$, изоморфное $\mathbb{Z}$. В поле содержатся также обратные ко всем ненулевым элементам, то есть в $\mathbb{K}$ имеют смысл дроби $k \cdot 1/l \cdot 1$, $l \neq 0$, причем две такие дроби $k \cdot 1/l \cdot 1$ и $m \cdot 1/n \cdot 1$ задают один и тот же элемент в $\mathbb{K}$ тогда и только тогда, когда $kn = lm$. (В самом деле,

$$k \cdot 1/l \cdot 1 = m \cdot 1/n \cdot 1 \;\Leftrightarrow\; (k \cdot 1)(n \cdot 1) = (l \cdot 1)(m \cdot 1) \;\Leftrightarrow\; kn = lm).$$

Сложение и умножение таких дробей в поле $\mathbb{K}$ подчиняются обычным правилам действия с дробями. (Например, чтобы сложить $k \cdot 1/l \cdot 1 + m \cdot 1/n \cdot 1$, умножим это выражение на $(ln) \cdot 1$, получим $(kn+lm) \cdot 1$, откуда указанная сумма представляется дробью $(kn + lm) \cdot 1/(ln) \cdot 1)$. Поэтому классы эквивалентности указанных дробей составляют подполе в $\mathbb{K}$, изоморфное $\mathbb{Q}$. ■

Задача 5.52. *Докажите, что группа $\mathbb{Z}$ не изоморфна аддитивной группе никакого векторного пространства.*

Некоторые формулы в полях положительной характеристики имеют особенности, являющиеся следствием соотношения $1 + 1 + \ldots + 1 = 0$. Рассмотрим, например, формулу

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Она справедлива в любом поле, однако в поле характеристики 2 она принимает более простой вид

$$(a+b)^2 = a^2 + b^2.$$

Более общо, в поле характеристики p справедливо тождество

$$(a+b)^p = a^p + b^p,$$

поскольку биномиальные коэффициенты $\binom{p}{k}$ при $k \neq 0$, p делятся на p. Это, в частности, приводит к тому, что для поля $\mathbb{K}$ характеристики p отображение

$$\varphi_p\colon \mathbb{K} \to \mathbb{K}, \quad \varphi_p(x) = x^p$$

является эндоморфизмом (гомоморфизмом на себя) этого поля. φ_p называется *эндоморфизмом Фробениуса* и играет важную роль в теории полей положительной характеристики.

Пусть $\mathbb{F}$ — подполе поля $\mathbb{K}$. Сопоставляя определения, легко видеть, что тогда $\mathbb{K}$ является линейным пространством над полем $\mathbb{F}$ (нужно просто "забыть" про умножение элементов поля $\mathbb{K}$ друг на друга, и оставить только умножение их на элементы подполя $\mathbb{F}$). Например, $\mathbb{C}$ — двумерное линейное пространство над полем $\mathbb{R}$ (в качестве базиса в нем обычно выбирают $\{1, i\}$), а $\mathbb{R}$ и $\mathbb{C}$ — бесконечномерные (точнее, континуальномерные) пространства над полем $\mathbb{Q}$.[27]

Пусть $\mathbb{K}$ — конечное поле. Тогда его характеристика p конечна и оно содержит (поле, изоморфное) $\mathbb{Z}_p$ в качестве подполя. Так как $\mathbb{K}$ конечно, то размерность $\mathbb{K}$ как линейного пространства над $\mathbb{Z}_p$ конечна; пусть она равна n. Тогда можно установить биекцию между элементами $\mathbb{K}$ и столбцами высоты n с элементами из $\mathbb{Z}_p$, откуда $|\mathbb{K}| = p^n$. Тем самым мы доказали

[27] Задачу построить базис в $\mathbb{R}$ над $\mathbb{Q}$ мы читателю не предлагаем:)

Предложение 5.53. *Мощность конечного поля является степенью простого числа (его характеристики).*

На самом деле, для любого простого p и натурального n существует поле из p^n элементов и оно единственно с точностью до изоморфизма. Мы не будем доказывать этот общий результат, ограничившись ниже построением поля из p^2 элементов.

Задача 5.54. *Поля из скольких элементов* 3, 5, 9, 27 *содержатся или могут содержаться в поле из* 81 *элемента?*

Заметим, что аддитивная группа поля из p^n элементов изоморфна $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ (прямая сумма n слагаемых).

Выше мы видели, что конечные подгруппы в $\mathbb{C}^*$ циклические. На самом деле, это общий результат:

Теорема 5.55. *Конечная подгруппа мультипликативной группы $\mathbb{K}^*$ любого поля $\mathbb{K}$ (в частности, мультипликативная группа любого конечного поля) является циклической.*

Доказательство. Доказательству теоремы предпошлём следующую

Лемма 5.56. Пусть H — такая конечная группа порядка n, что для любого $d \mid n$

$$\sharp\{x \in H \mid x^d = 1\} \leq d$$

(здесь $\sharp S$ обозначает мощность множества S). Тогда H — циклическая группа.

Доказательство леммы. Если в H есть элемент x порядка d, то d различных элементов $\{1, x, x^2, \ldots, x^{d-1}\}$ циклической группы $\langle x \rangle$, порожденной x, являются решениями $x^d = 1$, и поэтому в группе H других элементов, удовлетворяющих этому уравнению, нет. Таким образом, в этом случае в H содержится ровно $\phi(d)$ элементов порядка d (сколько образующих в соответствующей циклической группе).

Таким образом, для каждого делителя d порядка группы $n = |H|$ в группе H содержится либо $\phi(d)$ либо 0 элементов порядка d, причем, как мы знаем, порядок любого элемента конечной группы делит порядок группы. Теперь используя Следствие 4.47 получаем, что при сформулированном на группу условии для каждого $d \mid n$ в H существует ровно $\phi(d)$ элементов порядка d, в частности, это верно и для $d = n$. ■

Вернемся к доказательству Теоремы. Пусть $H \subset \mathbb{K}^*$ — конечная подгруппа порядка n. Мы знаем, что число корней многочлена $x^d = 1$ в поле не превосходит d, и тем самым мы попадаем под условие Леммы. ■

Таким образом, $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ и $\mathbb{Z}_p^* = \{1, a, a^2, \ldots, a^{p-2}\}$, где $a \in \mathbb{Z}_p^*$ — образующая. Пусть p — нечетное простое число. Тогда, возводя перечисленные выше элементы a^i в квадрат мы видим, что (ненулевые) квадраты образуют подгруппу индекса 2 в группе $\mathbb{Z}_p^*$. Обозначим ее $(\mathbb{Z}_p^*)^2$.

Например, -1 является квадратом по модулю p (эквивалентно, уравнение $x^2 = -1$ разрешимо в $\mathbb{Z}_p$) тогда и только тогда, когда $p \equiv 1 \bmod 4$. В самом деле, поскольку -1 — единственный элемент порядка 2 в группе $\mathbb{Z}_p^*$, то он является квадратом тогда и только тогда, когда в $\mathbb{Z}_p^*$ есть элемент порядка 4, а в циклической группе порядка $p-1$ есть элемент порядка 4 тогда и только тогда, когда $4 \mid (p-1)$.

Предложение 5.57. *(ср. Задачу 2.21) Пусть элемент $\alpha \in \mathbb{K}^*$ не является квадратом. Тогда множество матриц*

$$\left\{ \begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{K} \right\} \subset \mathrm{Mat}_2(\mathbb{K}) \tag{43}$$

является полем, содержащим $\mathbb{K}$ в качестве подполя и являющегося 2-мерным векторным пространством над $\mathbb{K}$.

Доказательство. Легко проверяется, что указанное подмножество матриц образует коммутативное подкольцо с 1 (при этом удобно использовать представление

$$\begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix} = aE + bF, \quad \text{где} \quad F := \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} \quad \text{и соотношение} \quad F^2 = \alpha E).$$

Оно содержит $\mathbb{K}$ в качестве подполя, если последнее отождествить со скалярными матрицами aE.

Проверим, что любая ненулевая матрица указанного вида обратима:

$$\det \begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix} = a^2 - \alpha b^2,$$

и если $a^2 - \alpha b^2 = 0$, то либо $b = 0$ (и тогда $a = 0$), либо $b \neq 0$ и $(a/b)^2 = \alpha$, но по условию α не является квадратом в $\mathbb{K}$ и значит для a, $b \in \mathbb{K}$ указанное равенство невозможно. ■

Конструкцию из доказанного Предложения можно понимать так: хотя уравнение $x^2 = \alpha$ не разрешимо в $\mathbb{K}$, оно оказывается разрешимым в матрицах указанного вида, поскольку $F^2 = \alpha E$.

Если в предыдущем Предложении положить $\mathbb{K} = \mathbb{R}$ и $\alpha = -1$, то мы получим известное представление поля $\mathbb{C}$ вещественными матрицами порядка 2. (С полем $\mathbb{C}$ в качестве $\mathbb{K}$ такой фокус не проходит, поскольку все элементы поля $\mathbb{C}$ являются квадратами в силу алгебраической замкнутости).

Если для нечетного простого p в предыдущем Предложении положить $\mathbb{K} = \mathbb{Z}_p$ и взять $\alpha \in \mathbb{Z}_p^* \backslash (\mathbb{Z}_p^*)^2$ (например, $\alpha = -1$ при $p \equiv 3 \bmod 4$), то мы получим поле из p^2 элементов.

Замечание 5.58. Если $\alpha \in \mathbb{K}^*$ является квадратом в $\mathbb{K}$, то матрицы вида (43) также будут образовывать подкольцо в $\mathrm{Mat}_2(\mathbb{K})$, но на этот раз содержащее делители нуля (например,

$$\begin{pmatrix} \beta & \alpha \\ 1 & \beta \end{pmatrix} \begin{pmatrix} -\beta & \alpha \\ 1 & -\beta \end{pmatrix} = \begin{pmatrix} -\beta^2 + \alpha & 0 \\ 0 & \alpha - \beta^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

где $\beta \in \mathbb{K}$, $\beta^2 = \alpha$). На самом деле, это — двумерная алгебра над $\mathbb{K}$, изоморфная прямой сумме полей $\mathbb{K} \oplus \mathbb{K}$ (с покомпонентными операциями). Читатель может проверить, что указанный изоморфизм задается сопоставлением

$$\begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix} \mapsto (a + \beta b,\, a - \beta b),$$

где $\beta \in \mathbb{K}$, $\beta^2 = \alpha$.

Задача 5.59. *Убедитесь, что матрицы вида*

$$\left\{ \begin{pmatrix} a & b \\ b & a + b \end{pmatrix} \mid a,\, b \in \mathbb{Z}_2 \right\} \subset \mathrm{Mat}_2(\mathbb{Z}_2)$$

образуют поле из 4-х элементов.

Тем самым для любого простого p мы предъявили поле из p^2 элементов.

6 Начала линейной алгебры

В данной главе определяется понятие размерности линейного пространства (в конечномерном случае), которая является единственным инвариантом изоморфизма линейного пространства. Далее на основе понятия размерности линейного пространства вводится и изучается важное понятие ранга матрицы, а также описывается структура множества решений системы линейных уравнений.

6.1 Базисы и размерность конечномерных линейных пространств

Лемма 6.1. Система векторов $\{v_1, \ldots, v_m\}$ линейного пространства V (см. Определение 1.60) линейно зависима тогда и только тогда, когда (хотя бы) один из ее векторов представляется в виде линейной комбинации остальных.

Доказательство. Пусть система линейно зависима и $\lambda_1 v_1 + \ldots + \lambda_m v_m = 0$ — равная нулю ее нетривиальная линейная комбинация[28]. Пусть $\lambda_k \neq 0$, тогда

$$v_k = -\lambda_k^{-1}(\lambda_1 v_1 + \ldots + \lambda_{k-1} v_{k-1} + \lambda_{k+1} v_{k+1} + \ldots + \lambda_m v_m).$$

Обратно, если $v_k = \lambda_1 v_1 + \ldots + \lambda_{k-1} v_{k-1} + \lambda_{k+1} v_{k+1} + \ldots + \lambda_m v_m$, то собирая все в одной части, получаем равную нулю нетривиальную линейную комбинацию векторов $\{v_1, \ldots, v_m\}$. ■

Заметим, что в предыдущей лемме не утверждается, что из линейной зависимости системы следует, что *любой* ее вектор представляется как линейная комбинация остальных (читателю предлагается привести контрпример к этому утверждению).

Лемма 6.2. Пусть система векторов $\{v_1, \ldots, v_m\}$ линейного пространства V линейно независима. Тогда для $u \in V$ существует представление $u = \sum_{i=1}^m \lambda_i v_i$ тогда и только тогда, когда система $\{v_1, \ldots, v_m, u\}$ линейно зависима.

Доказательство. Доказательство в одну сторону следует из предыдущей леммы.

Обратно, предположим что $\{v_1, \ldots, v_m, u\}$ линейно зависима и $\lambda_1 v_1 + \ldots + \lambda_m v_m + \mu u = 0$ — нетривиальная линейная зависимость. Тогда $\mu \neq 0$, иначе мы получили бы нетривиальную линейную зависимость между векторами системы $\{v_1, \ldots, v_m\}$, что противоречит условию. Таким образом, $u = -\mu^{-1}(\lambda_1 v_1 + \ldots + \lambda_m v_m)$. ■

Лемма 6.3. Пусть $u = \sum_{i=1}^m \lambda_i v_i$; тогда такое разложение единственно тогда и только тогда, когда система $\{v_1, \ldots, v_m\}$ линейно независима.

Доказательство. Если система $\{v_1, \ldots, v_m\}$ линейно зависима и $0 = \sum_{i=1}^m \mu_i v_i$ — нетривиальное разложение по ней нулевого вектора, то прибавляя его к данному разложению вектора u, получаем новое разложение вектора u.

Обратно, если существует два разных разложения вектора u по системе $\{v_1, \ldots, v_m\}$, то, вычитая одно из другого, получаем нетривиальное разложение нулевого вектора по указанной системе, то есть нетривиальную линейную зависимость. ■

[28] Напомним, что линейная комбинация $\lambda_1 v_1 + \ldots + \lambda_m v_m$ называется *нетривиальной*, если хотя бы один из коэффициентов λ_i отличен от нуля. В этой терминологии система векторов $\{v_1, \ldots, v_m\}$ линейно зависима тогда и только тогда, когда существует ее нетривиальная линейная комбинация, равная нулю.

Предложение 6.4. (Основная лемма о линейной зависимости). *Если векторы $u_1, \ldots, u_n$ линейного пространства V линейно выражаются через векторы $v_1, \ldots, v_m$ того же пространства, причем $n > m$, то (какова бы ни была система $\{v_1, \ldots, v_m\}$) система векторов $\{u_1, \ldots, u_n\}$ линейно зависима.*

Доказательство. По условию имеем

$$\begin{aligned} u_1 &= a_{11}v_1 + a_{21}v_2 + \ldots + a_{m1}v_m, \\ u_2 &= a_{12}v_1 + a_{22}v_2 + \ldots + a_{m2}v_m, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_n &= a_{1n}v_1 + a_{2n}v_2 + \ldots + a_{mn}v_m. \end{aligned}$$

Подставляя эти выражения в условие линейной зависимости

$$\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n = 0, \tag{44}$$

получим

$$\lambda_1(a_{11}v_1 + a_{21}v_2 + \ldots + a_{m1}v_m) + \lambda_2(a_{12}v_1 + a_{22}v_2 + \ldots + a_{m2}v_m) + \ldots$$

$$+\lambda_n(a_{1n}v_1 + a_{2n}v_2 + \ldots + a_{mn}v_m) = 0,$$

то есть

$$(a_{11}\lambda_1 + a_{12}\lambda_2 + \ldots + a_{1n}\lambda_n)v_1 + (a_{21}\lambda_1 + a_{22}\lambda_2 + \ldots + a_{2n}\lambda_n)v_2 + \ldots$$

$$+(a_{m1}\lambda_1 + a_{m2}\lambda_2 + \ldots + a_{mn}\lambda_n)v_m = 0.$$

Данное соотношение удовлетворяется при любом решении $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ системы линейных однородных уравнений

$$\begin{cases} a_{11}\lambda_1 + a_{12}\lambda_2 + \ldots + a_{1n}\lambda_n &= 0 \\ a_{21}\lambda_1 + a_{22}\lambda_2 + \ldots + a_{2n}\lambda_n &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}\lambda_1 + a_{m2}\lambda_2 + \ldots + a_{mn}\lambda_n &= 0. \end{cases}$$

Согласно Следствию 2.58, последняя система имеет нетривиальное решение, которое дает нетривиальную линейную зависимость (44). ∎

Замечание 6.5. Вместо ссылки на Следствие 2.58 в конце предыдущего доказательства можно было бы заметить, что утверждение о том, что однородная система, число неизвестных у которой больше числа уравнений, имеет нетривиальное решение, легко следует из результатов раздела 2.3. Действительно, любой столбец упрощенной матрицы является линейной комбинацией ее главных столбцов, но в упрощенном виде матрицы A размера $m \times n$, где $m < n$, есть неглавные столбцы, поэтому по Лемме 6.2 между столбцами такой матрицы A есть нетривиальная линейная зависимость (ср. Лемму 6.1).

Приведем доказательство Предложения 6.4, не использующее результаты теории систем линейных уравнений.

Воспользуемся индукцией по m. При $m = 0$ Предложение верно: через пустую систему векторов линейно выражается только нулевой вектор. Пусть утверждение верно для $m - 1 \geq 0$, докажем что тогда оно справедливо и для m. Пусть $\{u_1, \ldots, u_n\}$ линейно выражаются через $\{v_1, \ldots, v_m\}$, $n > m$. Без ограничения общности можно считать, что вектор v_m входит в разложение u_n с ненулевым коэффициентом. (В самом деле, если v_m не входит в разложение ни одного из векторов $u_1, \ldots, u_n$, то работает предположение индукции; если входит в разложение какого-то вектора u_i но не u_n, то перенумеруем векторы в системе $\{u_1, \ldots, u_n\}$). Тогда существует набор скаляров $\{\alpha_1, \ldots, \alpha_{n-1}\}$ таких, что в разложения векторов $\overline{u}_i := u_i - \alpha_i u_n$ $1 \leq i \leq n-1$ вектор v_m входит с нулевым коэффициентом. Другими словами, система $\{\overline{u}_1, \ldots, \overline{u}_{n-1}\}$ линейно выражается через $\{v_1, \ldots, v_{m-1}\}$. Так как по условию $n > m \geq 1$, то $n-1 > m-1 \geq 0$, и значит по предположению индукции существует нетривиальная линейная зависимость $\lambda_1 \overline{u}_1 + \ldots + \lambda_{n-1}\overline{u}_{n-1} = 0$, то есть $\lambda_1 u_1 + \ldots + \lambda_{n-1} u_{n-1} - (\lambda_1\alpha_1 + \ldots + \lambda_{n-1}\alpha_{n-1})u_n = 0$. ■

Пусть V — векторное пространство, а $S \subset V$ — его произвольное подмножество (не обязательно конечное).

Определение 6.6. *Линейной оболочкой* подмножества $S \subset V$ называется множество всех векторов из V, представимых в виде (конечных!) линейных комбинаций элементов из S. Линейная оболочка обозначается $\langle S \rangle$.

Таким образом, $\langle S \rangle$ состоит из всех векторов из V, представимых в виде $\sum_s \lambda_s s$, $s \in S$, $\lambda_s \in \mathbb{K}$, где $\lambda_s \neq 0$ только для конечного числа $s \in S$. По определению линейная комбинация пустого множества векторов равна нулевому вектору.

Легко видеть, что для произвольного подмножества $S \subset V$ его линейная оболочка не просто подмножество в V, а линейное подпространство. Действительно, во-первых, это множество непусто (например, $\langle \varnothing \rangle = 0$ и, поскольку любое множество S содержит пустое подмножество, любая линейная оболочка содержит нулевой вектор). Во-вторых, сумма двух конечных линейных комбинаций векторов из S снова является конечной линейной комбинацией векторов из S; то же для умножения на скаляр.

Заметим, что для $S \subset V$ $\langle S \rangle = V$ тогда и только тогда, когда S содержит некоторый базис V; в частности, $\langle V \rangle = V$.

Задача 6.7. *Покажите, что $\langle S \rangle$ — наименьшее по включению линейное подпространство в V, содержащее S (то есть любое подпространство $U \subset V$, содержащее S, содержит также и $\langle S \rangle$).*

Говорят, что пространство V *порождается* своим подмножеством $S \subset V$, если $V = \langle S \rangle$.

Определение 6.8. Пространство V называется *конечномерным*, если оно порождается некоторым своим конечным подмножеством.

В дальнейшем мы сосредоточимся почти исключительно на изучении конечномерных векторных пространств.

Заметим, что определение базиса можно переформулировать следующим образом: базис в V — линейно независимая система, порождающая V. Напомним, что, в частности, базис нулевого векторного пространства — пустое множество векторов (которое по определению линейно независимо).

Теорема 6.9. *Из всякого конечного порождающего множества S пространства V можно выбрать базис пространства V.*

Доказательство. Если S линейно независимо, то S (после произвольного упорядочивания) — базис в V. Если S линейно зависимо, то по Лемме 6.1 в S найдется вектор, линейно выражающийся через остальные. Выкидывая его из S получим порождающее множество из меньшего числа элементов. Так как число элементов в произвольном конечном множестве неотрицательно, этот процесс должен оборваться. ∎

Следствие 6.10. *Всякое конечномерное векторное пространство обладает базисом.*

Заметим, что если в векторном пространстве V есть базис из n элементов, то любые $m > n$ векторов из V линейно зависимы по Предложению 6.4.

Теорема 6.11. *Все базисы конечномерного линейного пространства V содержат одно и то же число векторов.*

Доказательство следует из Предложения 6.4. ∎

Таким образом, нами доказана корректность следующего определения.

Определение 6.12. *Размерностью* конечномерного векторного пространства V называется число элементов его произвольного базиса.

Размерность конечномерного векторного пространства — натуральное число (включая 0). Размерность пространства V обозначается $\dim V$.

Пример 6.13. Размерность пространства $\mathbb{K}^n$ столбцов высоты n (или строк длины n) равна n. Стандартный базис $\{e_1, \dots, e_n\}$ образуют в нем столбцы $e_i := (0, \dots, 0, 1, 0, \dots 0)^T$ (единица на i-м месте), $i = 1, \dots, n$.

Задача 6.14. *Докажите, что любая линейно независимая система из n векторов $\{v_1, \dots, v_n\}$ в n-мерном пространстве V является базисом в V.*

Решение. Предположим, что какой-то вектор $v \in V$ не раскладывается по системе $\{v_1, \dots, v_n\}$, тогда система $\{v_1, \dots, v_n, v\}$ линейно независима, что противоречит Предложению 6.4. ∎

Задача 6.15. *Докажите, что любая система из n векторов $\{v_1, \dots, v_n\}$ в n-мерном пространстве V, по которой раскладывается любой вектор $v \in V$, является базисом в V.*

Решение. Предположим, что система $\{v_1, \ldots, v_n\}$ линейно зависима, тогда один из ее векторов является линейной комбинацией остальных, и значит его можно выбросить из системы, сохранив условие разложимости по ней любого вектора. Если полученная система снова линейно зависима, выбрасываем из нее следующий лишний вектор и т.д. В конце концов приходим к линейно независимой системе, порождающей V, которая таким образом является базисом в V, но содержащей менее n векторов. Получили противоречие с Предложением 6.4. ∎

Предложение 6.16. *Пусть $S \subset V$ — произвольное (конечное или бесконечное) подмножество в V, $\dim V = n < \infty$. Тогда любое линейно независимое подмножество T в S можно дополнить до максимального линейно независимого подмножества в S.*

Доказательство. Действительно, если T не максимально среди линейно независимых подмножеств в S, к нему можно добавить новый элемент из S с сохранением условия линейной независимости, причем этот процесс оборвется на конечном шаге, поскольку любые $m > n$ векторов в V линейно зависимы (по Предложению 6.4). ∎

Применяя приведенное в доказательстве предыдущего Предложения рассуждение к $\varnothing \subset S$ получаем, что в любом подмножестве $S \subset V$ содержится максимальное линейно независимое подмножество.

Предложение 6.17. *Любое максимальное линейно независимое подмножество $\{e_1, \ldots, e_k\}$ в S является базисом в линейной оболочке $\langle S \rangle$.*

Доказательство. Так как по условию $\{e_1, \ldots, e_k\}$ — линейно независимая система векторов из $\langle S \rangle$, достаточно показать, что она порождает указанную линейную оболочку. По определению линейной оболочки, любой вектор из $\langle S \rangle$ является линейной комбинацией векторов из S, поэтому достаточно проверить, что любой вектор из S является линейной комбинацией векторов из $\{e_1, \ldots, e_k\}$, а это следует (с учетом максимальности) из Леммы 6.2. ∎

В частности, все максимальные линейно независимые подмножества в S состоят из одинакового количества элементов.

Мы видим, что произвольный базис в линейном пространстве может быть охарактеризован либо как максимальная (по включению) линейно независимая система, либо как минимальная (тоже по включению) порождающая система. То есть максимальная линейно независимая система автоматически является порождающей, а минимальная порождающая — линейно независимой.

Теорема 6.18. *Всякую линейно независимую систему векторов конечномерного векторного пространства V можно дополнить до базиса в V.*

Доказательство. Возьмем $S = V$ и, применив к нему Предложение 6.16, дополним данную в условии систему до максимальной линейно независимой системы. Согласно Предложению 6.17, она будет базисом в $\langle V \rangle = V$.

Менее формально: всякую линейно независимую систему векторов конечномерного пространства V можно дополнить до максимальной линейно независимой системы, которая, очевидно (см. Лемму 6.2), будет базисом V. ∎

Теорема 6.19. (Свойство монотонности размерности). *Если U — линейное подпространство в V, то $\dim U \leq \dim V$, причем если $\dim U = \dim V$, то $U = V$.*

Доказательство. Пусть $\{e_1, \ldots, e_k\}$ — максимальное линейно независимое подмножество в U. По Предложению 6.17 это — базис в U. Данная система линейно независима и как система векторов из V[29], поэтому по Теореме 6.18 $\dim V \geq k = \dim U$.

Если при этом $U \neq V$, то существует $v \in V$, который не раскладывается по линейно независимой системе $\{e_1, \ldots, e_k\}$, а значит по Лемме 6.2 система векторов $\{e_1, \ldots, e_k, v\}$ пространства V линейно независима, откуда с учетом Теоремы 6.18 получаем, что $\dim V > k = \dim U$. ∎

Дадим еще одно доказательство Теоремы 6.11, не опирающееся на факты из теории СЛУ. В его основе лежит следующая Лемма Штайница, представляющая независимый интерес.

Лемма 6.20. Пусть система векторов $\{u_1, \ldots, u_n\}$ порождает пространство V, а система $\{v_1, \ldots, v_m\}$ векторов из V линейно независима. Тогда $n \geq m$.

Доказательство. Так как $v_1 \in V = \langle u_1, \ldots, u_n \rangle$, то $v_1 = \alpha_1 u_1 + \ldots + \alpha_n u_n$ для некоторых $\alpha_i \in \mathbb{K}$, причем среди α_i обязательно есть коэффициент не равный нулю. Без ограничения общности можно считать, что $\alpha_1 \neq 0$ (в противном случае переупорядочим систему $\{u_1, \ldots, u_n\}$). Тогда $u_1 = \frac{1}{\alpha_1}(v_1 - \alpha_2 u_2 - \ldots - \alpha_n u_n)$ и значит $V = \langle v_1, u_2, \ldots, u_n \rangle$.

Далее, $v_2 = \beta_1 v_1 + \beta_2 u_2 + \ldots + \beta_n u_n$ для некоторых $\beta_i \in \mathbb{K}$, причем среди $\beta_2, \ldots, \beta_n$ есть ненулевой коэффициент (в противном случае векторы v_1, v_2 оказались бы линейно зависимыми). Без ограничения общности можно считать, что $\beta_2 \neq 0$ (в противном случае переупорядочим систему $\{u_2, \ldots, u_n\}$). Тогда u_2 лежит в линейной оболочке $\langle v_1, v_2, u_3, \ldots, u_n \rangle$, которая тем самым совпадает с V.

Шаг индукции: пусть система $\{v_1, \ldots, v_k, u_{k+1}, \ldots, u_n\}$ порождает V. Тогда $v_{k+1} = \gamma_1 v_1 + \ldots + \gamma_k v_k + \gamma_{k+1} u_{k+1} + \ldots + \gamma_n u_n$ для некоторых $\gamma_i \in \mathbb{K}$. Среди $\gamma_{k+1}, \ldots, \gamma_n$ обязательно есть ненулевой коэффициент: в противном случае система $\{v_1, \ldots, v_m\}$ оказалась бы линейно зависимой вопреки предположению. В случае необходимости меняя порядок у $u_{k+1}, \ldots, u_n$, можно считать, что $\gamma_{k+1} \neq 0$. Тогда u_{k+1} лежит в $\langle v_1, \ldots, v_{k+1}, u_{k+2}, \ldots u_n \rangle$, и тогда $\langle v_1, \ldots, v_k, u_{k+1}, \ldots, u_n \rangle \subseteq \langle v_1, \ldots, v_{k+1}, u_{k+2}, \ldots u_n \rangle$, а значит последняя линейная оболочка совпадает с V и шаг индукции доказан.

В конце концов приходим к следующей альтернативе: если в противоречии с условием $n < m$, то $V = \langle v_1, \ldots, v_n \rangle$, что противоречит линейной независимости системы $\{v_1, \ldots, v_m\}$ (поскольку в этом случае векторы $v_{n+1}, \ldots, v_m$ являются линейными комбинациями векторов $v_1, \ldots, v_n$). Таким образом, $n \geq m$ (и $V = \langle v_1, \ldots, v_m, u'_{m+1}, \ldots, u'_n \rangle$, где $u'_{m+1}, \ldots, u'_n$ — некоторые из векторов системы $\{u_1, \ldots, u_n\}$). ∎

Теорема 6.11 является непосредственным следствием Леммы Штайница, так как каждый базис является одновременно и порождающей, и линейно независимой системой.

[29] так как операции сложения и умножения на скаляр в подпространстве $U \subset V$ получаются ограничением соответствующих операций в пространстве V.

6.2 Ранг матрицы

Определение 6.21. *Рангом* системы векторов $\{a_1, \ldots, a_k\}$ векторного пространства V называется размерность ее линейной оболочки $\langle a_1, \ldots, a_k \rangle$. *Рангом матрицы* называется ранг системы ее строк (рассматриваемых как векторы пространства строк соответствующей длины). Ранг матрицы A обозначается $\operatorname{rk} A$.

Поясним вторую часть предыдущего определения. Пусть A — матрица размера $m \times n$. Тогда ее строки являются векторами арифметического линейного пространства $\mathbb{K}^n$ и порождают в нем подпространство некоторой размерности $r \leq \min\{m, n\}$. Это число и называется рангом матрицы A.

Заметим, что согласно Предложению 6.17 любая максимальная линейно независимая система строк матрицы A является базисом в линейной оболочке ее строк, поэтому называется также *базисной системой строк*. В частности, любая строка матрицы A является линейной комбинацией строк базисной системы и все такие системы состоят из одинакового числа строк. Кроме того, из Предложения 6.16 следует, что любую линейно независимую систему строк матрицы можно дополнить до базисной системы строк.

Из определения размерности следует, что ранг матрицы равен мощности ее базисной системы строк.

Замечание 6.22. В обозначениях предыдущего параграфа множество S строк матрицы A является конечным порождающим множеством своей линейной оболочки $\langle S \rangle \subset \mathbb{K}^n$. Используя результаты предыдущего параграфа легко видеть, что (некоторую) базисную систему строк матрицы A (и значит ее ранг) теоретически можно искать следующими двумя алгоритмами.

1. Если матрица A нулевая, ее система базисных строк пуста, а ранг равен нулю. Пусть $A \neq 0$, значит у нее есть ненулевая строка a_i. Если все остальные строки ей пропорциональны, то ранг A равен 1 и система, состоящая из a_i — базисная. В противном случае есть (хотя бы одна) непропорциональная ей строка, добавляя любую такую строку a_j к a_i, получаем линейно независимую систему из двух строк $\{a_1, a_2\}$, и таким образом $\operatorname{rk} A \geq 2$. Если все строки линейно выражаются через выбранные две, то $\{a_1, a_2\}$ — уже базисная система строк, в противном случае добавляем к ним произвольную линейно независимую от выбранных двух третью строку a_k и т.д. В конце концов мы придем к максимальной линейно независимой системе строк. То есть в этом случае мы добавляем к данной линейно независимой системе строк новые строки с сохранением условия линейной независимости, пока это возможно. На последнем шаге мы получаем максимальную линейно независимую систему, которая также будет порождающей (для линейной оболочки строк).

2. Можно также рассуждать в противоположном направлении — не добавляя новые строки к уже имеющимся линейно независимым, а наоборот, выбрасывая линейно зависимые. Более подробно: если система из всех m строк матрицы A линейно независима, то $\operatorname{rk} A = m$. В противном случае какая-то из строк линейно выражается через остальные,

выбросим ее из системы. Получим систему из $m-1$ строки; если она линейно независима, то $\operatorname{rk} A = m-1$; в противном случае выбросим какую-то из строк, которая выражается через остальные $m-2$, получим систему из $m-2$ строк и т.д. Продолжая этот процесс, мы придем к линейно независимой системе строк (возможно, пустой, если матрица A нулевая), которая будет базисной системой строк. То есть в данном случае мы выбрасываем из данной порождающей системы строк лишние с сохранением условия порождаемости, пока это возможно. На последнем шаге мы получаем минимальную порождающую систему, которая будет также линейно независимой.

Задача 6.23. *Докажите, что произвольную матрицу ранга* 1 *можно представить в виде произведения столбца на строку.*

Задача 6.24. *Докажите, что произвольную матрицу ранга r можно представить в виде суммы r матриц ранга* 1*, но нельзя в виде суммы меньшего их числа.*

Задача 6.25. *Что может произойти с рангом матрицы при добавлении к ней дополнительной строки?*

Две системы $\{a_1, \ldots, a_n\}$ и $\{b_1, \ldots, b_m\}$ векторов одного векторного пространства V назовем *эквивалентными*, если каждый вектор второй системы b_j линейно выражается через векторы первой системы a_i, и наоборот. Очевидно, что

$$\{a_1, \ldots, a_n\} \sim \{b_1, \ldots, b_m\} \quad \Leftrightarrow \quad \langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_m\rangle.$$

Отсюда, в частности, следует, что *ранги эквивалентных систем равны.*

При элементарном преобразовании (любого из трех типов) строк матрицы система ее строк заменяется на эквивалентную. Поэтому ранг матрицы не меняется при элементарных преобразованиях ее строк. (Другими словами, ранг — функция, постоянная на классах строчно эквивалентных матриц). С другой стороны, любую матрицу с помощью элементарных преобразований строк можно привести к ступенчатому виду. Поэтому для вычисления рангов матриц достаточно научиться считать ранги ступенчатых матриц.

Предложение 6.26. *Ранг ступенчатой матрицы равен числу ее ненулевых строк.*

Доказательство. Для нулевой матрицы утверждение очевидно. Покажем, что ненулевые строки ненулевой ступенчатой матрицы линейно независимы. Пусть некоторая их линейная комбинация равна нулю (=нулевой строке). Рассматривая ведущий элемент $a_{1j_1} \neq 0$ первой строки получаем, что первая ненулевая строка входит в линейную комбинацию с нулевым коэффициентом (иначе в линейной комбинации элемент на j_1-м месте был бы отличен от нуля). Рассуждая дальше по индукции, получаем требуемое. Утверждение Предложения теперь следует из того, что добавление нулевых векторов к системе не меняет ее ранга. ■

В частности, число ненулевых строк одинаково для всех ступенчатых матриц, которые можно получить из данной матрицы с помощью элементарных преобразований строк.

Помимо приведенного выше определения ранга матрицы как размерности линейной оболочки ее строк, можно определить *столбцовый ранг* матрицы как размерность линейной оболочки ее столбцов. Аналогично определяется понятие *базисной системы столбцов*.

Предложение 6.27. *Столбцовый ранг матрицы не меняется при элементарных преобразованиях ее строк. Более того, при элементарных преобразованиях строк базисная система столбцов переходит в базисную систему столбцов (с теми же номерами).*

Доказательство. Очевидно, что первое утверждение из формулировки следует из второго, которое мы и докажем. Пусть A' — матрица, полученная из A элементарными преобразованиями строк. Согласно Следствию 2.38, элементарные преобразования строк матрицы не изменяют линейные зависимости между ее столбцами. Значит, столбцы с номерами $j_1, \ldots, j_r$ образуют максимальную линейно независимую систему столбцов матрицы A тогда и только тогда, когда то же верно для матрицы A'.

Более подробно, пусть столбцы с номерами $j_1, \ldots, j_r$ образуют максимальную линейно независимую систему столбцов матрицы A. Если бы столбцы с номерами $j_1, \ldots, j_r$ матрицы A' оказались линейно зависимы, то, так как (в силу обратимости элементарных преобразований) матрица A получается из A' элементарными преобразованиями строк, столбцы матрицы A с теми же номерами оказались бы связаны той же нетривиальной линейной зависимостью, а это не так по условию. Если бы система столбцов матрицы A' с номерами $j_1, \ldots, j_r$ оказалась бы немаксимальной среди линейно независимых систем, то при добавлении некоторого столбца (скажем, с номером j_{r+1}) матрицы A', не входящего в указанную систему, мы снова получили бы линейно независимую систему. С другой стороны, по условию система столбцов матрицы A с номерами $j_1, \ldots, j_r, j_{r+1}$ линейно зависима, и нетривиальная линейная зависимость между ними должна перейти в аналогичную нетривиальную линейную зависимость между соответствующими столбцами матрицы A' — противоречие с немаксимальностью системы столбцов матрицы A' с номерами $j_1, \ldots, j_r$. ∎

Теорема 6.28. ("о ранге матрицы"). *Строчный и столбцовый ранги матрицы равны.*

Доказательство. Временно обозначим $\widetilde{\mathrm{rk}}\, A$ столбцовый ранг матрицы A. Итак, пусть A — произвольная матрица. Пусть $r = \mathrm{rk}\, A$. Приведем ее к упрощенному виду с помощью элементарных преобразований строк. При этом строчный и столбцовый ранги не меняются. У полученной матрицы r ненулевых строк и r главных столбцов. Поскольку главные столбцы являются столбцами единичной матрицы порядка r с (возможно) дописанными внизу нулями, они линейно независимы. Отсюда следует, что для произвольной матрицы столбцовый ранг не меньше чем строчный, то есть $\widetilde{\mathrm{rk}}\, A \geq \mathrm{rk}\, A$. Другими словами,

при транспонировании матрицы (строчный) ранг не уменьшается. Если он увеличился, то транспонируя матрицу еще раз, получаем противоречие. ■

Таким образом, для любой матрицы A верно равенство $\operatorname{rk} A = \operatorname{rk} A^T$.

Из доказательства предыдущей Теоремы следует, что главные столбцы ступенчатой матрицы образуют максимальную линейно независимую систему ее столбцов. Этот факт вместе со Следствием 2.38 служит обоснованием следующего алгоритма нахождения базисной системы столбцов произвольной матрицы A. А именно, приведем матрицу A к ступенчатому виду с помощью элементарных преобразований строк, пусть главные столбцы полученной ступенчатой матрицы имеют номера $j_1, \ldots, j_r$, тогда столбцы матрицы A с теми же номерами образуют максимальную линейно независимую систему ее столбцов.

Теорема 6.29. *Ранг произведения матриц (когда оно определено) не превосходит ранга каждого из сомножителей.*

Доказательство. Пусть $C := AB$. Согласно Предложению 2.7 i-й столбец матрицы C является линейной комбинацией столбцов матрицы A с коэффициентами из i-го столбца матрицы B, поэтому линейная оболочка столбцов матрицы C содержится в линейной оболочке столбцов матрицы A, а значит $\operatorname{rk} C \leq \operatorname{rk} A$ (см. Теорему 6.19). Далее, то же Предложение показывает, что линейная оболочка строк матрицы C содержится в линейной оболочке строк матрицы B, откуда $\operatorname{rk} C \leq \operatorname{rk} B$. ■

Обобщим теперь Задачу 6.23.

Задача 6.30. *Докажите, что произвольную матрицу C размера $m \times n$ и ранга r можно представить в виде произведения AB, где A — матрица размера $m \times r$, а B — размера $r \times n$. Существует ли аналогичное представление в виде произведения матриц размеров $m \times s$ и $s \times n$, где $s < r$?*

Решение. Составим матрицу A из (некоторой системы) базисных столбцов матрицы C. Напомним, что i-й столбец матрицы AB есть линейная комбинация столбцов матрицы A с коэффициентами из i-го столбца матрицы B. Таким образом, i-й столбец B нужно составить из коэффициентов разложения i-го столбца C по выбранной системе базисных столбцов.

Другой способ: существуют последовательности элементарных преобразований строк и столбцов, приводящие матрицу C к блочному виду $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$, где E_r — единичная матрица порядка r. То есть существуют невырожденные матрицы S, T порядков m и n такие, что $C = S \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} T$. С другой стороны, $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} E_r \\ 0 \end{pmatrix} \begin{pmatrix} E_r & 0 \end{pmatrix}$, откуда все следует.

Ответ на вопрос отрицательный, так как существование такого представления противоречило бы Теореме 6.29. ■

Задача 6.31. *Пусть A — невырожденная матрица порядка n. Тогда для любой матрицы B, для которой существует произведение AB, верно равенство* $\operatorname{rk}(AB) = \operatorname{rk} B$. *Аналогично для невырожденной матрицы B.*

Решение. Так как матрица A невырождена, то она строчно эквивалентна единичной E. То есть существует конечный набор элементарных матриц $S_1, \ldots, S_p$ такой, что $S_p \ldots S_1 A = E$ (тогда, как мы знаем, $S_p \ldots S_1 = A^{-1}$). Равенство $S_p \ldots S_1 AB = B$ показывает, что та же последовательность элементарных преобразований строк, которая матрицу A приводит к единичной E, приводит матрицу AB к B. При элементарных преобразованиях строк ранг матрицы не меняется, поэтому $\operatorname{rk}(AB) = \operatorname{rk} B$. ∎

Задача 6.32. *Пусть A — матрица с линейно независимыми столбцами. Тогда для любой матрицы B, для которой существует произведение AB, верно равенство* $\operatorname{rk}(AB) = \operatorname{rk} B$. *Аналогично для матрицы B с линейно независимыми строками.*

Решение. 1-й способ является обобщением решения предыдущей задачи. Пусть матрица A имеет размер $m \times n$, из условия следует, что $m \geq n$. Если $m = n$ то матрица A невырождена и мы возвращаемся к условию предыдущей задачи. Если $m > n$, то матрица A элементарными преобразованиями строк приводится к виду $A' := \begin{pmatrix} E \\ 0 \end{pmatrix}$, где E — единичная матрица порядка n, а 0 — нулевая матрица размера $(m-n) \times n$. Поэтому $\operatorname{rk}(AB) = \operatorname{rk}(A'B)$. С другой стороны,

$$\begin{pmatrix} E \\ 0 \end{pmatrix} B = \begin{pmatrix} B \\ 0 \end{pmatrix},$$

а ранг последней матрицы, очевидно, равен $\operatorname{rk} B$.

2-й способ. Пусть $C := AB$. Используя идею из доказательства Теоремы 6.29 мы видим, что столбцы матрицы B — координатные столбцы столбцов матрицы C в базисе (соответствующей линейной оболочки), образованном столбцами матрицы A. Теперь требуемое следует из того, что ранг произвольной системы векторов равен рангу системы из их координатных столбцов в произвольном базисе. ∎

Теорема 6.33. *Ранг суммы матриц не превосходит суммы их рангов.*

Доказательство. Приведем два доказательства. Первое следует из цепочки более-менее очевидных (не)равенств:

$$\operatorname{rk}(A+B) \leq \operatorname{rk} \begin{pmatrix} A+B \\ B \end{pmatrix} = \operatorname{rk} \begin{pmatrix} A \\ B \end{pmatrix} \leq \operatorname{rk} A + \operatorname{rk} B$$

(читателю предлагается детально обдумать каждый шаг). Второе — геометрическое — доказательство изложим более подробно. Пусть $\{u_1, \ldots, u_m\}$ и $\{v_1, \ldots, v_m\}$ — две системы векторов некоторого линейного пространства (в нашем случае в качестве указанных

векторов выступают строки матриц A и B). Ясно, что имеет место включение линейных оболочек

$$\langle u_1 + v_1, \ldots, u_m + v_m \rangle \subseteq \langle u_1, \ldots, u_m, v_1, \ldots, v_m \rangle.$$

По Теореме 6.19 $\dim \langle u_1 + v_1, \ldots, u_m + v_m \rangle \leq \dim \langle u_1, \ldots, u_m, v_1, \ldots, v_m \rangle$. Кроме того, верно неравенство

$$\dim \langle u_1, \ldots, u_m, v_1, \ldots, v_m \rangle \leq \dim \langle u_1, \ldots, u_m \rangle + \dim \langle v_1, \ldots, v_m \rangle.$$

Действительно, объединение максимальных линейно независимых подмножеств (то есть базисов) линейных оболочек $\langle u_1, \ldots, u_m \rangle$ и $\langle v_1, \ldots, v_m \rangle$ порождает линейную оболочку $\langle u_1, \ldots, u_m, v_1, \ldots, v_m \rangle$. По Теореме 6.9 это множество содержит некоторый базис последней линейной оболочки, откуда следует требуемое. ■

Легко привести пример, когда в предыдущей теореме имеет место равенство.

Очевидно, что матрица A порядка n невырождена $\Leftrightarrow \operatorname{rk} A = n$.

Пусть A — невырожденная матрица порядка n. Это означает, что ее столбцы образуют базис в пространстве $\mathbb{K}^n$ столбцов высоты n. Значит, для любого столбца $\mathbf{c} \in \mathbb{K}^n$ существует единственный столбец $\mathbf{b} \in \mathbb{K}^n$ такой, что $A\mathbf{b} = \mathbf{c}$ (ср. Предложение 2.7). То есть квадратная СЛУ $A\mathbf{x} = \mathbf{c}$ с невырожденной матрицей A разрешима для любого столбца $\mathbf{c}$ и для любого $\mathbf{c}$ имеет единственное решение (нам это уже известно, см. Теорему 3.44). Беря в качестве $\mathbf{c}$ столбцы единичной матрицы $e_1, \ldots, e_n$ получим систему столбцов $\mathbf{b}_1, \ldots \mathbf{b}_n$ такую, что $A(\mathbf{b}_1 \ldots \mathbf{b}_n) = E$, то есть $AB = E$, $B := (\mathbf{b}_1 \ldots \mathbf{b}_n)$. Из Теоремы 6.29 следует, что матрица B также невырождена. Применяя к ней аналогичные соображения, найдем для нее матрицу C такую, что $BC = E$. Теперь имеем $A = A(BC) = (AB)C = C$, то есть B является обратной для A. Таким образом, мы еще раз доказали, что невырожденная матрица имеет обратную. Необходимость следует из Теоремы 6.29, поскольку единичная матрица, очевидно, невырождена.

Заметим, что нами фактически доказано следующее утверждение: для квадратной матрицы A любая матрица B, удовлетворяющая одному из уравнений $AB = E$ или $BA = E$, является обратной (то есть автоматически удовлетворяет и второму из уравнений).

Таким образом, для матриц порядка n условия $\operatorname{rk} A = n$, $\det A \neq 0$ и существования обратной равносильны, поскольку все они эквивалентны невырожденности.

Задача 6.34. *Правой обратной для (вообще говоря, прямоугольной) матрицы A с m строками называется такая матрица B, что $AB = E$ (где E — единичная матрица порядка m). Найдите критерий*

a) существования;

b) существования и единственности

правой обратной матрицы. Те же вопросы для левой обратной матрицы.

Какая связь между понятиями ранга и определителя в общем случае?

Напомним, что минором матрицы называется определитель ее квадратной подматрицы, а его порядком — порядок соответствующей подматрицы.

Теорема 6.35. *Ранг матрицы равен наибольшему порядку ее миноров, отличных от нуля.*

Доказательство. Пусть A — матрица размера $m \times n$ и ранга r, $r \leq \min\{m, n\}$. Покажем, что для любого $s > r$, $s \leq \min\{m, n\}$ все миноры порядка s матрицы A равны нулю. Действительно, любые s строк матрицы A линейно зависимы, тем более линейно зависимы их пересечения с произвольными s столбцами. Следовательно, любая подматрица порядка s матрицы A вырождена, значит, ее определитель равен нулю.

С другой стороны, в матрице A ранга r найдется ненулевой минор порядка r. Действительно, поскольку $\operatorname{rk} A = r$, в матрице A есть система из r линейно независимых строк. Последние образуют подматрицу ранга r, и значит среди ее столбцов тоже найдется r линейно независимых. Квадратная подматрица в A порядка r, образованная выбранными строками и столбцами матрицы A, невырождена, и значит ее определитель — соответствующий минор матрицы A — отличен от нуля. ∎

Пусть A — матрица ранга r. Любая ее невырожденная подматрица порядка r называется *базисной подматрицей* матрицы A, а определитель базисной подматрицы — *базисным минором* матрицы A. Согласно доказанной Теореме, r — максимальный порядок невырожденных подматриц (ненулевых миноров) матрицы A. Название “базисный” оправдывает следующее утверждение.

Следствие 6.36. (“о базисном миноре”). *Строки матрицы A, в которых содержится ее произвольная базисная подматрица, образуют базисную систему строк матрицы A. То же верно и для столбцов.*

Доказательство. Так как базисная подматрица невырождена, ее строки линейно независимы. Тем более независимы строки матрицы A, которые их содержат. Таким образом, данные строки образуют систему из r (где $r = \operatorname{rk} A$) линейно независимых строк матрицы A. Теперь требуемое утверждение следует из того, что любые r линейно независимых векторов в r-мерном пространстве образуют базис (см. Задачу 6.14). ∎

Следующая задача усиливает предыдущую Теорему.

Задача 6.37. *Если в матрице A есть ненулевой минор порядка r, а все миноры порядка $r+1$, получаемые приписыванием к нему одной строки и одного столбца (так называемые окаймляющие миноры), равны нулю, то* $\operatorname{rk} A = r$.

Решение. Пусть, напротив, $\operatorname{rk} A \geq r + 1$. Мы знаем, что всякую линейно независимую систему строк матрицы A можно дополнить до максимальной линейно независимой системы, которая является базисом в линейной оболочке строк матрицы A. Используя это, дополним систему r линейно независимых строк

матрицы A, на пересечении которых стоит ненулевой минор порядка r, до линейно независимой системы из $r+1$ строки. Последние образуют подматрицу в A ранга $r+1$ и ее столбцы, отвечающие ненулевому минору порядка r, линейно независимы. Снова используя сформулированный результат (для столбцов), получим, что набор из данных r линейно независимых столбцов можно продолжить до аналогичного набора из $r+1$ столбца. Подводя итог, мы видим, что если $\operatorname{rk} A \geq r+1$, то для данного ненулевого минора порядка r найдется ненулевой окаймляющий минор порядка $r+1$. ■

Задача 6.38. *В матрице A ранга r любой минор порядка r, образуемый пересечением r линейно независимых строк с r линейно независимыми столбцами, отличен от нуля.*

Решение. r линейно независимых строк в матрице A ранга r являются базисными, то есть каждая из остальных строк — их линейная комбинация. Вычитая из небазисных строк линейные комбинации базисных, которые им равны, получаем матрицу A', в которой все базисные строки остались без изменения, а небазисные заменились нулевыми. Поскольку при этом используются только элементарные преобразования строк (типа I), то $\operatorname{rk} A = \operatorname{rk} A'$. Кроме того, линейные зависимости между столбцами при этом также не изменились, и значит r столбцов матрицы A' с теми же номерами, что r линейно независимых столбцов из формулировки Теоремы, останутся линейно независимыми. По теореме 6.35 в подматрице матрицы A', образованной этими r линейно независимыми столбцами, должен быть ненулевой минор порядка r, которым может быть только минор, образованный пересечением данной системы столбцов с исходной системой из r линейно независимых строк, который совпадает с соответствующим минором матрицы A. ■

Заметим, что в предыдущей задаче условие равенства числа строк и столбцов рангу существенно. Например, в единичной матрице порядка 2 на пересечении 1-й строки и 2-го столбца стоит нулевая подматрица.

6.3 Системы линейных уравнений III

С использованием понятия ранга матрицы мы можем дать общепринятые формулировки результатов о системах линейных уравнений, доказанных в разделе 2.7. Кроме того, мы ответим на вопросы, сформулированные в конце указанного раздела.

Теорема 6.39. (Теорема Кро́некера-Капелли). *Система линейных уравнений совместна тогда и только тогда, когда ранг расширенной матрицы системы равен рангу матрицы коэффициентов.*

Доказательство. Действительно, в обозначениях раздела 2.7 это условие $\tilde{r} = r$. ■

Заметим, что доказанная теорема очевидна и без приведения к ступенчатому виду. Действительно, условие, что ранг расширенной матрицы равен рангу матрицы коэффициентов в точности означает, что столбец правых частей принадлежит линейной оболочке столбцов матрицы коэффициентов, то есть является линейной комбинацией указанных столбцов, а как мы знаем, коэффициенты такой линейной комбинации образуют решение.

Теорема 6.40. *Совместная система линейных уравнений является определенной тогда и только тогда, когда ранг ее матрицы коэффициентов равен числу неизвестных.*

Доказательство. Действительно, в обозначениях раздела 2.7 это условие $r = n$ (в предположении $\tilde{r} = r$). ■

Опять же, доказанная теорема очевидна без приведения к ступенчатому виду. Действительно, ранг матрицы коэффициентов системы равен числу неизвестных в точности тогда, когда столбцы матрицы коэффициентов линейно независимы, далее можно воспользоваться Леммой 6.3.

Следующая простая и фундаментальная теорема показывает, какие подмножества в пространстве столбцов $\mathbb{K}^n$ могут быть множествами решений СЛУ и, в частности, СЛОУ, и играет исключительно важную роль в теории систем линейных уравнений (причем не только алгебраических, но и дифференциальных). Читателю предлагается продумать ее геометрический смысл, используя результаты аналитической геометрии.

Теорема 6.41. *1) Множество решений СЛОУ $Ax = 0$ от n неизвестных является линейным подпространством в пространстве столбцов $\mathbb{K}^n$.*

2) Зафиксируем некоторое решение x_0 совместной СЛУ $Ax = b$. Тогда всякое ее решение представляется в виде $x_0 + y$, где y — некоторое решение $Ax = 0$. И обратно, любая такая сумма — решение $Ax = b$.

Утверждение второй части теоремы кратко формулируют так: *"общее решение совместной неоднородной системы является суммой ее частного решения и общего решения соответствующей однородной системы"*.

Доказательство. 1) Нулевой столбец (нулевой вектор в $\mathbb{K}^n$) является решением СЛОУ. Далее непосредственно проверяется, что для двух решений СЛОУ их сумма также будет ее решением, а также что вместе с каждым решением его произведение на скаляр тоже будет решением. Ясно, что все эти утверждения достаточно проверить для одного однородного уравнения $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$.

2) Пусть x_1 — еще одно решение неоднородной системы. Тогда разность $x_1 - x_0$ является решением однородной системы. В самом деле, $A(x_1 - x_0) = Ax_1 - Ax_0 = b - b = 0$. Обозначая его y, получаем $x_1 = x_0 + y$. Наоборот, $A(x_0 + y) = Ax_0 + Ay = b + 0 = b$, то есть всякая такая сумма является решением неоднородной системы. ■

Раз пространство $U = U_A$ решений СЛОУ $Ax = 0$ от n неизвестных является линейным подпространством в $\mathbb{K}^n$, то $0 \leq \dim U \leq n$. Легко привести примеры систем для каждого возможного значения размерности. От каких характеристик СЛОУ (ее матрицы коэффициентов) зависит размерность пространства решений? Интуиция подсказывает, что каждое независимое уравнение системы уменьшает размерность пространства решений на единицу. То есть пространство решений пустой системы от n неизвестных есть все

$\mathbb{K}^n$, системы, состоящей из одного ненулевого уравнения является $n-1$-мерным подпространством в $\mathbb{K}^n$, из двух независимых уравнений — $n-2$-мерным подпространством и т.д. Очевидно, что формализацией понятия "система из независимых уравнений" является условие, что строки матрицы коэффициентов системы линейно независимы, то есть ранг указанной матрицы равен числу ее строк (=числу уравнений системы).

Теорема 6.42. *Размерность пространства решений СЛОУ $Ax = 0$ от n неизвестных равна $n - \operatorname{rk} A$.*

Доказательство. Элементарными преобразованиями строк приведем матрицу A к упрощенному виду; если в нем есть нулевые строки, отбросим их, и обозначим полученную матрицу A'. При этом класс эквивалентности системы не изменился (то есть системы $A'x = 0$ и $Ax = 0$ задают одно и то же подпространство в $\mathbb{K}^n$). Главные столбцы матрицы A', которые являются столбцами коэффициентов перед главными неизвестными, образуют единичную матрицу. Например, если главные неизвестные идут подряд (это наиболее частый случай; общий случай сводится к этому переименованием переменных), то $A' = (E_r\ C)$, где $C = (c_{ij})$ — некоторая матрица размера $r \times (n-r)$. Перенося слагаемые со свободными неизвестными в правую часть, мы получаем выражение главных неизвестных через свободные

$$\begin{cases} x_1 &= -c_{11}x_{r+1} - c_{12}x_{r+2} - \ldots - c_{1\,n-r}x_n \\ x_2 &= -c_{21}x_{r+1} - c_{22}x_{r+2} - \ldots - c_{2\,n-r}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r &= -c_{r1}x_{r+1} - c_{r2}x_{r+2} - \ldots - c_{r\,n-r}x_n. \end{cases} \tag{45}$$

Последовательно присваивая одной из свободных неизвестных $x_{r+1}, x_{r+2}, \ldots, x_n$ значение 1, а остальным — 0, получаем следующий набор решений

$$\begin{gathered} u_1 := (-c_{11}, -c_{21}, \ldots, -c_{r1}, 1, 0, \ldots, 0)^T, \\ u_2 := (-c_{12}, -c_{22}, \ldots, -c_{r2}, 0, 1, \ldots, 0)^T, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_{n-r} := (-c_{1\,n-r}, -c_{2\,n-r}, \ldots, -c_{r\,n-r}, 0, 0, \ldots, 1)^T. \end{gathered}$$

Полезно заметить, что указанные столбцы являются столбцами матрицы $\begin{pmatrix} -C \\ E_{n-r} \end{pmatrix}$, где E_{n-r} — единичная матрица порядка $n-r$.

Покажем, что полученные решения образуют базис в пространстве решений, отсюда и будет следовать теорема. Действительно, выписанные столбцы линейно независимы, так как составленная из них матрица имеет единичную подматрицу порядка $n-r$ и, значит, ее ранг не меньше $n-r$. С другой стороны, каждое решение системы $A'x = 0$ однозначно определяется (по формулам (45)) значениями свободных неизвестных, а для любых

$\lambda_1, \lambda_2, \ldots, \lambda_{n-r} \in \mathbb{K}$ линейная комбинация $\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_{n-r} u_{n-r}$ является решением системы $A'x = 0$, для которого свободные неизвестные равны $x_{r+1} = \lambda_1$, $x_{r+2} = \lambda_2, \ldots, x_n = \lambda_{n-r}$ (то есть произвольному набору); таким образом, любое решение указанной системы является линейной комбинацией $u_1, u_2, \ldots, u_{n-r}$. ■

Замечание 6.43. Приведем идею альтернативного доказательства предыдущей теоремы. Её утверждение, очевидно, равносильно тому, что для матрицы A размера $m \times n$ и ранга r максимальный ранг матрицы B, такой что $AB = O$, равен $n - r$. План доказательства этого утверждения разобьем на пункты.

1) Существуют невырожденные матрицы C и D порядков соответственно m и n такие, что

$$CAD = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Равносильное утверждение: любую матрицу A как в условии с помощью элементарных преобразований строк и столбцов можно привести к указанному виду.

2) Для матрицы $A' := \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ матрицы B' такие, что $A'B' = O$, имеют вид $\begin{pmatrix} 0 \\ F \end{pmatrix}$, где верхний блок из нулей состоит из r строк, а нижний блок F — из $n - r$ строк. То есть для матрицы A' максимальный ранг матрицы B' такой, что $A'B' = O$, равен $n - r$ (например, в качестве F можно взять единичную матрицу порядка $n - r$).

3) В предыдущих обозначениях имеем $O = A'B' = CADB'$, а поскольку C невырождена, $ADB' = O$, и снова в силу невырожденности матрицы D, $\operatorname{rk}(DB') = \operatorname{rk} B'$. Таким образом, для данной матрицы A мы нашли матрицу $B := DB'$ ранга $n - r$ такую, что $AB = O$.

4) Наоборот, пусть $A\widetilde{B} = O$. Тогда $CADD^{-1}\widetilde{B} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} D^{-1}\widetilde{B} = O$, откуда, как мы знаем из пункта 2), следует $\operatorname{rk}(D^{-1}\widetilde{B}) \leq n - r$, но в силу невырожденности D, $\operatorname{rk}(D^{-1}\widetilde{B}) = \operatorname{rk}\widetilde{B}$.

Заметим, что любая матрица B размера $n \times (n - r)$ и ранга $n - r$ такая, что $AB = O$, является фундаментальной матрицей СЛОУ $Ax = 0$. В самом деле, линейная оболочка столбцов B содержится в пространстве решений U_A этой системы. Если бы включение было строгим, то нашлось бы решение нашей системы, не принадлежащее линейной оболочке столбцов B, и добавив его к столбцам матрицы B мы получили бы матрицу B' ранга $n - r + 1$ такую, что $AB' = O$, в противоречии с доказанным ранее.

Задача 6.44. *Допустим, что добавление к некоторой СЛОУ еще одного уравнения (от того же множества неизвестных) не меняет множества решений. Докажите, что добавленное уравнение является линейной комбинацией уравнений исходной системы.*

Решение. Раз множество решений СЛОУ не меняется, то не изменяются линейные зависимости между столбцами, то есть сохраняется столбцовый ранг матрицы коэффициентов, а значит и ее строчный ранг. Другой способ: пространство решений не меняется, следовательно, не меняется его размерность, а значит не меняется ранг матрицы коэффициентов. ■

Задача 6.45. *Докажите, что две СЛОУ от одинакового числа неизвестных эквивалентны тогда и только тогда, когда уравнения каждой из них являются линейными комбинациями уравнений другой системы.*

Решение. В силу предыдущей задачи добавление любого из уравнений второй системы к первой системе не меняет ранга ее матрицы коэффициентов. ■

Заметим, что выбор базиса в пространстве решений не единственен (за исключением тривиальных случаев), но так как число базисных векторов пространства не зависит от выбора базиса, количество базисных решений для данной системы ни от каких выборов не зависит (а зависит, как показывает предыдущая теорема, только от числа неизвестных и ранга матрицы коэффициентов).

Базис в пространстве решений СЛОУ называется *фундаментальной системой решений* (кратко ФСР), а матрица, полученная выписыванием фундаментальных решений в столбцы — *фундаментальной матрицей системы.*

Из предыдущего обсуждения следует, что число столбцов (а значит размер) фундаментальных матриц для данной СЛОУ один и тот же. Сформулируем и докажем критерий того, что данная матрица является фундаментальной матрицей данной СЛОУ.

Пусть A — матрица с n столбцами и рангом r.

Предложение 6.46. *Матрица* Φ *размера* $n \times (n-r)$ *является фундаментальной матрицей СЛОУ* $Ax = 0$ *тогда и только тогда, когда выполнены следующие два условия:*

1) $A\Phi = 0$*;*

2) $\operatorname{rk} \Phi = n - r$.

Например, матрица $\Phi := \begin{pmatrix} -C \\ E_{n-r} \end{pmatrix}$ — фундаментальная матрица для системы однородных уравнений с упрощенной матрицей $A := (E_r\, C)$ (у которой главные неизвестные идут подряд). В том, что $A\Phi = 0$ (нулевой матрице) проще всего убедиться, записав $\begin{pmatrix} -C \\ E_{n-r} \end{pmatrix} = \begin{pmatrix} -C \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ E_{n-r} \end{pmatrix}$ и воспользовавшись дистрибутивностью умножения матриц относительно сложения.

Доказательство. Если Φ — фундаментальная матрица системы $Ax = 0$, то ее столбцы являются решениями указанной системы, откуда следует соотношение $A\Phi = 0$. Кроме того, столбцы фундаментальной матрицы образуют базис в пространстве решений, откуда следует, что они линейно независимы и их $n-r$ штук (см. Теорему 6.42), то есть $\operatorname{rk} \Phi = n-r$.

Обратно, если Φ — матрица размера $n \times (n-r)$ такая, что $A\Phi = 0$, то ее столбцы являются решениями системы $Ax = 0$, а если при этом ее ранг равен числу ее столбцов $n - r$, то они линейно независимы и, значит, образуют базис в пространстве решений системы $Ax = 0$, поскольку, согласно Теореме 6.42, размерность указанного пространства равна $n - r$. ■

Задача 6.47. *Найдите ФСР однородной системы с матрицей коэффициентов* $(C\, E_r)$.

Задача 6.48. *Пусть* A *— матрица ранга* r*, состоящая из* n *столбцов. Известно, что для матрицы* B *определено произведение* $AB = 0$*. Оцените сверху* $\operatorname{rk} B$.

Решение. Столбцы матрицы B являются решениями СЛОУ $Ax = 0$, поэтому среди них не более $n - r$ линейно независимых. Если B — ФСР указанной системы, то $AB = 0$ и $\operatorname{rk} B = n - r$, то есть оценка является точной. ■

Теорема 6.49. *Пусть* Φ *— фундаментальная матрица СЛОУ* $A\mathbf{x} = \mathbf{0}$*. Тогда система* $\Phi^T\mathbf{y} = \mathbf{0}$ *задает линейную оболочку столбцов матрицы* A^T *(то есть, по существу, строк матрицы* A*).*

Доказательство. Равенство $A\Phi = 0$ равносильно равенству $\Phi^T A^T = 0$. Последнее означает, что столбцы матрицы A^T являются решениями системы $\Phi^T y = 0$. Другими словами, линейная оболочка столбцов A^T содержится в пространстве решений указанной системы, осталось лишь проверить, что ее размерность совпадает с размерностью пространства решений.

Если матрица A состоит из n столбцов и имеет ранг r, то Φ имеет размер $n \times (n-r)$ и ранг $n-r$, а значит Φ^T размера $(n-r)\times n$ и ранга $n-r$, откуда получаем, что размерность пространства решений системы $\Phi^T y = 0$ равна $n - (n - r)$, что совпадает с $r = \operatorname{rk} A = \operatorname{rk} A^T$. ■.

Задача 6.50. *Используя предыдущую Теорему, придумайте алгоритм, как по подпространству пространства* $\mathbb{K}^n$*, заданному как линейная оболочка некоторой конечной системы столбцов, построить СЛОУ, для которой данное подпространство является пространством решений. (Из существования такого алгоритма следует, что любое подпространство в* $\mathbb{K}^n$ *является пространством решений некоторой СЛОУ).*

Наряду с теоремой Кронекера-Капелли есть еще удобный критерий разрешимости системы линейных уравнений, причем легко обобщающийся на бесконечномерный случай — теорема Фредгольма.

Для СЛУ $Ax = b$ СЛОУ $A^T y = 0$ называется *сопряженной однородной системой.* Заметим, что последняя может быть переписана в виде $y^T A = 0$.

Теорема 6.51. (Теорема Фредгольма). *Система* $Ax = b$ *разрешима тогда и только тогда, когда для любого решения* y_0 *сопряженной однородной системы* $A^T y = 0$ *выполнено равенство* $y_0^T b = 0$.

Заметим, что условие $y_0^T b = 0$ над полем $\mathbb{R}$ можно интерпретировать как условие ортогональности (относительно "стандартного" скалярного произведения столбцов, а именно такого, для которого столбцы e_i образуют ортонормированный базис) столбца b произвольному столбцу, являющемуся решением сопряженной однородной системы.

Доказательство. Пусть система $Ax = b$ разрешима и x_0 — ее решение. Тогда для произвольного решения y_0 сопряженной однородной системы

$$y_0^T A x_0 = (y_0^T A)x_0 = 0x_0 = 0,$$

с другой стороны,

$$y_0^T A x_0 = y_0^T (A x_0) = y_0^T b,$$

откуда $y_0^T b = 0$.

Предположим теперь, что система $Ax = b$ несовместна. Это равносильно тому, что в упрощенном виде ее расширенной матрицы $(A \mid b)$ есть строка $(0 \dots 0 \mid 1)$ (последняя ненулевая строка сверху). Так как упрощенный вид получается из исходной матрицы элементарными преобразованиями строк, строка $(0 \dots 0 \mid 1)$ является линейной комбинацией строк матрицы $(A \mid b)$. То есть существует такой столбец y_0, что $y_0^T (A \mid b) = (0 \dots 0 \mid 1)$. Последнее равенство равносильно системе $y_0^T A = 0,\ \ y_0^T b = 1$. То есть предположив несовместность системы $Ax = b$, мы нашли такое решение y_0 сопряженной однородной системы, что $y_0^T b \neq 0$. ∎

Задача 6.52. *Системы вида $Ax = b$ над полем $\mathbb{R}$ совместны для любого столбца правых частей b тогда и только тогда, когда строки матрицы A линейно независимы. Докажите это, используя а) теорему Кронекера-Капелли, b) теорему Фредгольма.*

6.4 Координаты вектора в базисе

Пусть в n-мерном пространстве V над полем $\mathbb{K}$ зафиксирован базис $\{e_1, \dots, e_n\}$. Тогда любой вектор $v \in V$ единственным образом по нему раскладывается:

$$v = v_1 e_1 + v_2 e_2 + \dots + v_n e_n. \tag{46}$$

Согласно Лемме 6.3 из линейной независимости базисных векторов следует, что набор скаляров $(v_1, v_2, \dots, v_n) \in \mathbb{K}^n$ определен однозначно, и v_i называется *i-й координатой вектора v в базисе* $\{e_1, \dots, e_n\}$. Согласно стандартному соглашению, набор $(v_1, v_2, \dots, v_n)$ записывается в виде столбца и называется столбцом координат вектора v в базисе $\{e_1, \dots, e_n\}$. Равенство (46) часто записывают в "матричной форме"

$$v = (e_1, e_2, \dots, e_n)(v_1, v_2, \dots, v_n)^T \tag{47}$$

(произведение строки из базисных векторов на столбец координат).

Предложение 6.53. *Сопоставление каждому вектору n-мерного линейного пространства V его координатного столбца в фиксированном базисе $e := \{e_1, \dots, e_n\}$ задает биекцию*

$$\varphi_e \colon V \to \mathbb{K}^n, \quad \varphi_e(v) = (v_1, \dots, v_n)^T$$

пространства V с пространством столбцов $\mathbb{K}^n$ высоты n. Кроме того, данная биекция сохраняет операции: $\varphi_e(u + v) = \varphi_e(u) + \varphi_e(v)$ (координатный столбец суммы векторов равен сумме координатных столбцов слагаемых) и $\varphi_e(\lambda v) = \lambda \varphi_e(v)$ (координатный столбец произведения вектора на скаляр равен произведению координатного столбца вектора на тот же скаляр).

Доказательство. Как уже отмечалось, тот факт, что φ_e корректно определено, следует из существования и единственности разложения вектора по базису. Если двум векторам отвечает один и тот же столбец, то они совпадают, поскольку имеют одинаковые разложения по выбранному базису. Значит, φ_e инъективно. Произвольный столбец $(v_1, \ldots, v_n)^T$ является координатным столбцом вектора $v = v_1e_1 + \ldots + v_ne_n$, который существует в силу аксиом векторного пространства.

Вторая часть предложения следует из свойств операций над векторами, вытекающих из аксиом линейного пространства: если $u = \sum u_ie_i, \quad v = \sum v_ie_i$, то $u + v = \sum(u_i + v_i)e_i, \quad \lambda v = \sum(\lambda v_i)e_i$. ∎

Следствие 6.54. *При любом выборе базиса в пространстве V линейные зависимости между векторами V — то же, что линейные зависимости между их координатными столбцами.*

Доказательство. Заметим, что при биекции φ_e нулевой вектор пространства V соответствует нулевому столбцу в $\mathbb{K}^n$. Пусть $\sum_i \lambda_i v_i = 0$ — линейная зависимость. Тогда

$$(0, \ldots, 0)^T = \varphi_e(0) = \varphi_e\left(\sum_i \lambda_i v_i\right) = \sum_i \lambda_i \varphi_e(v_i),$$

то есть линейная зависимость между векторами при биекции φ_e переходит в линейную зависимость между их координатными столбцами.

Обратно, если $\sum_i \lambda_i \varphi_e(v_i) = (0, \ldots 0)^T$ — линейная зависимость между столбцами, то

$$(0, \ldots 0)^T = \sum_i \lambda_i \varphi_e(v_i) = \varphi_e\left(\sum_i \lambda_i v_i\right),$$

а значит в силу сказанного в начале доказательства $\sum_i \lambda_i v_i = 0$. ∎

В частности, ранг системы векторов равен рангу их координатных столбцов в произвольном базисе, координатные столбцы максимальной линейно независимой подсистемы системы векторов образуют максимальную линейно независимую подсистему их системы столбцов и т.д.

Зафиксировав базис и заменяя векторы их координатными столбцами мы сводим геометрию линейного пространства к алгебре столбцов, что полезно для конкретных вычислений. Может показаться, что про геометрию после этого можно забыть, но это далеко не так. Как правило, смысл теорем и их доказательства намного прозрачнее, если их излагать на геометрическом языке.

Заметим, что построенная выше биекция зависит от базиса — каждому базису e в V отвечает своя биекция $\varphi_e \colon V \to \mathbb{K}^n$. (Вообще, до тех пор, пока мы не выбрали какой-то базис, все базисы в пространстве V равноправны). Пространство $\mathbb{K}^n$ с этой точки зрения не

просто n-мерное пространство над полем $\mathbb{K}$, а n-мерное пространство с выбранным "стандартным" базисом из столбцов $e_i = (0, \dots, 1, \dots 0)^T$ (1 на i-м месте), в который переходит при биекции выбранный базис в V.

Вообще говоря, в линейном пространстве много базисов, все что мы пока знаем — что они содержат одинаковое число векторов. Сейчас мы построим биекцию между множеством базисов в n-мерном пространстве над полем $\mathbb{K}$ и множеством невырожденных матриц порядка n с элементами из $\mathbb{K}$.

Пусть в n-мерном пространстве V выбран базис $\{e_1, \dots, e_n\}$ и система векторов $\{e'_1, \dots, e'_n\}$. Запишем разложения векторов системы по базису:

$$\begin{aligned} e'_1 &= c_{11}e_1 + c_{21}e_2 + \ldots + c_{n1}e_n \\ e'_2 &= c_{12}e_1 + c_{22}e_2 + \ldots + c_{n2}e_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e'_n &= c_{1n}e_1 + c_{2n}e_2 + \ldots + c_{nn}e_n \end{aligned}$$

и составим матрицу $C = (c_{ij})$. Подчеркнем, что матрица C получается выписыванием координат векторов системы относительно базиса в *столбцы*. Приведенное определение равносильно тому, что C удовлетворяет равенству

$$(e'_1, e'_2, \dots, e'_n) = (e_1, e_2, \dots, e_n)C \tag{48}$$

(единственность матрицы C, удовлетворяющей приведенному равенству, следует из линейной независимости системы $\{e_1, \dots, e_n\}$).

Предложение 6.55. *Пусть $\{e_1, \dots, e_n\}$ — базис в V. Система векторов $\{e'_1, \dots, e'_n\}$, задаваемая (48), линейно независима (является базисом в V) тогда и только тогда, когда матрица C невырождена.*

Доказательство сразу вытекает из Следствия 6.54.

Вот другое рассуждение. Если матрица C вырождена, то существует такой столбец $x_0 \neq 0$ высоты n, что $Cx_0 = 0$. Тогда, умножая обе части (48) справа на x_0, получаем нетривиальную линейную зависимость между векторами $e'_1, \dots, e'_n$.

Наоборот, если система $\{e'_1, \dots, e'_n\}$ линейно зависима, то существует ненулевой столбец x_0 высоты n такой, что $(e'_1, e'_2, \dots, e'_n)x_0 = 0$. Тогда из (48) и линейной независимости системы $\{e_1, \dots, e_n\}$ получаем, что $Cx_0 = 0$, то есть столбцы матрицы C линейно зависимы, а значит эта матрица вырождена. ∎

Определение 6.56. *Матрицей перехода от базиса $\{e_1, \dots, e_n\}$ к базису $\{e'_1, \dots, e'_n\}$* называется матрица C, определенная равенством (48).

Зафиксируем некоторый базис $\{e_1, \dots, e_n\}$ пространства V. Из предыдущего Предложения следует, что сопоставляя базису $\{e'_1, \dots, e'_n\}$ матрицу перехода к нему от фиксированного базиса мы получаем биекцию между множеством базисов в n-мерном пространстве V и множеством невырожденных матриц порядка n над данным полем (над

которым определено векторное пространство V). В частности, самому фиксированному базису $\{e_1, \ldots, e_n\}$ при этом соответствует единичная матрица E (разумеется, определенная биекция зависит от того, какой базис зафиксирован).

Задача 6.57. *Пусть V — n-мерное векторное пространство над полем $\mathbb{F}$, состоящим из q элементов. Найти:*

a) число векторов в пространстве V;

b) число решений уравнения $AX = 0$, где A — прямоугольная матрица ранга r, X — столбец неизвестных высоты n;

c) число базисов пространства V;

d) число невырожденных матриц порядка n над полем $\mathbb{F}$;

e) число k-мерных подпространств пространства V.

Задача 6.58. *Опишите множество всех фундаментальных матриц СЛОУ $Ax = 0$, если Φ — какая-то ее фундаментальная матрица.*

Решение. Пусть для определенности матрица A имеет размер $m \times n$ и ранг r. Если $\Phi = (\phi_1 \ldots \phi_{n-r})$ — фундаментальная матрица системы $Ax = 0$, то ее столбцы $\{\phi_1, \ldots, \phi_{n-r}\}$ образуют базис в пространстве решений $U_A \subset \mathbb{K}^n$ этой системы. Если Φ' — еще одна фундаментальная матрица той же системы $Ax = 0$, то система ее столбцов $\{\phi'_1, \ldots, \phi'_{n-r}\}$ образует еще один базис в том же пространстве U_A. Так как ϕ'_i являются линейными комбинациями ϕ_j, то существует такая матрица C порядка $n - r$, что $\Phi' = \Phi C$ (в i-м столбце C стоят коэффициенты разложения ϕ'_i по $\{\phi_1, \ldots, \phi_{n-r}\}$). Так как, наоборот, ϕ_i выражаются через ϕ'_j, то матрица C должна быть обратимой. То есть матрица C является матрицей перехода между базисами $\{\phi_1, \ldots, \phi_{n-r}\}$ и $\{\phi'_1, \ldots, \phi'_{n-r}\}$. ∎

Предложение 6.59. *Если C — матрица перехода от базиса $\{e_1, \ldots, e_n\}$ к базису $\{e'_1, \ldots, e'_n\}$, а D — матрица перехода от $\{e'_1, \ldots, e'_n\}$ к базису $\{e''_1, \ldots, e''_n\}$, то CD — матрица перехода от $\{e_1, \ldots, e_n\}$ к $\{e''_1, \ldots, e''_n\}$.*

Доказательство. Имеем

$$(e''_1, e''_2, \ldots, e''_n) = ((e_1, e_2, \ldots, e_n)C)D.$$

Тогда если мы докажем следующую “ассоциативность”

$$((e_1, e_2, \ldots, e_n)C)D = (e_1, e_2, \ldots, e_n)(CD),$$

то требуемое утверждение будет следовать из единственности матрицы перехода (см. фразу после равенства (48)).

Подставляя $e'_j = \sum_{i=1}^n e_i c_{ij}$ в $e''_k = \sum_{j=1}^n e'_j d_{jk}$, имеем

$$e''_k = \sum_{j=1}^n e'_j d_{jk} = \sum_{j=1}^n \left(\sum_{i=1}^n e_i c_{ij} \right) d_{jk} = \sum_{j=1}^n (e_1 c_{1j} + e_2 c_{2j} + \ldots + e_n c_{nj}) d_{jk} =$$

$$= e_1 \sum_{j=1}^{n} c_{1j} d_{jk} + e_2 \sum_{j=1}^{n} c_{2j} d_{jk} + \ldots + e_n \sum_{j=1}^{n} c_{nj} d_{jk} = \sum_{i=1}^{n} e_i \left(\sum_{j=1}^{n} c_{ij} d_{jk} \right). \quad \blacksquare$$

Кстати, из доказанного Предложения и невырожденности матрицы перехода между базисами можно еще раз вывести, что произведение невырожденных матриц невырождено. В то же время следующая задача, в частности, означает, что невырожденная матрица обратима (впрочем, мы это уже знаем и так).

Задача 6.60. *Если C — матрица перехода от базиса $\{e_1, \ldots, e_n\}$ к базису $\{e'_1, \ldots, e'_n\}$, то матрицей перехода "в обратном направлении" — от $\{e'_1, \ldots, e'_n\}$ к $\{e_1, \ldots, e_n\}$ — будет C^{-1}.*

Координаты ненулевого вектора $v \in V$ в базисе $\{e_1, \ldots, e_n\}$ пространства V зависят от базиса. Например, любой такой вектор можно включить в базис в качестве первого вектора (см. Теорему 6.18), и тогда его координаты в таком базисе будут составлять столбец $(1, 0, \ldots, 0)^T$.

Решим следующую задачу: пусть вектор v имеет координатный столбец $(v_1, v_2, \ldots, v_n)^T$ в базисе $\{e_1, \ldots, e_n\}$ и пусть задан новый базис $\{e'_1, \ldots, e'_n\}$, связанный с первым матрицей перехода C. Какие координаты вектор v будет иметь в новом базисе?

Используя запись (47) и равенство (48), имеем

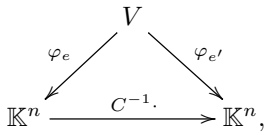
$$v = (e_1, \ldots, e_n)(v_1, \ldots, v_n)^T = (e'_1, \ldots, e'_n)(v'_1, \ldots, v'_n)^T = ((e_1, \ldots, e_n)C)(v'_1, \ldots, v'_n)^T.$$

Сравнивая второе выражение с последним и используя ассоциативность умножения матриц и единственность разложения вектора по базису, получаем

$$(v_1, \ldots, v_n)^T = C(v'_1, \ldots, v'_n)^T \qquad \text{или} \qquad (v'_1, \ldots, v'_n)^T = C^{-1}(v_1, \ldots, v_n)^T. \tag{49}$$

Обратим внимание читателя на особенность полученной формулы: чтобы получить столбец координат вектора в новом базисе, нужно умножить столбец его координат в старом базисе на матрицу, *обратную* к матрице перехода от старого базиса к новому. Заметим, что оба равенства в (49) эквивалентны в силу Задачи 6.60.

Полученный результат можно выразить следующим образом. Пусть φ_e, $\varphi_{e'} \colon V \to \mathbb{K}^n$ — линейные биекции, построенные по базисам e и e'. Тогда коммутативна диаграмма



(50)

где горизонтальная стрелка отвечает умножению столбцов слева на C^{-1} (коммутативность диаграммы в данном случае означает, что два пути из вершины в правый нижний угол совпадают, то есть $\varphi_{e'} = C^{-1} \circ \varphi_e$).

Замечание 6.61. Столбцы матрицы можно считать координатными столбцами некоторой системы векторов в некотором базисе. Тогда элементарные преобразования столбцов отвечают элементарным преобразованиям этой системы векторов, а элементарные преобразования строк — элементарным преобразованиям системы базисных векторов. Это дает еще одну интерпретацию известного нам результата о том, что элементарные преобразования строк не меняют не только строчный, но и столбцовый ранг.

7 Линейные пространства и отображения

Данная глава начинается с изучения важного для дальнейшего понятия прямой суммы подпространств. Далее изучаются линейные отображения между линейными пространствами. Вводятся важные понятия ядра и образа линейного отображения. Показывается, как относительно выбранных базисов линейные отображения записываются матрицами. Это дает новую интерпретацию результатов предыдущей главы о системах линейных уравнений и рангах матриц. Далее доказывается, что известные операции с матрицами (сложение, умножение) отвечают соответствующим операциям над линейными отображениями. Именно использование аппарата матриц делает линейную алгебру столь эффективной в вычислительном отношении.

7.1 Подпространства и прямые суммы

Пусть $U \subset V$ — подпространство линейного пространства V.

Определение 7.1. Базис $\{e_1, \ldots, e_n\}$ в V называется *согласованным* с подпространством U, если $U = \langle e_{i_1}, \ldots, e_{i_k} \rangle$ (то есть U является линейной оболочкой некоторого подмножества векторов данного базиса).

Например, базис $\{e_1, e_2\}$ в двумерном пространстве V согласован с нулевым подпространством, одномерными подпространствами $\langle e_1 \rangle$, $\langle e_2 \rangle$ и самим пространством V, а, например, с одномерным подпространством $\langle e_1 + e_2 \rangle$ не согласован.

Очевидно, что для всякого подпространства $U \subset V$ существует согласованный с ним базис в V. Действительно, выберем произвольный базис в U и продолжим его до базиса в V.

Пусть теперь в V выбраны два подпространства $U \subset V$, $W \subset V$. Существует ли базис в V, согласованный одновременно с подпространствами U и W? Чтобы изучить этот вопрос, введем две важные операции над подпространствами фиксированного пространства (пока для случая двух подпространств).

Для двух подпространств U, $W \subset V$ определим подмножество

$$U + W := \{u + w \mid u \in U, w \in W\} \subset V$$

(векторы из разных подпространств одного и того же пространства V можно складывать как элементы из V). Мгновенно проверяется, что $U + W$ — не просто подмножество в V, а *подпространство* в V.

Определение 7.2. *Суммой* подпространств U, $W \subset V$ называется подпространство $U + W$ в V.

Заметим, что объединение двух подпространств U, $W \subset V$ как правило *не является* подпространством в V (только подмножеством).

Задача 7.3. *Докажите, что теоретико-множественное объединение $U \cup W$ двух подпространств $U, W \subset V$ является подпространством в V тогда и только тогда, когда одно из них содержится в другом: $U \subset W$ или $W \subset U$.*

Решение. Пусть $U \cup W$ подпространство, но U не содержится в W; выберем $u \in U,\ u \notin W$. Тогда $\forall w \in W\ u + w \in U$ (иначе $u + w = w' \in W$ и значит $u = w' - w \in W$ в противоречии с выбором u). Откуда $W \subset U$. Если же одно из подпространств содержится в другом, то их объединение совпадает с этим подпространством. ■

Задача 7.4. *Докажите, что сумма $U + W$ является наименьшим из подпространств в V, содержащим и U и W. Эквивалентно, $U + W$ есть линейная оболочка объединения этих подпространств, то есть $U + W = \langle U \cup W \rangle$.*

В отличие от объединения, пересечение любого (конечного или бесконечного) семейства подпространств данного пространства всегда является подпространством (докажите!).

Определение 7.5. *Пересечением* подпространств $U, W \subset V$ называется подпространство, множество элементов которого является их обычным теоретико-множественным пересечением $U \cap W$ как подмножеств в V.

Задача 7.6. *Докажите, что*

$$\max(\dim U,\ \dim V) \leq \dim(U + V) \leq \dim U + \dim V.$$

Вскоре мы серьезно улучшим результат предыдущей задачи.

Теорема 7.7. *Для любой пары подпространств $U, W \subset V$ существует базис в V, согласованный с U и W.*

Доказательство. Выберем базис $\{e_1, \ldots, e_p\}$ в $U \cap W$. Это — линейно независимая система векторов и в U и в W. Пусть $\{e_1, \ldots, e_p, e_{p+1}, \ldots, e_k\}$ и $\{e_1, \ldots, e_p, e_{k+1}, \ldots, e_{k+l-p}\}$ — ее дополнения до базисов в U и W соответственно (наши обозначения предполагают, что $\dim(U \cap W) = p,\ \dim U = k,\ \dim W = l$).

Мы утверждаем, что система векторов

$$\{e_1, \ldots, e_p, e_{p+1}, \ldots, e_k, e_{k+1}, \ldots, e_{k+l-p}\} \tag{51}$$

линейно независима (и значит является базисом в $U + W$, поскольку она, очевидно, порождает $U + W$). Действительно, пусть

$$\sum_{i=1}^{k+l-p} \lambda_i e_i = 0$$

— линейная зависимость. Тогда

$$x := \sum_{i=1}^{k} \lambda_i e_i = -\sum_{i=k+1}^{k+l-p} \lambda_i e_i. \tag{52}$$

Заметим, что в (52) первая линейная комбинация лежит в U, вторая — в W, поэтому вектор x лежит в пересечении $U \cap W$. Значит $\exists \mu_i,\ i = 1, \ldots, p$ такие, что $x = \sum_{i=1}^{p} \mu_i e_i$. Из линейной независимости системы $\{e_1, \ldots, e_p, e_{k+1}, \ldots, e_{k+l-p}\}$ (как базиса в W) следует, что правая часть в (52) равна нулю, а значит $x = 0$, откуда все λ_i равны нулю. Таким образом, система (51) линейно независима, как и утверждалось. Теперь осталось дополнить ее до базиса в V, при этом, очевидно, получится требуемый базис, согласованный с подпространствами U и W. ∎

В качестве иллюстрации к доказанной теореме читателю предлагается представить два двумерных подпространства U и W в трехмерном пространстве, пересекающихся по одномерному $U \cap W$. Тогда $\{e_1\}$ — базис в $U \cap W$, $\{e_1, e_2\}$ — в U, $\{e_1, e_3\}$ — в W, а $\{e_1, e_2, e_3\}$ — в $U + W$.

Следствие 7.8. $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$.

Задача 7.9. *Дайте простое доказательство Теоремы 6.33 с использованием понятия суммы подпространств.*

Определение 7.10. Сумма $U + W$ подпространств $U, W \subset V$ называется *прямой* (обозначение $U \oplus W$), если для любого вектора $v \in U + W$ его представление $v = u + w$ в виде суммы $u \in U$ и $w \in W$ единственно. Другими словами, если $u + w = u' + w'$, то $u = u'$, $w = w'$.

Предложение 7.11. *Сумма двух подпространств $U + W$ прямая тогда и только тогда, когда $U \cap W = 0$.*

Доказательство. Если $0 \neq z \in U \cap W$, то $0 = 0 + 0 = z + (-z)$ — два разных представления нулевого вектора в виде суммы вектора из U и из W, значит сумма $U + W$ не прямая. Обратно, из $u + w = u' + w'$ следует $U \ni u - u' = w' - w \in W$, откуда $u - u' \in U \cap W$ и значит если $u \neq u'$ (и тогда $w \neq w'$), то $U \cap W \neq 0$. ∎

Рассмотрим подробнее случай, когда все пространство V представляется в виде прямой суммы своих подпространств U и W. Из предыдущего следует, что $V = U \oplus W \Leftrightarrow V = U + W$ и $U \cap W = 0$.

Предложение 7.12. $V = U \oplus W \Leftrightarrow U \cap W = 0$ *и* $\dim V = \dim U + \dim W$.

Доказательство. Если $V = U \oplus W$, то как показано выше, $U \cap W = 0$. Кроме того, $\dim V = \dim U + \dim W - \dim(U \cap W) = \dim U + \dim W$.

Обратно, $\dim(U + W) = \dim U + \dim W - \dim(U \cap W) = \dim U + \dim W = \dim V$, а так как $U + W \subset V$, то $U + W = V$ (см. Теорему 6.19) и сумма прямая так как $U \cap W = 0$. ∎

Определение 7.13. Пусть $U \subset V$ — некоторое подпространство. Подпространство $W \subset V$ называется *прямым дополнением* к U в V, если $V = U \oplus W$.

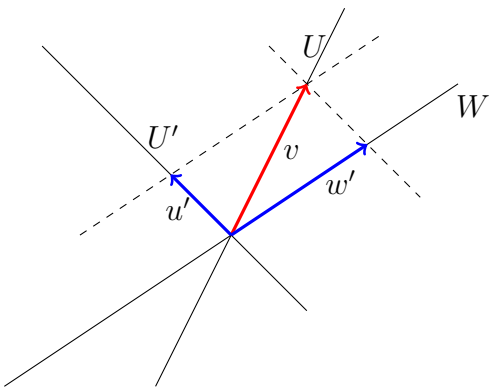
Задача 7.14. *Для любого подпространства в конечномерном линейном пространстве V существует прямое дополнение. (Указание: воспользуйтесь Теоремой 6.18).*

Прямое дополнение, за исключением тривиальных случаев ($U = 0$ или $U = V$) не единственно. Например, в двумерном пространстве над $\mathbb{R}$ прямым дополнением к одномерному подпространству является любое из континуального множества не совпадающих с ним одномерных подпространств.

Задача 7.15. *Найдите количество прямых дополнений к k-мерному подпространству в n-мерном линейном пространстве над конечным полем из q элементов (ср. Задачу 6.57).*

Определение 7.16. Если $V = U \oplus W$, то для любого $v \in V$ существуют единственные векторы $u \in U$, $w \in W$ такие, что $v = u + w$. В этой ситуации u называется *проекцией вектора v на подпространство U параллельно подпространству W* (обозначение $\mathrm{Pr}_U^{\|W} v$), а w — *проекцией вектора v на подпространство W параллельно подпространству U* (обозначение $\mathrm{Pr}_W^{\|U} v$).

Сложные обозначения для проекций в Определении 7.16 связаны с тем, что проекция вектора на подпространство зависит не только от этого подпространства, но и от выбранного прямого дополнения к нему. Пусть, например, $V = U \oplus W$ — представление двумерного пространства в виде прямой суммы одномерных подпространств. Тогда если $0 \neq v \in U$, то $\mathrm{Pr}_W^{\|U} v = 0$, однако заменяя U другим прямым дополнением U' к W, получим $\mathrm{Pr}_W^{\|U'} v \neq 0$, поскольку теперь $v \notin U'$:



Задача 7.17. *Докажите, что $\mathbb{R}^n = U \oplus W$, где*

$$U = \langle (1, 1, \ldots, 1)^T \rangle, \quad W = \{(w_1, \ldots, w_n)^T \mid \sum_i w_i = 0\}.$$

Найдите проекции векторов стандартного базиса.

Решение. 1-й способ. Докажем, что любой столбец $(v_1, \dots, v_n)^T \in \mathbb{R}$ можно представить, причем единственным образом, в виде суммы столбцов $\lambda(1, \dots, 1)^T \in U$ и $(w_1, \dots, w_n)^T \in W$. Если $(v_1, \dots, v_n)^T = \lambda(1, \dots, 1)^T + (w_1, \dots, w_n)^T$, то приравнивая суммы координат слева и справа, получаем $\sum_i v_i = n\lambda$, откуда λ однозначно определяется: $\lambda = \frac{1}{n}\sum_i v_i$. Теперь вычитая из столбца $(v_1, \dots, v_n)^T$ столбец $\lambda(1, \dots, 1)^T$, получаем столбец $(w_1, \dots, w_n)$ такой, что $\sum_i w_i = 0$. Таким образом, $\mathbb{R}^n = U \oplus W$.

2-й способ. Легко видеть, что $U \cap W = 0$, а также что $\dim U = 1$ и $\dim W = n - 1$ (W — пространство решений СЛОУ от n неизвестных с матрицей коэффициентов $(1 \dots 1)$ ранга 1). Теперь работает Предложение 7.12.

Проекции читателю предлагается найти самостоятельно. ■

Следующая задача обобщает предыдущую, если положить $A = (1, 1, \dots, 1)^T$.

Задача 7.18. *Дана вещественная матрица A из n строк. Докажите, что пространство $\mathbb{R}^n$ является прямой суммой линейной оболочки столбцов матрицы A и пространства решений системы $A^T x = 0$.*

Решение. Пусть $U \subset \mathbb{R}^n$ — линейная оболочка столбцов A, а $W \subset \mathbb{R}^n$ — пространство решений системы $A^T x = 0$. Заметим, что $\dim U = \operatorname{rk} A$, а $\dim W = n - \operatorname{rk} A$, поэтому достаточно доказать, что $U \cap W = 0$. Заметим, что столбец b принадлежит U тогда и только тогда, когда система $Ax = b$ разрешима, а по теореме Фредгольма 6.51 последнее равносильно тому, что для любого $y \in W$ $y^T b = 0$. Таким образом, $b \in U \cap W$ влечет $b^T b = 0$, откуда $b = 0$. ■

Пример 7.19. Докажем, что (бесконечномерное!) пространство $F(\mathbb{R})$ вещественнозначных функций на действительной прямой является прямой суммой подпространства $F(\mathbb{R})^+$ четных функций и подпространства $F(\mathbb{R})^-$ нечетных функций. Для этого докажем, что любая функция $f \in F(\mathbb{R})$ единственным образом представляется в виде суммы четной и нечетной функции. Действительно, легко проверить, что $f(x) = \frac{f(x)+f(-x)}{2} + \frac{f(x)-f(-x)}{2}$ — такое представление. Если $f(x) = f^+(x) + f^-(x)$ — произвольное такое представление, то $f(-x) = f^+(x) - f^-(x)$, откуда $f^+(x) = \frac{f(x)+f(-x)}{2}$, $f^-(x) = \frac{f(x)-f(-x)}{2}$.

Например, для функции $\exp(x)$ данное представление имеет вид $\exp(x) = \operatorname{ch}(x) + \operatorname{sh}(x)$.

Заметим, что в этом примере соображения, связанные с размерностью пространств не работают — все пространства бесконечномерные!

Задача 7.20. *Докажите, что пространство $\operatorname{Mat}_n(\mathbb{R})$ матриц порядка n является прямой суммой подпространств симметрических $\operatorname{Mat}_n(\mathbb{R})^+$ и кососимметрических $\operatorname{Mat}_n(\mathbb{R})^-$ матриц. Найдите проекции произвольной матрицы $A \in \operatorname{Mat}_n(\mathbb{R})$ на $\operatorname{Mat}_n(\mathbb{R})^+$ параллельно $\operatorname{Mat}_n(\mathbb{R})^-$ и на $\operatorname{Mat}_n(\mathbb{R})^-$ параллельно $\operatorname{Mat}_n(\mathbb{R})^+$. (Указание: попробуйте найти формулы для проекций по аналогии с предыдущим примером).*

Задача 7.21. *Докажите, что пространство $T_n(\mathbb{R})$ верхнетреугольных матриц порядка n является еще одним (помимо симметрических матриц) прямым дополнением к*

подпространству кососимметрических матриц $\mathrm{Mat}_n(\mathbb{R})^-$ *в* $\mathrm{Mat}_n(\mathbb{R})$ *и найдите соответствующие проекции произвольной матрицы* $A \in \mathrm{Mat}_n(\mathbb{R})$.

Перейдем теперь к определению и изучению сумм и прямых сумм произвольного конечного числа подпространств данного пространства.

Определение 7.22. Подпространства $U_1, \ldots, U_k$ линейного пространства V называются *линейно независимыми*, если из $u_1 + \ldots + u_k = 0$ $(u_i \in U_i,\ i = 1, \ldots, k)$ следует $u_i = 0\ \forall i,\ 1 \leq i \leq k$.

Определение 7.23. Суммой $U_1 + \ldots + U_k$ подпространств $U_i \subset V$ называется подпространство в V, состоящее из всех сумм вида $u_1 + \ldots + u_k \in V$ $(u_i \in U_i)$. Это — наименьшее линейное подпространство в V, содержащее все $U_i,\ i = 1, \ldots, k$.

Заметим, что подпространства $U_1, \ldots, U_k$ линейно независимы тогда и только тогда, когда для любого вектора $v \in U_1 + \ldots + U_k$ его представление вида $v = u_1 + \ldots + u_k$ $(u_i \in U_i)$ единственно (ср. Определение 7.10).

Определение 7.24. Сумма линейно независимой системы подпространств $U_1, \ldots, U_k$ линейного пространства V называется *прямой суммой* и обозначается $U_1 \oplus \ldots \oplus U_k$.

Предложение 7.25. *Следующие свойства системы подпространств* $U_1, \ldots, U_k \subset V$ *равносильны:*

1) подпространства $U_1, \ldots, U_k$ *линейно независимы;*

2) объединение базисов подпространств $U_1, \ldots, U_k$ *линейно независимо;*

3) $\dim(U_1 + \ldots + U_k) = \dim U_1 + \ldots + \dim U_k$.

Доказательство. 1) $\Rightarrow$ 2): Пусть $\dim U_i = n_i$ и $\{e_{i1}, \ldots, e_{in_i}\}$ — базис в $U_i,\ i = 1, \ldots, k$. Пусть

$$\sum_{i=1}^{k} \sum_{j=1}^{n_i} \lambda_{ij} e_{ij} = 0$$

— нетривиальная линейная зависимость. Обозначим $u_i := \sum_{j=1}^{n_i} \lambda_{ij} e_{ij} \in U_i$. Тогда $\sum_i u_i = 0$, но не все u_i равны нулю. Поэтому подпространства $U_1, \ldots, U_k$ линейно зависимы.

2) $\Rightarrow$ 1): Если подпространства $U_1, \ldots, U_k$ линейно зависимы, то существует система векторов $u_1, \ldots, u_k$ $(u_i \in U_i)$, среди которых не все равны нулю, такая, что $\sum_i u_i = 0$. Раскладывая эти векторы по базисам в U_i, получаем нетривиальную линейную зависимость между объединением базисов подпространств $U_1, \ldots, U_k$.

2) $\Rightarrow$ 3): Если объединение базисов подпространств $U_1, \ldots, U_k$ линейно независимо, то оно является базисом в их сумме $U_1 + \ldots + U_k$, поскольку оно порождает ее.

3) $\Rightarrow$ 2): Предположим, что объединение базисов подпространств $U_1, \ldots, U_k$ линейно зависимо. Поскольку оно порождает сумму $U_1 + \ldots + U_k$, оно содержит некоторый ее базис, а значит ее размерность меньше чем сумма размерностей подпространств U_i. ∎

Определение 7.26. Линейное пространство V раскладывается в прямую сумму своих подпространств $U_1, \ldots, U_k$, то есть $V = U_1 \oplus \ldots \oplus U_k$, если выполнены следующие два условия:

1) $V = U_1 + \ldots + U_k$;

2) подпространства $U_1, \ldots, U_k$ линейно независимы.

Заметим, что предыдущее Предложение позволяет заменить условие 2) из Определения, например, условием $\dim V = \dim U_1 + \ldots + \dim U_k$.

Кстати, для трех и большего числа подпространств аналог Теоремы 7.7 неверен. Например, выбирая базисы в трех попарно различных одномерных подпространствах в двумерном пространстве мы получаем линейно зависимую систему.

Задача 7.27. *Пусть U, V, W — подпространства конечномерного линейного пространства.*

a) Верна ли формула

$$\dim(U+V+W) = \dim U + \dim V + \dim W - \dim(U \cap V) -$$
$$-\dim(V \cap W) - \dim(W \cap U) + \dim(U \cap V \cap W)\,?$$

b) Следует ли из условий $U \cap V = V \cap W = W \cap U = 0$ что сумма $U+V+W$ прямая? Если нет, то как нужно изменить приведенные условия, чтобы это было верно?

Если $V = U_1 \oplus \ldots \oplus U_k$, то для любого $v \in V$ существует и единствен такой набор векторов $u_1, \ldots, u_k$ ($u_i \in U_i$), что $v = u_1 + \ldots + u_k$. Следующий пример показывает, что проекции u_i зависят не только от U_i, но и от остальных слагаемых прямого разложения[30].

Пример 7.28. Пусть $\{e_1, \ldots, e_n\}$ — базис векторного пространства V. Тогда

$$V = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle.$$

Проекция вектора $v \in V$ на $\langle e_i \rangle$ равна $v_i e_i$, где v_i — i-я координата вектора v в базисе $\{e_1, \ldots, e_n\}$.

7.2 Линейные отображения и преобразования

В современной математике (особенно в алгебре) при определении математических объектов какого-то типа определяется также тип отображений между ними. Если объекты представляют собой множества с некоторой операцией (или набором операций), то естественное требование на такие отображения — согласованность с этой операцией (операциями). Например, для групп (колец и т.п.) рассматривают гомоморфизмы групп (колец и т.п.), а в случае линейных пространств — линейные отображения, к определению и изучению которых мы переходим.

[30] точнее, u_i зависит не от остальных слагаемых по отдельности, а от их прямой суммы $\oplus_{j \neq i} U_j$.

Определение 7.29. Отображение $\varphi\colon V \to U$ между линейными пространствами (над фиксированным полем $\mathbb{K}$) называется *линейным*, если

1) $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ для любых $v_1,\, v_2 \in V$ ("аддитивность");

2) $\varphi(\lambda v) = \lambda\varphi(v)$ для любых $v \in V$ и $\lambda \in \mathbb{K}$ ("однородность").

В качестве следствия получаем, что линейное отображение φ переводит конечную линейную комбинацию $\sum \lambda_i v_i$ векторов $v_i \in V$ в линейную комбинацию $\sum \lambda_i \varphi(v_i)$ векторов $\varphi(v_i) \in U$ с теми же коэффициентами.

Задача 7.30. *Для линейного* $\varphi\colon V \to U$ *докажите, что* $\varphi(0) = 0$, $\varphi(-v) = -\varphi(v)$, $\varphi(v_1 - v_2) = \varphi(v_1) - \varphi(v_2)$.

Замечание 7.31. В связи с предыдущим Определением можно задаться вопросом: следует ли однородность из аддитивности? Оказывается, ответ зависит от поля $\mathbb{K}$: при $\mathbb{K} = \mathbb{Q}$ следует (читателю предлагается это доказать), а уже́ при $\mathbb{K} = \mathbb{R}$ — нет. Пример аддитивного, но не линейного отображения $f\colon \mathbb{R} \to \mathbb{R}$ (здесь $\mathbb{R}$ обозначает одномерное линейное пространство над полем $\mathbb{R}$) можно построить так. Рассмотрим $\mathbb{R}$ как линейное пространство над полем $\mathbb{Q}$. Оно бесконечномерно (более точно, континуальномерно), и его элементы $1,\, \sqrt{2} \in \mathbb{R}$ линейно независимы над $\mathbb{Q}$. По лемме Цорна систему $\{1,\, \sqrt{2}\}$ можно продолжить до некоторого базиса E в $\mathbb{R}$ над $\mathbb{Q}$. Рассмотрим линейную над полем $\mathbb{Q}$ функцию $f\colon \mathbb{R} \to \mathbb{R}$, задаваемую условиями $f(1) = 1$, $f(e) = 0$ при $e \in E\backslash\{1\}$. Из $\mathbb{Q}$-линейности f следует ее аддитивность, в то же время она не линейна над полем $\mathbb{R}$: $0 = f(\sqrt{2}) \neq \sqrt{2} f(1) = \sqrt{2}$.

Кстати, для поля $\mathbb{K} = \mathbb{C}$ есть более простой пример аддитивного, но не линейного отображения $f\colon \mathbb{C} \to \mathbb{C}$, $f(a + bi) = b + ai$. Его аддитивность легко проверяется, в то же время $1 = f(i) \neq if(1) = -1$.

Важнейшим частным случаем линейного отображения является линейное преобразование.

Определение 7.32. *Линейным преобразованием* линейного пространства V или, что то же, *линейным оператором* на V, называется линейное отображение V в себя.

Приведем некоторые примеры линейных отображений и преобразований. Читателю предлагается проверить их линейность там, где это не сделано.

Пример 7.33. *Нулевое отображение* $\varphi\colon V \to U$, $\varphi(v) = 0\, \forall\, v \in V$.

Пример 7.34. *Нулевое преобразование* $\varphi\colon V \to V$, $\varphi(v) = 0\, \forall\, v \in V$.

Пример 7.35. *Тождественное преобразование* $\varphi\colon V \to V$, $\varphi(v) = v\, \forall\, v \in V$. Тождественное преобразование пространства V обозначается Id_V.

Пример 7.36. Зафиксируем некоторый скаляр $\lambda \in \mathbb{K}$. Определим линейное преобразование ("гомотетию") $\varphi = \lambda\, \mathrm{Id}_V\colon V \to V$, $\varphi(v) = \lambda v\, \forall\, v \in V$. При $\lambda = 0$ получаем нулевое преобразование, при $\lambda = 1$ — тождественное.

Пример 7.37. Пусть $V = U \oplus W$. Определим линейное отображение $\varphi = \mathrm{Pr}_U^{\|W}\colon V \to U$ — *проектор на* U *параллельно* W следующим образом. По определению прямой суммы для

любого $v \in V$ однозначно определены $u \in U$ и $w \in W$ такие, что $v = u + w$. Тогда $\varphi(v) := u \in U$. Проверим, что так определенное отображение φ линейно. Пусть $v_i = u_i + w_i$, $i = 1, 2$. Тогда $v_1 + v_2 = (u_1 + u_2) + (w_1 + w_2)$, откуда $\varphi(v_1 + v_2) = u_1 + u_2 = \varphi(v_1) + \varphi(v_2)$. Аналогично, если $v = u + w$, то $\lambda v = \lambda u + \lambda w$, и тогда $\varphi(\lambda v) = \lambda u = \lambda\varphi(v)$.

Пример 7.38. Пусть снова $V = U \oplus W$. Определим линейное преобразование $\varphi = \mathrm{Pr}_U^{\|W} : V \to V$, которое как и отображение из предыдущего примера называется *проектором на U параллельно W*, следующим образом. Для любого $v \in V$ однозначно определены $u \in U$ и $w \in W$ такие, что $v = u + w$. Тогда $\varphi(v) := u$, но в данном случае u рассматривается как элемент самого пространства V (так как $U \subset V$), поэтому φ на этот раз действует из V в V и является линейным преобразованием.

Пример 7.39. Обозначим через $\mathbb{R}[x]_n$ линейное пространство многочленов с вещественными коэффициентами степени не выше n. Пусть $k \geq 0$ — некоторое натуральное число. Обозначим $V := \mathbb{R}[x]_n$, $U := \mathbb{R}[x]_{n-k}$. Определим отображение $\varphi\colon V \to U$, $\varphi(p) = p^{(k)}$ $\forall\, p \in V$ (k-кратное дифференцирование). Читателю предлагается проверить его линейность.

Пример 7.40. Любой многочлен степени не выше $n - k$ (при $k \geq 0$) можно рассматривать и как многочлен степени не выше n, поэтому k-кратное дифференцирование определяет линейное преобразование $\mathbb{R}[x]_n \to \mathbb{R}[x]_n$.

Пример 7.41. Поворот евклидовой плоскости на данный угол вокруг фиксированной точки определяет линейное преобразование свободных векторов плоскости. Чтобы убедиться в его линейности, читателю предлагается нарисовать соответствующую картинку.

Пример 7.42. Пусть V — n-мерное линейное пространство. Тогда выбор базиса в V определяет линейное отображение $V \to \mathbb{K}^n$ (при этом вектору сопоставляется его координатный столбец в выбранном базисе), см. раздел 6.4.

С каждым линейным отображением $\varphi\colon V \to U$ связаны два линейных подпространства — его ядро и его образ (первое является подпространством в V, второе — в U).

Рассмотрим множество K векторов из V, которые φ отображает в 0. K не пусто: действительно, ему принадлежит нулевой вектор. Кроме того, из $v_1, v_2 \in K$ следует $v_1 + v_2 \in K$ ($\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) = 0 + 0 = 0$), а из $v \in K$ следует $\lambda v \in K$. Таким образом, K является линейным подпространством в V.

Определение 7.43. *Ядром* линейного отображения $\varphi\colon V \to U$ называется линейное подпространство в V, состоящее из векторов, которые φ отображает в нулевой вектор. Ядро линейного отображения φ обозначается $\operatorname{Ker}\varphi$.

Таким образом,

$$\operatorname{Ker}\varphi = \{v \in V \mid \varphi(v) = 0\} \subset V.$$

Рассмотрим теперь множество I векторов из U, которые являются образами векторов пространства V относительно линейного отображения φ (то есть такие $u \in U$, для которых

существует (хотя бы один) $v \in V$ такой, что $\varphi(v) = u$). Читателю предлагается проверить, что I — не просто подмножество, а подпространство в U.

Определение 7.44. *Образом* линейного отображения $\varphi\colon V \to U$ называется линейное подпространство в U, состоящее из векторов, которые является образами векторов пространства V относительно φ. Образ линейного отображения φ обозначается $\operatorname{Im}\varphi$.

Таким образом,

$$\operatorname{Im}\varphi = \{u \in U \mid \exists v \in V \,:\, \varphi(v) = u\} \subset U.$$

Заметим, что если $\varphi\colon V \to V$ — линейное преобразование, то $\operatorname{Ker}\varphi$ и $\operatorname{Im}\varphi$ являются подпространствами одного пространства V.

Приведем некоторые примеры (читателю рекомендуется найти ядра и образы для остальных приведенных выше примеров линейных отображений самостоятельно).

Пример 7.45. Ядро преобразования из Примера 7.38 совпадает с подпространством $W \subset V$, а образ — с $U \subset V$.

Пример 7.46. Ядро преобразования из Примера 7.40 совпадает с подпространством $\mathbb{R}[x]_{k-1} \subset \mathbb{R}[x]_n$, а образ — с подпространством $\mathbb{R}[x]_{n-k} \subset \mathbb{R}[x]_n$. Данный пример показывает, что ядро и образ линейного преобразования могут иметь нетривиальное (то есть ненулевое) пересечение!

Пример 7.47. Ядро преобразования из Примера 7.42 нулевое (в этом случае говорят “тривиальное”), а образ совпадает со всем пространством $\mathbb{K}^n$.

Следующее предложение показывает, что для инъективности линейного отображения достаточно, чтобы прообраз нулевого вектора (то есть ядро) состоял бы только из нуля.

Предложение 7.48. (Критерий инъективности и сюръективности). *Линейное отображение $\varphi\colon V \to U$ инъективно (соответственно сюръективно) тогда и только тогда, когда $\operatorname{Ker}\varphi = 0$ (соответственно $\operatorname{Im}\varphi = U$).*

Доказательство. Докажем ту часть, которая касается ядра (часть про образ непосредственно следует из определений). Если $\operatorname{Ker}\varphi \neq 0$, то существует $0 \neq v \in \operatorname{Ker}\varphi$, значит $\varphi(v) = \varphi(0) = 0$ и поэтому φ не инъективно.

Наоборот (это самое интересное), пусть φ не инъективно. Тогда существуют v_1, $v_2 \in V$, $v_1 \neq v_2$ такие, что $\varphi(v_1) = \varphi(v_2)$. Тогда $\varphi(v_1 - v_2) = \varphi(v_1) - \varphi(v_2) = 0$, а значит $0 \neq v_1 - v_2 \in \operatorname{Ker}\varphi$, поэтому $\operatorname{Ker}\varphi \neq 0$. ∎

То есть для инъективности линейного отображения достаточно, чтобы прообраз нулевого вектора был одноэлементным (состоящим из нулевого вектора), тогда автоматически прообразы всех элементов из образа будут одноэлементными (ср. Задачу 7.51 ниже).

Следствие 7.49. *Линейное отображение $\varphi\colon V \to U$ биективно тогда и только тогда, когда $\operatorname{Ker}\varphi = 0$ и $\operatorname{Im}\varphi = U$.*

Биективные линейные отображения образуют важный класс линейных отображений и называются изоморфизмами. Мы вернемся к ним немного позже.

Задача 7.50. *Пусть $\varphi\colon V \to U$ — биективное линейное отображение. Тогда для него существует теоретико-множественное обратное отображение φ^{-1}. Докажите, что φ^{-1} линейно.*

Пусть $\varphi\colon V \to U$ — произвольное линейное отображение. Определим *полный прообраз* вектора $u \in U$ как множество

$$\varphi^{-1}(u) := \{v \in V \mid \varphi(v) = u\} \subset V$$

(заметим, что обозначение $\varphi^{-1}(u)$ здесь не предполагает что φ обратимо, то есть биективно). Нетрудно проверить, что $\varphi^{-1}(u)$ является линейным подпространством в V тогда и только тогда, когда $u = 0$.

Посмотрим, как устроены полные прообразы векторов из U. Очевидно, что $\varphi^{-1}(u) \neq \varnothing \Leftrightarrow u \in \operatorname{Im}\varphi$.

Задача 7.51. *Предположим, что $u \in \operatorname{Im}\varphi$ и $v \in V$ такой, что $\varphi(v) = u$. Тогда*

$$\varphi^{-1}(u) = v + \operatorname{Ker}\varphi := \{v + v' \mid v' \in \operatorname{Ker}\varphi\}.$$

Решение. Пусть $v' \in \varphi^{-1}(u)$, тогда $v' - v \in \operatorname{Ker}\varphi$, и поэтому $v' \in v + \operatorname{Ker}\varphi$. Обратно, пусть $v' \in v + \operatorname{Ker}\varphi$, то есть $v' = v + w$, $w \in \operatorname{Ker}\varphi$. Тогда $\varphi(v') = \varphi(v) = u$, поэтому $v' \in \varphi^{-1}(u)$. ∎

Решив предыдущую задачу читатель, наверное, почувствовал аналогию между структурой множества $\varphi^{-1}(u)$ и общего решения совместной СЛУ. Такая аналогия действительно есть, мы объясним ее после того, как определим понятие матрицы линейного отображения. Мы увидим, что (при данных φ и u и "неизвестном" v) $\varphi(v) = u$ — "бескоординатная" запись СЛУ с соответствующей СЛОУ $\varphi(v) = 0$.

7.3 Задание линейных отображений на базисах. Изоморфизмы

Докажем Лемму, которая показывает, что линейные отображения удобно задавать их значениями на базисах.

Лемма 7.52. Если $\{e_1, \ldots, e_n\}$ — базис в V, то для любого векторного пространства U над тем же полем и любой системы векторов $\{u_1, \ldots, u_n\}$ в U существует и единственно такое линейное отображение $\varphi\colon V \to U$, что $\varphi(e_i) = u_i$, $i = 1, \ldots, n$.

Доказательство. Так как $\{e_1, \ldots, e_n\}$ является базисом в V, то произвольный вектор из V однозначно раскладывается по нему: $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$. Если линейное отображение $\varphi\colon V \to U$, удовлетворяющее условию леммы, существует, то $\varphi(v) = \lambda_1 u_1 + \ldots + \lambda_n u_n$. Таким образом, существует не более одного такого отображения. Теоретико-множественно φ

указанной формулой корректно определено. Осталось доказать его линейность. Проверим аддитивность. Пусть $w = \mu_1 e_1 + \ldots + \mu_n e_n \in V$. Тогда имеем

$$\varphi(v + w) = (\lambda_1 + \mu_1)u_1 + \ldots + (\lambda_n + \mu_n)u_n = \varphi(v) + \varphi(w).$$

Аналогично проверяется однородность. ■

Из доказанной Леммы можно сделать вывод, что для определения линейного отображения $\varphi\colon V \to U$ достаточно задать его значения на произвольном базисе V, причем с базиса линейное отображение по линейности продолжается на все пространство V однозначно.

Следующие Предложения отвечают на вопрос, когда заданное на базисе линейное отображение является инъективным или сюръективным.

Предложение 7.53. *Пусть V — линейное пространство, $\{e_1, \ldots, e_n\}$ — базис в V. Пусть U — еще одно пространство над тем же полем, $\{u_1, \ldots, u_n\}$ — система векторов в U. Тогда линейное отображение $\varphi\colon V \to U$ такое, что $\varphi(e_i) = u_i,\ \ i = 1, \ldots, n$ является инъективным тогда и только тогда, когда система $\{u_1, \ldots, u_n\}$ линейно независима.*

Доказательство. 1) Предположим, что система $\{u_1, \ldots, u_n\}$ линейно зависима и $\lambda_1 u_1 + \ldots + \lambda_n u_n = 0$ — нетривиальная линейная зависимость. Тогда ядро φ содержит ненулевой вектор $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$, следовательно, φ не инъективно.

Обратно, пусть φ не инъективно; тогда найдется $v \in V,\ \ v \neq 0$ такой, что $\varphi(v) = 0$. Пусть $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$ — его разложение по выбранному базису в V. Тогда $0 = \varphi(v) = \lambda_1 u_1 + \ldots + \lambda_n u_n$ — нетривиальная линейная зависимость между векторами системы $\{u_1, \ldots, u_n\}$. ■

Предложение 7.54. *Пусть $\varphi\colon V \to U$ и $\{e_1, \ldots, e_n\}$ — базис в V. Тогда $\operatorname{Im}\varphi = \langle \varphi(e_1), \ldots, \varphi(e_n) \rangle$.*

Доказательство. $u \in \operatorname{Im}\varphi \ \Leftrightarrow\ \exists v \in V$ такой, что $\varphi(v) = u \ \Leftrightarrow\ \exists \lambda_1, \ldots, \lambda_n \in \mathbb{K}$ такие, что $u = \sum_i \lambda_i \varphi(e_i) \ \Leftrightarrow\ u \in \langle \varphi(e_1), \ldots, \varphi(e_n) \rangle$. ■

Таким образом, отображение $\varphi\colon V \to U$, заданное (с использованием предыдущих обозначений) на базисе условиями $\varphi(e_i) = u_i,\ i = 1, \ldots, n$ сюръективно тогда и только тогда, когда $U = \langle u_1, u_2, \ldots, u_n \rangle$.

Следствие 7.55. *Линейное отображение $\varphi\colon V \to U$ биективно тогда и только тогда, когда для некоторого (а значит и для любого) базиса $\{e_1, \ldots, e_n\}$ в V система $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ является базисом в U.*

Задача 7.56. *Пусть V — конечномерное линейное пространство над полем $\mathbb{K}$. Докажите, что система векторов $\{e_1, \ldots, e_n\}$ является базисом в V тогда и только тогда, когда для любого векторного пространства U над тем же полем и любой системы векторов $\{u_1, \ldots, u_n\}$ в U существует и единственно такое линейное отображение $\varphi\colon V \to U$, что $\varphi(e_i) = u_i,\ \ i = 1, \ldots, n$.*

Теперь докажем следующую важную Теорему.

Теорема 7.57. *Пусть* $\varphi\colon V \to U$ *— линейное отображение, причем* V *конечномерно. Тогда* $\dim \operatorname{Im}\varphi + \dim \operatorname{Ker}\varphi = \dim V$.

Доказательство. Пусть для определенности $\dim V = n$. Тогда $\operatorname{Ker}\varphi$ — подпространство в V размерности $k \le n$. Пусть $\{e_1, \ldots, e_n\}$ — такой базис в V, что последние k его векторов $e_{n-k+1}, \ldots, e_n$ образуют базис в $\operatorname{Ker}\varphi$ (такой базис можно получить, выбирая базис в ядре и дополняя его до базиса во всем V).

Мы утверждаем, что система векторов $\{\varphi(e_1), \ldots, \varphi(e_{n-k})\}$ линейно независима и значит составляет базис в $\operatorname{Im}\varphi$ (поскольку из Предложения 7.54 следует, что они порождают $\operatorname{Im}\varphi$). Действительно, пусть $\lambda_1\varphi(e_1) + \ldots + \lambda_{n-k}\varphi(e_{n-k}) = 0$ — произвольная линейная зависимость. Тогда $\lambda_1 e_1 + \ldots + \lambda_{n-k}e_{n-k} \in \operatorname{Ker}\varphi$. Значит существуют $\mu_1, \ldots, \mu_k$ такие, что $\lambda_1 e_1 + \ldots + \lambda_{n-k}e_{n-k} = \mu_1 e_{n-k+1} + \ldots + \mu_k e_n$. Из линейной независимости $\{e_1, \ldots, e_n\}$ теперь следует, что все λ_i равны нулю. ∎

Замечание 7.58. Может показаться, что если $\varphi\colon V \to V$ — линейное преобразование, то предыдущую Теорему можно усилить так: $V = \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$. В общем случае **это неверно**: контрпример см. в Примере 7.46. См. также Задачу 7.59.

Задача 7.59. *Для каких конечномерных пространств* V *существует преобразование* $\varphi\colon V \to V$*, для которого* $\operatorname{Ker}\varphi = \operatorname{Im}\varphi$ *(как подпространства в* V*)?*

Решение. Если V — такое пространство и φ — преобразование как в условии, то $\dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = \dim V$ и $\dim \operatorname{Ker}\varphi = \dim \operatorname{Im}\varphi$, откуда следует, что $\dim V$ четна.

Обратно, пусть $\dim V = 2k$. Пусть $U \subset V$ — произвольное k-мерное подпространство. Выберем базис $\{e_1, \ldots, e_k\}$ в U и продолжим его векторами $\{e_{k+1}, \ldots, e_{2k}\}$ до базиса в V. Определим линейное преобразование $\varphi\colon V \to V$, полагая $\varphi(e_i) = 0$, $\varphi(e_{k+i}) = e_i$ при $1 \le i \le k$. Тогда легко проверить, что оно обладает требуемыми свойствами. В частности, $\operatorname{Ker}\varphi = \operatorname{Im}\varphi = U$.

Если хочется предъявить более "естественный" пример такого преобразования, то можно рассмотреть оператор $\varphi = \frac{d^k}{dx^k}\colon \mathbb{K}[x]_{2k-1} \to \mathbb{K}[x]_{2k-1}$, где $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$. ∎

Следствие 7.60. *Для конечномерных пространств* V *и* U *одинаковой размерности любое из условий 1)* $\operatorname{Ker}\varphi = 0$*, 2)* $\operatorname{Im}\varphi = U$ *влечет оставшееся.*

Рассмотрим более подробно биективные линейные отображения.

Пусть U и V — линейные пространства над полем $\mathbb{K}$.

Определение 7.61. Линейное отображение $\varphi\colon U \to V$ называется *изоморфизмом*, если оно биективно.

Из Следствия 7.60 вытекает, что для конечномерных пространств V и U одинаковой размерности выполнение любого из условий 1) $\operatorname{Ker}\varphi = 0$, 2) $\operatorname{Im}\varphi = U$ достаточно для того, чтобы линейное отображение $\varphi\colon V \to U$ было изоморфизмом.

Определение 7.62. Мы скажем, что пространство U *изоморфно* V, если существует изоморфизм $\varphi\colon U \to V$.

Линейные пространства, между которыми существует (хотя бы один) изоморфизм, называются *изоморфными*.

Заметим, что линейные пространства могут быть равномощными как множества, но не изоморфными (примеры таких пространств мы скоро получим). Это связано с тем, что не всякая биекция между линейными пространствами является линейной.

Предложение 7.63. *Отношение изоморфности на множестве всех линейных пространств над данным полем — отношение эквивалентности.*

Доказательство. Действительно, оно рефлексивно, так как тождественное отображение — изоморфизм.

Далее, оно симметрично. Это следует из того, что обратное отображение к изоморфизму — изоморфизм. Покажем это. Пусть $\varphi\colon U \to V$ — изоморфизм и $\varphi^{-1}\colon V \to U$ — обратное отображение для φ. Оно существует в силу биективности φ и определяется так: $\varphi^{-1}(v) = u$, если $v = \varphi(u)$. Докажем, что $\varphi^{-1}(v_1+v_2) = \varphi^{-1}(v_1)+\varphi^{-1}(v_2)\ \ \forall v_1,\, v_2 \in V$. Пусть $v_i = \varphi(u_i),\ i = 1, 2$. Тогда в силу линейности φ имеем $\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2) = v_1 + v_2$, откуда по определению обратного $\varphi^{-1}(v_1 + v_2) = u_1 + u_2 = \varphi^{-1}(v_1) + \varphi^{-1}(v_2)$. Аналогично доказывается равенство $\varphi^{-1}(\lambda v) = \lambda\varphi^{-1}(v)$.

Наконец, оно транзитивно. Это следует из того, что композиция изоморфизмов — изоморфизм. Покажем это. Пусть $\varphi\colon U \to V,\ \ \psi\colon V \to W$ — отображения, тогда определена их композиция $\psi \circ \varphi\colon U \to W,\ \ (\psi \circ \varphi)(u) = \psi(\varphi(u))\ \ \forall\, u \in U$. Если φ и ψ линейны, то их композиция $\psi \circ \varphi$ тоже линейна. Действительно,

$$(\psi \circ \varphi)(u_1 + u_2) = \psi(\varphi(u_1 + u_2)) = \psi(\varphi(u_1) + \varphi(u_2)) =$$

$$\psi(\varphi(u_1)) + \psi(\varphi(u_2)) = (\psi \circ \varphi)(u_1) + (\psi \circ \varphi)(u_2).$$

Аналогично проверяется равенство $(\psi \circ \varphi)(\lambda u) = \lambda(\psi \circ \varphi)(u)$. Поскольку композиция биекций является биекцией, отсюда следует, что композиция изоморфизмов — изоморфизм. ■

Тот факт, что два пространства U и V изоморфны, обозначают $U \cong V$.

Таким образом, возникает задача классифицировать линейные пространства над данным полем с точностью до изоморфизма (описать классы указанной эквивалентности). Следующая теорема решает ее для конечномерных пространств — единственным инвариантом изоморфизма линейного пространства является его размерность.

Теорема 7.64. *Два конечномерных пространства U, V над полем $\mathbb{K}$ изоморфны тогда и только тогда, когда они имеют одинаковую размерность.*

Доказательство. Из Следствия 7.55 вытекает, что если между U и V есть изоморфизм, то $\dim V = \dim U$.[31]

Наоборот, предположим что $\dim V = \dim U$ и $\{e_1, \dots, e_n\}$, $\{f_1, \dots, f_n\}$ — базисы в пространствах V и U соответственно. Определим линейное отображение $\varphi\colon U \to V$, задав его значения на базисных векторах $\varphi(e_i) = f_i$, $i = 1, \dots, n$, как в Лемме 7.52. Снова применяя Следствие 7.55 получаем, что такое φ биективно, то есть изоморфизм. ∎

Заметим, что Предложение 6.53 означает, что выбор базиса в n-мерном пространстве V определяет его изоморфизм с $\mathbb{K}^n$. Таким образом, в каждом классе изоморфизма конечномерных векторных пространств есть конкретный представитель — пространство $\mathbb{K}^n$.

Как уже отмечалось выше, существуют векторные пространства, которые равномощны, но не изоморфны. Читатель, возможно, знает, что каждое множество вида $\mathbb{R}^n$, $n > 0$, имеет мощность континуума, но как следует из доказанной теоремы, при разных n они не изоморфны как линейные пространства — любая биекция между ними не является линейной.

Замечание 7.65. (ср. Замечание 7.31) Заметим, что с использованием аксиомы выбора можно доказать, что аддитивные группы всех пространств $\mathbb{R}^n$, $n > 0$ изоморфны. В самом деле, эти пространства изоморфны как линейные пространства над полем $\mathbb{Q}$, поскольку все они имеют одинаковую размерность (континуум). Это еще раз (см. Замечание 7.31) показывает, что условие однородности в определении линейного отображения над произвольным полем (в частности, над $\mathbb{R}$) не следует из условия аддитивности.

7.4 Матрица линейного отображения

Пусть $\varphi\colon V \to U$ — линейное отображение между конечномерными линейными пространствами, $\{e_1, \dots, e_n\}$, $\{f_1, \dots, f_m\}$ — базисы в V и U соответственно.

Определение 7.66. Матрица A размера $m \times n$ называется *матрицей линейного отображения* φ относительно выбранных базисов, если

$$(\varphi(e_1), \varphi(e_2), \dots, \varphi(e_n)) = (f_1, f_2, \dots, f_m)A.$$

То есть рецепт получения матрицы A такой: действуем отображением на векторы выбранного в V базиса и получившиеся векторы из U раскладываем по выбранному базису в U, результат записываем в столбцы A (i-й столбец матрицы A — координатный столбец вектора $\varphi(e_i)$ в базисе $\{f_1, \dots, f_m\}$).

Пусть $\mathcal{L}(V, U)$ обозначает множество всех линейных отображений $V \to U$. Заметим, что матрица A однозначно определена отображением φ и выбранными базисами. Тем самым

[31] Также для доказательства можно использовать Теорему 7.57 вместе с условиями инъективности и сюръективности в терминах ядра и образа.

сопоставление линейному отображению его матрицы в выбранной паре базисов задает некоторое отображение $\mu = \mu_{e,f} \colon \mathcal{L}(V, U) \to \mathrm{Mat}_{m\times n}(\mathbb{K})$.

Предложение 7.67. *Отображение μ является биекцией (зависящей от выбранных базисов в V и U).*

Доказательство. Действительно, если два линейных отображения имеют одинаковые матрицы в данной паре базисов, то их значения на базисных векторах равны, а по Лемме 7.52 эти значения линейное отображение однозначно определяют.

С другой стороны, так как согласно все той же Лемме набор значений линейного отображения на базисных векторах может быть произвольным, то любая матрица размера $m \times n$ с элементами из поля $\mathbb{K}$ является матрицей некоторого линейного отображения в выбранной паре базисов. ■

Далее мы покажем, что построенная биекция согласована с операциями над матрицами (сложения, умножения на скаляры и композиции). Ситуация является аналогичной биекции между множеством векторов n-мерного линейного пространства V над полем $\mathbb{K}$ и множеством столбцов $\mathbb{K}^n$, зависящей от базиса и задаваемой сопоставлением вектору его координатного столбца.

Частным случаем линейного отображения является линейное преобразование — это линейное отображение из пространства в себя. Так как при определении матрицы линейного отображения мы в каждом пространстве выбираем по одному базису, то матрица линейного преобразования определяется с помощью выбора одного базиса в V. Так как этот частный случай особенно важен, то приведем специализацию предыдущего определения на случай линейных преобразований.

Пусть $\varphi \colon V \to V$ — линейное преобразование конечномерного линейного пространства V, $\{e_1, \ldots, e_n\}$ — выбранный базис в V.

Определение 7.68. Матрица A порядка n называется *матрицей линейного преобразования φ* в выбранном базисе, если

$$(\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)) = (e_1, e_2, \ldots, e_n)A.$$

То, что в определении матрицы линейного преобразования участвует только один базис отражает большую “жесткость” линейных преобразований по сравнению с отображениями и приводит к более богатой и тонкой теории для одного линейного преобразования, как мы убедимся в дальнейшем.

Задача 7.69. *Напишите матрицы следующих линейных преобразований:*

1) *тождественного преобразования n-мерного пространства V в произвольном базисе в V;*

2) *проектора на подпространство U параллельно подпространству W (см. Пример (7.38)), заданного разложением $V = U \oplus W$ пространства V в прямую сумму ненулевых подпространств, в базисе V, полученном объединением базисов U и W;*

3) *оператора дифференцирования $\frac{d}{dx}$ на пространстве $\mathbb{R}[x]_n$ в базисе $\{1, x, x^2, \dots, x^n\}$;*

4) *оператора из предыдущего пункта в базисе $\{1, \frac{x}{1!}, \frac{x^2}{2!}, \dots, \frac{x^n}{n!}\}$;*

5) *оператора дифференцирования на линейной оболочке $\langle \sin x, \cos x \rangle$ в базисе $\{\sin x, \cos x\}$;*

6) *оператора поворота на угол α против часовой стрелки в правом ортонормированном базисе $\{e_1, e_2\}$ на евклидовой плоскости.*

Лемма 7.52 говорит о том, что зная матрицу A линейного отображения φ и относительно каких базисов она записана, можно восстановить само отображение φ.

Предложение 7.70. *Если $\xi := (v_1, \dots, v_n)^T$ — координатный столбец вектора $v \in V$ в базисе $\{e_1, \dots, e_n\}$, то $A\xi$ — координатный столбец вектора $\varphi(v) \in U$ в базисе $\{f_1, \dots, f_m\}$.*

Доказательство. Воспользуемся матричной записью $v = (e_1, \dots, e_n)(v_1, \dots, v_n)^T$ разложения вектора по базису. Из линейности φ следует

$$\varphi(v) = (\varphi(e_1), \dots, \varphi(e_n))(v_1, \dots, v_n)^T = (f_1, \dots, f_m)A(v_1, \dots, v_n)^T = (f_1, \dots, f_m)(u_1, \dots, u_m)^T,$$

где $\eta := (u_1, \dots, u_m)^T$ — координатный столбец вектора $\varphi(v)$ в базисе $\{f_1, \dots, f_m\}$. Из линейной независимости последнего следует $\eta = A(v_1, \dots, v_n)^T$. ∎

Предыдущее Предложение показывает, зачем нужны матрицы линейных отображений: действие линейного отображения в базисах сводится просто к умножению координатных столбцов векторов на его матрицу.

Доказанный в Предложении результат можно наглядно изобразить как условие коммутативности диаграммы

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & U \\ {\scriptstyle \varphi_e}\downarrow & & \downarrow{\scriptstyle \varphi_f} \\ \mathbb{K}^n & \xrightarrow{A\cdot} & \mathbb{K}^m, \end{array} \tag{53}$$

в которой вертикальные стрелки обозначают определяемые выбранными базисами линейные биекции, сопоставляющие вектору его координатный столбец (см. Предложение 6.53). Доказанное Предложение равносильно тому, что два пути по стрелкам из V в $\mathbb{K}^m$ совпадают.

Матрица линейного отображения зависит от выбора базисов. Выведем формулу, выражающую матрицу отображения в новых базисах через матрицу того же отображения в старых базисах и матрицы перехода от старых базисов к новым.

Предложение 7.71. *Пусть $\varphi\colon V \to U$ — линейное отображение, A — его матрица относительно старых базисов $\{e_1, \dots, e_n\}$ и $\{f_1, \dots, f_m\}$ в V и U соответственно, C — матрица перехода от $\{e_1, \dots, e_n\}$ к новому базису в V $\{e'_1, \dots, e'_n\}$, а D — матрица перехода от $\{f_1, \dots, f_m\}$ к новому базису $\{f'_1, \dots, f'_m\}$ в U. Пусть A' — матрица отображения φ относительно новых базисов. Тогда*

$$A' = D^{-1}AC. \tag{54}$$

В частности, если φ — линейное преобразование (то есть $U = V$), то

$$A' = C^{-1}AC. \tag{55}$$

Доказательство. Из линейности φ непосредственно следует, что

$$(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C \quad \text{влечет} \quad (\varphi(e'_1), \dots, \varphi(e'_n)) = (\varphi(e_1), \dots, \varphi(e_n))C.$$

Поэтому (с учетом ассоциативности произведения матриц) имеем

$$(\varphi(e'_1), \dots, \varphi(e'_n)) = (\varphi(e_1), \dots, \varphi(e_n))C = (f_1, \dots, f_m)AC = (f'_1, \dots, f'_m)D^{-1}AC,$$

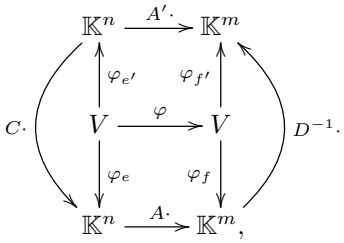
откуда $A' = D^{-1}AC$ — матрица φ относительно новых базисов. ∎

Заметим связь между формулами изменения координат вектора (49) и матрицы линейного отображения (54) при замене базисов: если $x \in \mathbb{K}^n$ и $y \in \mathbb{K}^m$ — координатные столбцы векторов $v \in V$ и $u \in U$ в базисах e и f соответственно и $u = \varphi(v)$, то для матрицы A линейного отображения φ в базисах e, f имеем равенство $y = Ax$. Теперь для координатного столбца $x' = C^{-1}x$ вектора v в базисе e' имеем

$$A'x' = D^{-1}ACC^{-1}x = D^{-1}Ax = D^{-1}y = y',$$

что равно координатному столбцу y' вектора $u = \varphi(v)$ в базисе f' (чего, конечно, и следовало ожидать).

Замечание 7.72. Еще один вывод формулы (54) можно извлечь из коммутативности диграммы



(56)

построенной из коммутативных диаграмм (53) и (50).

Задача 7.73. *Матрицы каких линейных отображений не зависят от выбора базисов? Матрицы каких линейных преобразований не зависят от выбора базиса?*

Мы видим, что за исключением очень специальных случаев, матрицы линейных преобразований и отображений зависят от базисов. Какие свойства матриц одного и того

же отображения (преобразования) от базиса не зависят? Нет ли простого критерия того, что две данные матрицы одинакового размера являются матрицами одного и того же отображения (преобразования) относительно разных базисов?

Вообще, формализовать эту задачу для отображений можно так. Назовем две прямоугольные матрицы одинакового размера эквивалентными, если они являются матрицами одного того же линейного отображения в разных базисах. Равносильно, две матрицы A и A' назовем эквивалентными, если существуют две невырожденные матрицы C, D подходящих порядков такие, что $A' = D^{-1}AC$ (читателю предлагается проверить, что это — действительно отношение эквивалентности). Теперь задача свелась к описанию классов введенной эквивалентности.

Аналогично, для преобразований назовем две матрицы одинаковых порядков A и A' эквивалентными, если найдется такая невырожденная матрица C, что $A' = C^{-1}AC$ (это условие равносильно тому, что две данные матрицы A и A' являются матрицами одного и того же линейного преобразования в разных базисах).

Второе отношение эквивалентности (для преобразований) намного более "жесткое" в том смысле, что классов эквивалентности больше (для полей $\mathbb{R}$ или $\mathbb{C}$ за исключением случая преобразований нульмерного пространства их будет континуум) и их описание — намного более сложная задача, которую мы в этом курсе полностью решим лишь для случая алгебраически замкнутого поля $\mathbb{C}$ (в разделе про жорданову нормальную форму). Пока же мы займемся изучением первого из определенных выше отношений эквивалентности (для отображений).

Во-первых, докажем следующее Предложение.

Предложение 7.74. *Если A — матрица линейного отображения $\varphi\colon V \to U$ (относительно произвольной пары базисов), то* $\operatorname{rk} A = \dim \operatorname{Im} \varphi$.

Доказательство. Согласно Предложению 7.54, для любого базиса $\{e_1, \dots, e_n\}$ $\operatorname{Im}\varphi = \langle \varphi(e_1), \dots, \varphi(e_n)\rangle$. По определению матрицы отображения A, ее столбцы — координатные столбцы образов базисных векторов $\varphi(e_1), \dots, \varphi(e_n)$ (относительно выбранного базиса в U). Из этих двух фактов следует, что при отождествлении U с координатным пространством $\mathbb{K}^m$ (задаваемым выбранным базисом в U) подпространство $\operatorname{Im}\varphi \subset U$ отождествляется с линейной оболочкой столбцов матрицы A в $\mathbb{K}^m$, размерность которой равна рангу матрицы A (ср. Следствие 6.54). ∎

Приведем модификацию предыдущего доказательства. Координатные столбцы векторов из $\operatorname{Im}\varphi$ — в точности те столбцы b, для которых система $Ax = b$ разрешима, то есть выбор базиса в U отождествляет $\operatorname{Im}\varphi$ с линейной оболочкой столбцов матрицы A, размерность которой, как мы знаем, равна $\operatorname{rk} A$.

Замечание 7.75. Заметим, кстати, что так как при элементарных преобразованиях столбцов матрицы A их линейная оболочка не меняется, то из формулы (54) следует, что она не зависит от базиса в V, как и должно быть, поскольку $\operatorname{Im}\varphi$ — подпространство в U, зависящее только от φ. Та же формула

показывает, что линейная оболочка столбцов зависит от базиса в U, поскольку его выбор задает способ отождествления U с $\mathbb{K}^m$.

Следствие 7.76. *Ранг матрицы линейного отображения не зависит от выбора базисов, в которых она записана.*

Доказательство. Действительно, ранг равен размерности образа линейного отображения, а она ни от каких базисов не зависит. ■

Замечание 7.77. Другое доказательство предыдущего Следствия можно получить, используя Задачу 6.31.

Таким образом, если две матрицы данного размера являются матрицами одного и того же линейного отображения, то их ранги равны[32]. Оказывается, верно и обратное, то есть ранг является единственным инвариантом для матриц линейных отображений. Это вытекает из следующего Предложения.

Предложение 7.78. *Если для линейного отображения $\varphi\colon V \to U$ $r := \dim \operatorname{Im} \varphi$, то существует пара базисов, относительно которых матрица φ имеет блочно-диагональный вид*

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Доказательство. 1-й способ. Построим базис $\{e_1, \ldots, e_n\}$ в V такой, что его последние $n-r$ векторов образуют базис в $\operatorname{Ker} \varphi \subset V$. Аналогичный базис (при $r = n - k$) уже строился в доказательстве Теоремы 7.57, где было доказано, что система векторов $\{\varphi(e_1), \ldots, \varphi(e_r)\}$ из U линейно независима. Положим $f_1 := \varphi(e_1), \ldots, f_r := \varphi(e_r)$ и продолжим данную систему до базиса $\{f_1, \ldots, f_m\}$ в U. Теперь легко проверяется, что в паре базисов $\{e_1, \ldots, e_n\}$ в V и $\{f_1, \ldots, f_m\}$ в U матрица линейного отображения φ имеет требуемый вид.

2-й способ. Напомним, что любая невырожденная матрица является произведением элементарных, и обратно, произведение конечного числа элементарных матриц невырождено. Формула $A' = D^{-1}AC$ показывает, что замена базиса в V отвечает композиции элементарных преобразований столбцов матрицы A, в то время как замена базиса в U отвечает композиции элементарных преобразований строк матрицы A. С помощью элементарных преобразований строк и столбцов любую прямоугольную матрицу ранга r можно привести к виду из условия Предложения. ■

Таким образом, для матриц размера $m \times n$ получается $\min(m, n) + 1$ классов указанной эквивалентности, что отвечает возможным значениям ранга таких матриц.

Задача 7.79. *Докажите, что*

[32]Это позволяет определить понятие ранга линейного отображения как ранга любой его матрицы. В силу доказанного выше это — просто другое название для размерности его образа.

1) ранг матрицы сюръективного линейного отображения равен числу ее строк;

2) ранг матрицы инъективного линейного отображения равен числу ее столбцов.

Решение. Пусть A — матрица $\varphi\colon V \to U$, $\dim V = n$, $\dim U = m$. Тогда размер A равен $m \times n$. Сюръективность φ равносильна тому, что $\operatorname{Im}\varphi = U$, откуда $\dim \operatorname{Im}\varphi = m$, а по Предложению 7.74 $\dim \operatorname{Im}\varphi = \operatorname{rk} A$, откуда следует пункт 1).

Инъективность φ равносильна тому, что $\operatorname{Ker}\varphi = 0$, что в свою очередь равносильно тому, что СЛОУ $Ax = 0$ имеет только тривиальное решение, что равносильно тому, что столбцы матрицы A линейно независимы, то есть $\operatorname{rk} A$ равен их числу, то есть n. ■

В оставшейся части этого параграфа применим полученные результаты о линейных отображениях к системам линейных уравнений.

Пусть $\varphi\colon V \to U$ — линейное отображение. Выбирая базисы $\{e_1, \dots, e_n\}$ в V и $\{f_1, \dots, f_m\}$ в U мы отождествляем V и U с пространствами столбцов $\mathbb{K}^n$ и $\mathbb{K}^m$ соответственно, при этом применение линейного отображения φ к вектору $v \in V$ сводится к умножению координатного столбца ξ этого вектора (в базисе $\{e_1, \dots, e_n\}$) на матрицу A отображения φ относительно указанных базисов (см. Предложение 7.70 и диаграмму (53)). Теперь легко видеть, что ядро отображения φ — то есть подпространство векторов $v \in V$ таких, что $\varphi(v) = 0$ — при указанном отождествлении совпадает с подпространством столбцов $x \in \mathbb{K}^n$ таких, что $Ax = 0$, то есть с пространством решений СЛОУ с матрицей коэффициентов A. В то же время образ φ отождествляется с подпространством таких столбцов $b \in \mathbb{K}^m$, для которых система $Ax = b$ разрешима, то есть с линейной оболочкой столбцов матрицы A.

Наглядно вышесказанное выражает следующая диаграмма

$$\begin{array}{ccccc} \operatorname{Ker}\varphi & \subset & V & \supset & \operatorname{Im}\varphi \\ \downarrow & & \downarrow{\scriptstyle \varphi_e} \quad \xrightarrow{\varphi} \quad \downarrow{\scriptstyle \varphi_f} & & \downarrow \\ \{x \mid Ax = 0\} & \subset & \mathbb{K}^n \xrightarrow{A\cdot} \mathbb{K}^m & \supset & \langle a_1, \dots, a_n \rangle, \end{array}$$

в которой $a_1, \dots, a_n$ — столбцы матрицы A.

Заметим, что Теорема 7.57 теперь дает еще одно, независимое доказательство Теоремы 6.42 о размерности пространства решений СЛОУ. Действительно, число неизвестных $n = \dim V$, $r = \operatorname{rk} A = \dim \operatorname{Im}\varphi$, а размерность пространства решений $\dim \operatorname{Ker}\varphi$ по Теореме 7.57 равна $n - r$.

Также легко видеть, что пункт 2) Теоремы 6.41 следует из Задачи 7.51 (в то время как пункт 1) следует из того, что ядро линейного отображения — подпространство).

Задача 7.80. *Докажите, используя линейные отображения и их матрицы, следующее утверждение. Для данной матрицы A системы линейных уравнений $Ax = b$ совместны при любом столбце b тогда и только тогда, когда ранг матрицы A равен числу ее строк (ср. Задачу 6.52).*

Решение. Любая матрица A размера $m \times n$ является матрицей некоторого линейного отображения $\varphi\colon V \to U$, где $\dim V = n$, $\dim U = m$, относительно выбранных базисов. Напомним, что $\operatorname{rk} A = \dim \operatorname{Im} \varphi$. Условие совместности систем $Ax = b$ при любом столбце b равносильно сюръективности φ, что, в свою очередь, равносильно $\operatorname{Im} \varphi = U$, то есть $\operatorname{rk} \varphi = \dim U = m$. ∎

7.5 Операции с линейными отображениями

Как мы увидим, операции на линейных отображениях аналогичны операциям с матрицами, но так как операции на отображениях с точки зрения математики более фундаментальны, мы их определим независимо.

Пусть $\varphi, \psi\colon V \to U$ — пара линейных отображений между одними и теми же пространствами. Тогда можно определить их сумму как такое отображение $\varphi + \psi\colon V \to U$, что $(\varphi + \psi)(v) = \varphi(v) + \psi(v)\ \forall\, v \in V$. Читателю предлагается провести несложную проверку линейности $\varphi + \psi$, а также следующего утверждения: если A и B — матрицы φ и ψ соответственно относительно базисов $\{e_1, \ldots, e_n\}$ в V и $\{f_1, \ldots, f_m\}$ в U, то матрица $\varphi + \psi$ относительно той же пары базисов равна $A + B$.

Кроме того, линейные отображения можно умножать на скаляры: $(\lambda\varphi)(v) = \lambda\varphi(v)\ \forall\, v \in V$, эта операция отвечает умножению матрицы на тот же скаляр.

Далее непосредственно проверяется, что множество $\mathcal{L}(V, U)$ (см. абзац перед Предложением 7.67) всех линейных отображений $\varphi\colon V \to U$ относительно определенных операций сложения и умножения на скаляры является векторным пространством. Более того, установленная в Предложении 7.67 биекция $\mu\colon \mathcal{L}(V, U) \to \operatorname{Mat}_{m\times n}(\mathbb{K})$ является линейным отображением, то есть изоморфизмом линейных пространств.

Пусть у нас есть два линейных отображения $\varphi\colon V \to U$ и $\psi\colon U \to W$. Тогда определена их композиция $\psi \circ \varphi\colon V \to W$, которая (как было проверено в доказательстве Предложения 7.63) также является линейным отображением. Пусть $\{e_1, \ldots, e_n\}$, $\{f_1, \ldots, f_m\}$, $\{g_1, \ldots, g_k\}$ — выбранные базисы соответственно в пространствах V, U и W, а A и B — матрицы φ и ψ в них.

Предложение 7.81. *В введенных выше обозначениях матрица D композиции $\psi \circ \varphi$ относительно пары базисов $\{e_1, \ldots, e_n\}$ и $\{g_1, \ldots, g_k\}$ есть BA.*

Доказательство. Имеем

$$(\varphi(e_1), \ldots, \varphi(e_n)) = (f_1, \ldots, f_m)A,$$

то есть $\varphi(e_k) = a_{1k}f_1 + \ldots + a_{mk}f_m$ при $1 \leq k \leq n$. Из линейности ψ следует, что $\psi(\varphi(e_k)) = a_{1k}\psi(f_1) + \ldots + a_{mk}\psi(f_m)$ при $1 \leq k \leq n$, то есть

$$(\psi(\varphi(e_1)), \ldots, \psi(\varphi(e_n))) = (\psi(f_1), \ldots, \psi(f_m))A,$$

откуда, используя равенство

$$(\psi(f_1),\dots,\psi(f_m)) = (g_1,\dots,g_k)B,$$

получаем

$$(\psi(\varphi(e_1)),\dots,\psi(\varphi(e_n))) = ((g_1,\dots,g_k)B)A.$$

Проверим прямым вычислением (ср. доказательство Предложения 6.59), что $((g_1,\dots,g_k)B)A = (g_1,\dots,g_k)(BA)$, откуда будет следовать, что $D = BA$. В самом деле, для любого $1 \le l \le n$

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{k} g_i b_{ij}\right) a_{jl} = \sum_{\substack{1\le i\le k,\\ 1\le j\le m}} g_i b_{ij} a_{jl} = \sum_{i=1}^{k} g_i \left(\sum_{j=1}^{m} b_{ij} a_{jl}\right),$$

то есть $\psi(\varphi(e_l)) = \sum_{i=1}^{k} g_i d_{il}$, где $d_{il} = \sum_{j=1}^{m} b_{ij} a_{jl}$. ∎

Доказанный результат о том, что матрица композиции линейных отображений φ и ψ есть произведение их матриц (в соответствующих базисах) служит основной мотивацией определения произведения матриц, данного в начале этого курса.

Заметим, что эта формула верна и для матрицы композиции линейных *преобразований* пространства V (в этом случае все матрицы записываются в фиксированном базисе $\{e_1,\dots,e_n\}$ пространства V).

Задача 7.82. *Из того, что композиция поворотов евклидовой плоскости на углы α и β есть поворот на угол $\alpha+\beta$, получите "формулы сложения" для тригонометрических функций. (Указание: перемножьте матрицы поворотов на указанные углы, записанные в ортонормированном базисе).*

Задача 7.83. *Пусть $V = U \oplus W$ и $\varphi\colon V \to V$ — проектор на подпространство U параллельно его прямому дополнению W (см. Пример 7.38). Докажите, что φ удовлетворяет тождеству $\varphi^2 = \varphi$*[33].

Заметим, что из предыдущей Задачи следует, что матрица проектора A в произвольном базисе удовлетворяет равенству $A^2 = A$.

Роль единичных матриц играют тождественные операторы: для любого $\varphi\colon V \to U$ выполнены соотношения $\mathrm{Id}_U \circ \varphi = \varphi = \varphi \circ \mathrm{Id}_V$.

Рассмотрим теперь аналог для линейных отображений операции взятия обратной матрицы.

Пусть линейное отображение $\varphi\colon V \to U$ биективно, то есть изоморфизм. Тогда его матрица A (относительно произвольной пары базисов) невырождена. Действительно, так

[33] Верно и обратное: любой оператор, удовлетворяющий указанному тождеству, является проектором на $U := \operatorname{Im}\varphi$ параллельно $W := \operatorname{Ker}\varphi$, в частности, последние два пространства образуют прямую сумму. Это мы докажем далее в Примере 8.5.

как тогда $\dim V = \dim U$, то A квадратная и, например, из инъективности φ следует, что столбцы A линейно независимы (см. Задачу 7.79). Легко также непосредственно доказать, что A обратима.

Задача 7.84. *Пусть A — матрица изоморфизма $\varphi\colon V \to U$ относительно базисов $\{e_1, \dots, e_n\}$ в V и $\{f_1, \dots, f_n\}$ в U. Тогда матрицей обратного отображения $\varphi^{-1}\colon U \to V$ (которое, как мы знаем из доказательства Предложения 7.63, тоже линейно) относительно базисов $\{f_1, \dots, f_n\}$ и $\{e_1, \dots, e_n\}$ будет A^{-1}.*

Решение. Пусть B — матрица φ^{-1} относительно базисов $\{f_1, \dots, f_n\}$ и $\{e_1, \dots, e_n\}$. Тогда из тождеств

$$\varphi^{-1} \circ \varphi = \mathrm{Id}_V, \quad \varphi \circ \varphi^{-1} = \mathrm{Id}_U$$

получаем $BA = E$, $AB = E$, а это и значит что $B = A^{-1}$. ■

Установленная связь умножения матриц с композицией линейных отображений позволяет дать концептуальное доказательство ассоциативности умножения матриц. А именно, если $\chi\colon W \to Z$ — еще одно линейное отображение с матрицей C относительно пары базисов $\{g_1, \dots, g_k\}$ в W и $\{h_1, \dots, h_l\}$ в Z соответственно, то матрицей композиции $(\chi \circ \psi) \circ \varphi$ относительно базисов $\{e_1, \dots, e_n\}$ и $\{h_1, \dots, h_l\}$ будет $(CB)A$, а композиции $\chi \circ (\psi \circ \varphi)$ — $C(BA)$. Но мы знаем, что композиция отображений ассоциативна, поэтому $(\chi \circ \psi) \circ \varphi = \chi \circ (\psi \circ \varphi)$, откуда, используя биекцию между отображениями и матрицами, получаем $(CB)A = C(BA)$.

Композиция линейных отображений связана с линейными операциями тождествами

$$\chi \circ (\varphi + \psi) = \chi \circ \varphi + \chi \circ \psi, \quad (\chi + \psi) \circ \varphi = \chi \circ \varphi + \psi \circ \varphi,$$

$$(\lambda\psi) \circ \varphi = \psi \circ (\lambda\varphi) = \lambda(\psi \circ \varphi) \quad \forall \lambda \in \mathbb{K}.$$

Читатель легко убедится в их справедливости. Они отвечают аналогичным операциям над матрицами.

Заметим, что на пространстве $\mathcal{L}(V, V) =: \mathcal{L}(V)$ операция композиции линейных преобразований определяет умножение; в этом случае *алгебра* (см. Определение 1.69) $\mathcal{L}(V)$ изоморфна *алгебре* матриц $\mathrm{Mat}_n(\mathbb{K})$ порядка n.

Обратимые линейные операторы на V образуют группу относительно операции композиции. Она обозначается $\mathrm{GL}(V)$. Выбор базиса в V определяет ее изоморфизм с группой невырожденных матриц $\mathrm{GL}_n(\mathbb{K})$ порядка $n = \dim V$ относительно умножения.

Задача 7.85. *Пусть $U \xrightarrow{\varphi} V \xrightarrow{\psi} W$ — композиция линейных отображений. Оцените сверху $\dim(\mathrm{Im}(\psi\varphi))$ через $\dim(\mathrm{Im}\,\varphi)$ и $\dim(\mathrm{Im}\,\psi)$. Выведите из полученного результата теорему о ранге произведения матриц.*

Решение. С одной стороны, $\mathrm{Im}(\psi\varphi) \subset \mathrm{Im}\,\psi$, поэтому $\dim \mathrm{Im}(\psi\varphi) \leq \dim \mathrm{Im}\,\psi$. С другой стороны,

$$\mathrm{Im}(\psi\varphi) = \{w \in W \mid \exists u \in U\colon w = \psi(\varphi(u))\} = \{w \in W \mid \exists v \in \mathrm{Im}\,\varphi\colon w = \psi(v)\} = \mathrm{Im}(\psi|_{\mathrm{Im}\,\varphi}),$$

поэтому $\dim \mathrm{Im}(\psi\varphi) \leq \dim \mathrm{Im}\,\varphi$. Из этого очевидно, что ранг произведения матриц не превосходит рангов сомножителей. ■

Задача 7.86. *Пусть* $U \xrightarrow{\varphi} V \xrightarrow{\psi} W$ *— композиция линейных отображений, причем* $\dim V = n$, $\dim(\operatorname{Im}\psi) = r$. *Известно, что* $\psi\varphi = 0$. *Оцените сверху* $\dim(\operatorname{Im}\varphi)$. *Как это связано с Задачей 6.48?*

Решение. Заметим, что $\psi\varphi = 0$ тогда и только тогда, когда $\operatorname{Im}\varphi \subseteq \operatorname{Ker}\psi$. Кроме того, $\dim\operatorname{Ker}\psi = n - r$. Из этого следует, что $\dim(\operatorname{Im}\varphi) \leq n - r$. Положив $U = \operatorname{Ker}\psi$ и взяв в качестве φ вложение $\operatorname{Ker}\psi \subset V$, мы видим, что оценка точная. ■

Следующая задача обобщает предыдущую.

Задача 7.87. *1) Пусть* $U \xrightarrow{\varphi} V \xrightarrow{\psi} W$ *— композиция линейных отображений, причем* $\dim V = n$, $\dim(\operatorname{Im}\psi) = r_2$, $\dim(\operatorname{Im}\varphi) = r_1$. *Докажите, что* $\dim(\operatorname{Im}(\psi\varphi)) \geq r_1 + r_2 - n$.

2) Пусть

$$V \xrightarrow{\varphi_1} V \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_k} V$$

— последовательность линейных преобразований пространства V, *тогда*

$$\dim\operatorname{Ker}(\varphi_k \circ \ldots \circ \varphi_1) \leq \dim\operatorname{Ker}(\varphi_1) + \ldots + \dim\operatorname{Ker}(\varphi_k).$$

Решение. 1) Пусть $L \subset \varphi(U)$ — произвольное прямое дополнение к подпространству $\varphi(U) \cap \operatorname{Ker}\psi$ в $\varphi(U)$. Легко проверить, что ограничение ψ на L индуцирует изоморфизм $L \cong \operatorname{Im}(\psi\varphi)$. Тогда

$$r_1 = \dim\varphi(U) = \dim(\varphi(U) \cap \operatorname{Ker}\psi) + \dim L,$$

откуда

$$r_1 - \dim L = \dim(\varphi(U) \cap \operatorname{Ker}\psi) \leq \dim(\operatorname{Ker}\psi) = n - r_2.$$

2) Пусть $\dim V = n$, $\dim\operatorname{Im}\varphi_i =: r_i$, тогда $\dim\operatorname{Ker}\varphi_i = n - r_i$. Используя предположение индукции и предыдущий пункт, имеем:

$$n - \dim\operatorname{Ker}(\varphi_k \circ \ldots \circ \varphi_1) = \dim(\operatorname{Im}(\varphi_k \circ \ldots \circ \varphi_1)) \geq$$

$$\geq \dim(\operatorname{Im}(\varphi_{k-1} \circ \ldots \circ \varphi_1)) + r_k - n \geq r_1 + \ldots + r_k - (k-1)n =$$

$$= n - (n - r_1) - \ldots - (n - r_k) = n - \dim\operatorname{Ker}\varphi_1 - \ldots - \dim\operatorname{Ker}\varphi_k.$$ ■

7.6 Линейные функции и сопряженное пространство

Пусть V — векторное пространство над полем $\mathbb{K}$.

Определение 7.88. *Линейной функцией* на V называется такая функция $f\colon V \to \mathbb{K}$, что

1) $f(v_1 + v_2) = f(v_1) + f(v_2)\ \forall v_1,\ v_2 \in V$;

2) $f(\lambda v) = \lambda f(v)\ \forall v \in V,\ \lambda \in \mathbb{K}$.

Из определения следует, что для любой конечной линейной комбинации $\sum_{i=1}^{k} \lambda_i v_i$ векторов из V $f(\sum_{i=1}^{k} \lambda_i v_i) = \sum_{i=1}^{k} \lambda_i f(v_i)$.

Легко видеть, что линейная функция — то же самое, что линейное отображение из V в одномерное линейное пространство $\mathbb{K}$ столбцов высоты 1 над полем $\mathbb{K}$. В частности для

линейной функции определено понятие ядра, причем если $\dim V = n$ и $f\colon V \to \mathbb{K},\ f \neq 0$, то $\dim \operatorname{Ker} f = n - 1$.

В $\mathbb{K}$ есть фиксированный базис $\{\mathbf{1}\}$ (здесь $1 \in \mathbb{K}$ рассматривается как вектор, точнее, столбец высоты 1). Тогда любой элемент из *пространства* $\mathbb{K}$ однозначно запишется в виде $\lambda\mathbf{1}$, где λ принадлежит *полю* $\mathbb{K}$.

Приведем несколько примеров линейных функций. Проверка линейности в каждом случае тривиальна (читателю все же рекомендуется ее проделать).

Пример 7.89. Пусть V — евклидова плоскость или пространство, фиксируем $a \in V$ и определим $f = f_a\colon V \to \mathbb{R}$ формулой $\forall v \in V\ f(v) = (a, v)$ (где скобки обозначают скалярное произведение). Тогда f — линейная функция на V. (Полезно заметить, что любая линейная функция на V имеет такой вид для некоторого $a \in V$).

Пример 7.90. Пусть $V = C[a, b]$ — бесконечномерное пространство непрерывных функций на отрезке $[a, b]$. Определим отображение $\varphi\colon V \to \mathbb{R}$ формулой $\varphi(f) = \int_a^b f(x)\,dx\ \forall f \in V$. Тогда φ — линейная функция.

Пример 7.91. Пусть $V = \mathbb{K}^n,\ a := (a_1, \ldots, a_n)$ — заданная строка элементов из $\mathbb{K}$. Тогда $f = f_a\colon \mathbb{K}^n \to \mathbb{K},\ f(v) = av\ \forall v \in V$ (произведение строки на столбец) задает линейную функцию. Мы вскоре увидим, что так выглядит любая линейная функция на пространстве столбцов $\mathbb{K}^n$.

Пример 7.92. Пусть $V = \mathbb{K}[x]_n$ — пространство многочленов степени не выше n, $x_0 \in \mathbb{K}$ — фиксированный элемемент. Тогда $f = f_{x_0}\colon V \to \mathbb{K},\ f(p) = p(x_0)\ \forall p \in \mathbb{K}[x]_n$ (вычисление значения многочлена p в фиксированной точке x_0) определяет линейную функцию на V.

Пример 7.93. Пусть $V = \mathbb{R}[x]_n$, зафиксируем $k \in \mathbb{N}$. Тогда $f\colon V \to \mathbb{R},\ f(p) := p^{(k)}(0)$ (вычисление k-й производной многочлена в нуле) — линейная функция.

Пример 7.94. Пусть $V = \operatorname{Mat}_n(\mathbb{K})$, определим функцию $\operatorname{tr}(A) = \sum_i a_{ii}$ (сумма диагональных элементов матрицы A). Тогда $\operatorname{tr} : \operatorname{Mat}_n(\mathbb{K}) \to \mathbb{K}$ — линейная функция, называемая *следом*.

Задача 7.95. *Пусть линейная функция f на пространстве $V = \operatorname{Mat}_n(\mathbb{K})$ удовлетворяет условию $f(AB) = f(BA)\ \forall A, B \in \operatorname{Mat}_n(\mathbb{K})$. Докажите, что тогда $f = \alpha \operatorname{tr}$ для некоторого $\alpha \in \mathbb{K}$.*

Пусть пространство V конечномерно и $\{e_1, \ldots, e_n\}$ — некоторый базис в V. Линейная функция f однозначно задается своими значениями на базисных векторах: если $v = \sum_{i=1}^n v_i e_i$, то

$$f(v) = v_1 f(e_1) + \ldots + v_n f(e_n),$$

причем эти значения могут быть произвольными элементами поля $\mathbb{K}$. Матрица f как линейного отображения $V \to \mathbb{K}$ имеет размер $1 \times n$, то есть является строкой. Более точно, матрица f относительно базисов $\{e_1, \ldots, e_n\}$ в V и $\{\mathbf{1}\}$ в $\mathbb{K}$ есть строка $(f(e_1), \ldots, f(e_n))$,

которая называется *координатной строкой линейной функции* в базисе $\{e_1, \dots, e_n\}$. Более подробно,

$$(\mathbf{f}(e_1), \dots, \mathbf{f}(e_n)) = \mathbf{1}(f(e_1), \dots, f(e_n)),$$

где слева стоит строка элементов *пространства* $\mathbb{K}$, мы их выделили жирным шрифтом, чтобы отличить от строки чисел справа. При замене базиса в V координатная строка A преобразуется по формуле $A' = AC$ (см. (54)).

Задача 7.96. *Докажите, что система линейных функций $\{f_1, \dots, f_n\}$ на n-мерном пространстве V линейно зависима тогда и только тогда, когда найдется такой вектор $0 \neq v \in V$, что $f_1(v) = \dots = f_n(v) = 0$.*

Решение. Если линейные функции $\{f_1, \dots, f_n\}$ линейно зависимы, то их координатные строки тоже зависимы, то есть линейно зависимы строки матрицы $A = (a_{ij})$, где $a_{ij} = f_i(e_j)$. Тогда линейно зависимы и ее координатные столбцы, то есть

$$\lambda_1 \begin{pmatrix} f_1(e_1) \\ \vdots \\ f_n(e_1) \end{pmatrix} + \dots + \lambda_n \begin{pmatrix} f_1(e_n) \\ \vdots \\ f_n(e_n) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

где не все λ_i равны нулю. Отсюда получаем, что $f_i(v) = 0,\ i = 1, \dots, n$, где $v = \sum_{i=1}^{k} \lambda_i e_i \neq 0$. Легко видеть, что приведенное рассуждение обратимо. ∎

Мы знаем, что множество всех линейных отображений $\varphi\colon V \to U$ является линейным пространством $\mathcal{L}(V; U)$, размерность которого (в случае конечномерных пространств V и U) равна $\dim V \dim U$ (поскольку оно изоморфно пространству матриц соответствующего размера). То же верно в частном случае линейных функций: множество всех линейных функций $f\colon V \to \mathbb{K}$ образует линейное пространство той же размерности, что и V (в случае конечномерного V).

Определение 7.97. Линейное пространство всех линейных функций на V называется *сопряженным пространством* к V и обозначается V^*.

Таким образом,

$$V^* = \{f\colon V \to \mathbb{K} \mid f \text{ линейна}\}.$$

Заметим, что операцию перехода с сопряженному пространству можно итерировать: возникает второе сопряженное $V^{**} := (V^*)^*$ и т.д.

Несмотря на то, что ряд результатов для сопряженного пространства следует из общей теории линейных отображений, оно обладает рядом специальных свойств, связанных с "двойственностью" между векторами и линейными функциями[34], поэтому мы остановимся

[34]Причина указанной двойственности связана с существованием канонического (не зависящего ни от каких выборов) отображения

$$V^* \times V \to \mathbb{K}, \quad (f, v) \mapsto f(v),$$

линейного по каждому из аргументов.

подробнее на его свойствах (и частично передокажем уже известные результаты).

Пусть V — n-мерное линейное пространство над полем $\mathbb{K}$, $\{e_1, \dots, e_n\}$ — некоторый базис в V. Тогда мы имеем набор из n линейных функций $\varepsilon_i \colon V \to \mathbb{K}$, $\varepsilon_i(v) = v_i$ (i-я координата вектора v в базисе $\{e_1, \dots, e_n\}$), $i = 1, \dots, n$. Очевидно, координатные функции однозначно (как линейные функции) задаются равенствами

$$\varepsilon_i(e_j) = \delta_{ij} := \begin{cases} 1, & \text{если } i = j; \\ 0, & \text{если } i \neq j \end{cases}$$

(δ_{ij} называется *δ-символом Кронекера*).

Предложение 7.98. *Система координатных функций $\{\varepsilon_1, \dots, \varepsilon_n\}$ является базисом в V^*.*

Доказательство. Пусть $\sum_{i=1}^n \lambda_i \varepsilon_i = 0$ как линейная функция, это значит, ее значение на любом векторе из V равно нулю. Последовательно подставляя элементы базиса $\{e_1, \dots, e_n\}$ в качестве ее аргументов, получаем $\lambda_1 = \dots = \lambda_n = 0$.

Пусть теперь $f \in V^*$ — произвольная линейная функция, покажем, что она является линейной комбинацией ε_i, $i = 1, \dots, n$. Для этого заметим, что линейная функция

$$g := f - \sum_{i=1}^n f(e_i)\varepsilon_i$$

тождественно равна нулю, так как принимает нулевые значения на всех базисных векторах. ∎

Определение 7.99. Базис в V^*, состоящий из координатных функций $\{\varepsilon_1, \dots, \varepsilon_n\}$, называется *сопряженным* (или *биортогональным*) к базису $\{e_1, \dots, e_n\}$ в V.

Заметим, что из определения биортогонального базиса следует, что для любого вектора $v \in V$

$$v = \sum_{i=1}^n \varepsilon_i(v) e_i, \tag{57}$$

а для любой линейной функции $f \in V^*$

$$f = \sum_{i=1}^n f(e_i)\varepsilon_i. \tag{58}$$

Задача 7.100. *Пусть C — матрица перехода между базисами $\{e_1, \dots, e_n\}$ и $\{e'_1, \dots, e'_n\}$ в V. Найдите матрицу перехода между соответствующими биортогональными базисами $\{\varepsilon_1, \dots, \varepsilon_n\}$ и $\{\varepsilon'_1, \dots, \varepsilon'_n\}$ в V^*.*

Решение. Ясно, что элементы биортогонального базиса должны преобразовываться так же как координаты, то есть $(\varepsilon_1, \dots, \varepsilon_n)^T = C(\varepsilon'_1, \dots, \varepsilon'_n)^T$ (см. формулу (49)). Поэтому $(\varepsilon'_1, \dots, \varepsilon'_n) = (\varepsilon_1, \dots, \varepsilon_n)C^{-T}$. ∎

Задача 7.101. *Покажите, что любая ненулевая линейная функция $f\colon V \to \mathbb{K}$ является первой координатной функцией ε_1 относительно некоторого базиса $\{e_1, \ldots, e_n\}$ в V.*

Решение. Пусть $U := \operatorname{Ker} f \subset V$, тогда $\dim U = n - 1$. Выберем базис $\{e_2, \ldots, e_n\}$ в U и дополним его до базиса в V вектором e_1 таким, что $f(e_1) = 1$ (так как $f \neq 0$, то такой вектор $e_1 \in V$ существует). Тогда для любого вектора $v = \sum_{i=1}^{n} v_i e_i \in V$ имеем

$$f(v) = f\left(\sum_{i=1}^{n} v_i e_i\right) = \sum_{i=1}^{n} v_i f(e_i) = v_1. \quad \blacksquare$$

На самом деле предыдущий результат можно усилить: любой базис в V^* является биортогональным к некоторому (единственному) базису в V. Вот набросок одного из доказательств этого результата (детали оставим читателю в качестве упражнения). Пусть $\{f_1, \ldots, f_n\}$ — линейно независимые элементы в V^*. Тогда их координатные строки в произвольном базисе $\{e_1, \ldots, e_n\}$ пространства V линейно независимы. Составим из них матрицу порядка n. Она невырождена, поэтому приводится к единичной с помощью последовательности элементарных преобразований столбцов. Последняя, примененная к столбцам единичной матрицы, даст матрицу перехода от $\{e_1, \ldots, e_n\}$ к тому базису в V, к которому базис $\{f_1, \ldots, f_n\}$ в V^* является биортогональным. Ниже мы передокажем этот результат в качестве следствия из некоторой теории.

Из предыдущего следует, что если пространство V конечномерно, то оно изоморфно своему двойственному V^*. Например, можно выбрать базис $\{e_1, \ldots, e_n\}$ в V и биортогональный к нему $\{\varepsilon_1, \ldots, \varepsilon_n\}$ в V^* и определить изоморфизм $\varphi\colon V \to V^*$ условием $\varphi(e_i) = \varepsilon_i,\ \ i = 1, \ldots, n$. Можно показать, что выбирая разные базисы в V мы будем получать разные изоморфизмы, и нет никакого способа выбрать среди них изоморфизм "каноническим", ни от каких произвольных выборов не зависящим образом.

Замечание 7.102. Поясним сказанное выше. Определенный выше изоморфизм $\varphi\colon V \to V^*$ в паре базисов $\{e_1, \ldots, e_n\}$ в V и $\{\varepsilon_1, \ldots, \varepsilon_n\}$ в V^* имеет единичную матрицу. Тогда, используя результат Задачи 7.100, можно показать, что φ в другой паре сопряженных базисов $\{e'_1, \ldots, e'_n\}$ и $\{\varepsilon'_1, \ldots, \varepsilon'_n\}$ будет иметь матрицу $C^T C$, где C — матрица перехода от $\{e_1, \ldots, e_n\}$ к $\{e'_1, \ldots, e'_n\}$, в то время как изоморфизм φ', определенный штрихованной парой сопряженных базисов, будет иметь относительно нее единичную матрицу, то есть φ и φ', вообще говоря, разные изоморфизмы (если $C^T C \neq E$).

Однако существует канонический изоморфизм между пространством V и его дважды двойственным V^{**} (в случае, когда V конечномерно). Это имеет ряд важных следствий, в частности, для тензорной алгебры, поэтому мы обсудим эту тему более подробно.

Хотя на первый взгляд представить ненулевую линейную функцию на V^* непросто, все такие линейные функции (в случае конечномерных пространств) имеют простое описание. А именно, для произвольного $v \in V$ определим $\vartheta_v\colon V^* \to \mathbb{K}$ равенством $\vartheta_v(f) := f(v)\ \forall f \in V^*$.

Во-первых проверим, что ϑ_v линейна, то есть $\vartheta_v \in V^{**}$. В самом деле,

$$\vartheta_v(f_1 + f_2) = (f_1 + f_2)(v) = f_1(v) + f_2(v) = \vartheta_v(f_1) + \vartheta_v(f_2)\ \ \forall f_1, f_2 \in V^*.$$

Кроме того,

$$\vartheta_v(\lambda f) = (\lambda f)(v) = \lambda f(v) = \lambda \vartheta_v(f) \ \ \forall f \in V^*.$$

Теперь покажем, что (в случае конечномерного V) никаких линейных функций на V^* кроме тех, которые имеют вид ϑ_v для некоторого $v \in V$, не существует. Для этого определим линейное отображение $\vartheta\colon V \to V^{**}$, полагая $\vartheta(v) = \vartheta_v$.

Во-первых, покажем, что ϑ действительно линейно. Нам нужно проверить, что $\vartheta_{v_1+v_2} = \vartheta_{v_1} + \vartheta_{v_2}$ $\forall v_1,\, v_2 \in V$ и что $\vartheta_{\lambda v} = \lambda \vartheta_v$ $\forall \lambda \in \mathbb{K}$ и $v \in V$. Действительно,

$$\vartheta_{v_1+v_2}(f) = f(v_1 + v_2) = f(v_1) + f(v_2) = \vartheta_{v_1}(f) + \vartheta_{v_2}(f) = (\vartheta_{v_1} + \vartheta_{v_2})(f) \ \ \forall f \in V^*$$

и

$$\vartheta_{\lambda v}(f) = f(\lambda v) = \lambda f(v) = \lambda \vartheta_v(f)$$

(мы использовали линейность f).

Докажем теперь, что ϑ инъективно. Действительно, если $\vartheta_v = 0$, то для любого $f \in V^*$ $\vartheta_v(f) = f(v) = 0$, но если $v \neq 0$ то найдется такая $f \in V^*$ что $f(v) \neq 0$ (например, в произвольном базисе какая-то из координат вектора v отлична от нуля). Значит, $\operatorname{Ker} \vartheta = 0$. Используя теперь Следствие 7.60 получаем, что ϑ — изоморфизм между V и V^{**}. Заметим, что в определении ϑ не было никакого произвола, поэтому этот изоморфизм называется *каноническим*.

Подведем итог.

Теорема 7.103. *Если пространство V конечномерно, то оно канонически изоморфно своему дважды сопряженному пространству V^{**}.*

В предыдущих рассуждениях мы использовали существование канонического билинейного отображения $V^* \times V \to \mathbb{K}$, $(f,\, v) \mapsto f(v)$. Если в записи $(f,\, v)$ зафиксировать $f \in V^*$ и заставить v пробегать пространство V, мы получим линейную функцию на V, а если зафиксировать $v \in V$ и заставить f пробегать все пространство V^*, получим линейную функцию на V^*. Именно этот факт мы и использовали выше в записи $(f,\, v) = \vartheta_v(f)$ для фиксированного $v \in V$.

Преимущества канонических изоморфизмов перед “случайными” состоит в том, что отождествление пространств с помощью них обычно безобидно. То есть пространства V и V^{**} можно считать, по-существу, одним и тем же пространством, при этом вектор $v \in V$ отождествляется с $\vartheta_v \in V^{**}$, а значит базис $\{e_1, \ldots, e_n\}$ в V — с базисом $\{\vartheta_{e_1}, \ldots, \vartheta_{e_n}\}$ в V^{**}.

Замечание 7.104. (ср. Замечание 7.102). Определим изоморфизм $\theta\colon V \to V^{**}$ условием, что он переводит базис $\{e_1, \ldots, e_n\}$ в базис $\{\vartheta_{e_1}, \ldots, \vartheta_{e_n}\}$. В этой паре базисов θ по определению имеет единичную матрицу. Покажем, что θ будет иметь единичную матрицу в любой другой аналогичной паре базисов. Действительно, пусть $\{e'_1, \ldots, e'_n\}$ — другой базис в V такой, что матрица перехода от $\{e_1, \ldots, e_n\}$ к нему есть C. Тогда согласно Задаче 7.100

матрица перехода от $\{\vartheta_{e_1}, \ldots, \vartheta_{e_n}\}$ к $\{\vartheta_{e'_1}, \ldots, \vartheta_{e'_n}\}$ есть $(C^{-T})^{-T} = C$. Поэтому матрица линейного отображения θ относительно новой пары базисов будет $C^{-1}EC = E$. Ясно, что θ совпадает с определенным выше изоморфизмом ϑ. Это еще раз показывает смысл "каноничности" изоморфизма ϑ — его определение не зависит от выбора базиса $\{e_1, \ldots, e_n\}$ в V, а определяется самóй линейной структурой пространства V.

Задача 7.105. *Покажите, что любой базис $\{f_1, \ldots, f_n\}$ в V^* является биортогональным некоторому (единственному) базису $\{e_1, \ldots, e_n\}$ в V.*

Решение. Пусть $\{g_1, \ldots, g_n\}$ — базис в V^{**}, биортогональный к $\{f_1, \ldots, f_n\}$, то есть $g_i(f_j) = \delta_{ij}$. Мы знаем, что каждый g_i имеет вид ϑ_{e_i} для некоторого $e_i \in V$, причем

$$g_i(f_j) = \vartheta_{e_i}(f_j) = f_j(e_i) = \delta_{ij}.$$

Поэтому базис $\{f_1, \ldots, f_n\}$ биортогонален базису $\{e_1, \ldots, e_n\}$. ∎

Задача 7.106. *Пусть V — пространство многочленов $\mathbb{K}[x]_n$ степени $\leq n$. Покажите, что линейные функции $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$, определяемые равенствами*

$$\varepsilon_i(p) = p(x_i),$$

где $x_0, x_1, \ldots, x_n$ — попарно различные элементы поля $\mathbb{K}$, составляют базис пространства V^*, и найдите базис в пространстве V, которому он биортогонален. Покажите, что формула (57) в этом случае превращается в интерполяционную формулу Лагранжа.

Задача 7.107. *Пусть V такое же как в предыдущей задаче, причем $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$. Покажите, что линейные функции $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$, определяемые равенствами*

$$\varepsilon_i(p) = p^{(i)}(x_0),$$

где $x_0 \in \mathbb{K}$, составляют базис пространства V^*, и найдите базис пространства V, которому он биортогонален. Выясните смысл формулы (57) в этом случае.

Решение. Если $\{p_0, p_1, \ldots, p_n\}$ — искомый базис в V, то он состоит из многочленов, удовлетворяющих условиям $p_i^{(j)}(x_0) = \delta_{ij}$. Такие многочлены легко найти: $p_i(x) = \frac{(x-x_0)^i}{i!}$, $i = 0, \ldots, n$. Пусть

$$\lambda_0\varepsilon_0 + \lambda_1\varepsilon_1 + \ldots + \lambda_n\varepsilon_n = 0$$

— некоторая линейная зависимость, применяя ее последовательно к системе $\{p_0, p_1, \ldots, p_n\}$, находим, что $\lambda_0 = \lambda_1 = \ldots = \lambda_n = 0$.

Формула (57) в этом случае превращается в формулу Тейлора:

$$p(x) = p(x_0) + p'(x_0)\frac{(x-x_0)}{1!} + p''(x_0)\frac{(x-x_0)^2}{2!} + \ldots + p^{(n)}(x_0)\frac{(x-x_0)^n}{n!}.$$ ∎

Пусть $\dim V = n$. Для любого k, $0 \le k \le n$ построим явное взаимно однозначное соответствие между множествами k-мерных подпространств в V и $n-k$-мерных подпространств в V^*.

А именно, каждому k-мерному подпространству $U \subset V$ сопоставим некоторое подпространство $U^0 \subset V^*$ следующим образом:

$$U^0 := \{f \in V^* \mid f(u) = 0 \ \ \forall u \in U\}. \tag{59}$$

То есть U^0 состоит из тех и только тех линейных функций на V, которые обращаются в ноль на всех векторах из U. Подпространство $U^0 \subset V^*$ называется *аннулятором* подпространства $U \subset V$.

Предложение 7.108. $\dim U^0 = n - \dim U$.

Доказательство. Пусть $\{e_1, \dots, e_n\}$ — такой базис в V, что его подсистема $\{e_1, \dots, e_k\}$ является базисом в U. Тогда легко видеть, что $U^0 = \langle \varepsilon_{k+1}, \dots, \varepsilon_n \rangle$. ■

Поскольку выше мы отождествили пространства V и V^{**} с помощью канонического изоморфизма ϑ, $(U^0)^0$ можно рассматривать как подпространство в V. При этом, как легко проверит читатель, $(U^0)^0 = \{v \in V \mid f(v) = 0 \ \forall f \in U^0\} \subset V$.

Предложение 7.109. *Для любого подпространства $U \subset V$ имеет место равенство $(U^0)^0 = U$ подпространств в V. Более того, сопоставление подпространству его аннулятора определяет обращающую включение*[35] *биекцию между множествами подпространств в V и в V^*.*

Доказательство. Легко видеть, что $U \subset (U^0)^0$. С другой стороны, согласно предыдущему Предложению, $\dim (U^0)^0 = n - \dim U^0 = n - (n - \dim U) = \dim U$, откуда $U = (U^0)^0$. Это показывает, что сопоставление подпространству в V его аннулятора (как подпространства в V^*) и сопоставление подпространству в V^* его аннулятора (как подпространства в V) — взаимно обратные биекции между подпространствами в V и в V^*.

Если U и W — подпространства в V, то из $U \subset W$ следует $U^0 \supset W^0$ (включение подпространств в V^*). Обратная импликация следует из предыдущего абзаца. ■

Задача 7.110. *Не вычисляя количества подпространств явно, докажите, что в n-мерном линейном пространстве над конечным полем числа k-мерных и $n-k$-мерных подпространств равны. (Иначе в этом можно убедиться используя результат Задачи 6.57).*

Задача 7.111. *Докажите, что для подпространств U и W в V верны равенства $(U \cap W)^0 = U^0 + W^0$, $(U + W)^0 = U^0 \cap W^0$.*

Решение. В силу предыдущего Предложения, из $U \supset U \cap W \subset W$ следует $U^0 \subset (U \cap W)^0 \supset W^0$, откуда (в силу того, что сумма подпространств $L + M$ — наименьшее по включению подпространство, содержащее L и M) $U^0 + W^0 \subset (U \cap W)^0$.

Аналогично, из $U^0 \subset U^0 + W^0 \supset W^0$ следует $U \supset (U^0 + W^0)^0 \subset W$, откуда (в силу того, что пересечение $L \cap M$ — наибольшее подпространство, содержащееся и в L и в M) $(U^0 + W^0)^0 \subset U \cap W$, что равносильно $(U \cap W)^0 \subset U^0 + W^0$. Значит, $(U \cap W)^0 = U^0 + W^0$. Второе равенство можно доказать аналогично, а можно вывести из первого с использованием предыдущего Предложения. А именно, обозначив $L = U^0$, $M = W^0$, перепишем доказанное равенство в виде $(L^0 \cap M^0)^0 = L + M$, откуда, переходя к аннуляторам, получаем $(L + M)^0 = L^0 \cap M^0$. ■

Понятие аннулятора позволяет дать бескоординатное описание связи между подпространствами в $\mathbb{K}^n$ и системами линейных уравнений, которые их определяют (выбор базиса в V отождествляет аннулятор

[35] Что логично: чем меньше подпространство, тем больше линейных функций, которые на нем обращаются в нуль.

U^0 с пространством всех линейных уравнений, которым удовлетворяют все векторы из U). В частности, так как любое подпространство $U \subset V$ является аннулятором некоторого подпространства в V^* (а именно U^0), то любое подпространство после выбора базиса является пространством решений некоторой СЛОУ.

Замечание 7.112. Дадим другое решение Задачи 7.96. Пусть для линейных функций $\{f_1, \ldots, f_n\}$ на n-мерном пространстве V существует $v \in V$, $v \neq 0$ такой, что $f_1(v) = \ldots = f_n(v) = 0$; покажем, что данная система функций линейно зависима. В самом деле, положим $W := \langle f_1, \ldots, f_n \rangle \subseteq V^*$. Тогда из условия $0 \neq v \in W^0$, поэтому $\dim W < n = \dim V^*$ и значит система $\{f_1, \ldots, f_n\}$ линейно зависима.

Обратно, пусть система $\{f_1, \ldots, f_n\}$ линейно зависима. Тогда размерность $W = \langle f_1, \ldots, f_n \rangle$ меньше $n = \dim V^*$ и значит $W^0 \neq 0$, поэтому найдется вектор $0 \neq v \in V$ такой, что $f_1(v) = \ldots = f_n(v) = 0$.

Пусть $\varphi\colon V \to U$ — линейное отображение. Тогда оно индуцирует линейное отображение сопряженных пространств, направленное в обратную сторону:

$$\varphi^\star\colon U^* \to V^*, \quad \varphi^\star(f) = f \circ \varphi,$$

то есть для $f \in U^*$ линейная функция $\varphi^\star(f) \in V^*$ принимает значение $f(\varphi(v))$ на произвольном векторе $v \in V$. Отображение $\varphi^\star$ называется *линейно сопряженным* к φ.

Замечание 7.113. Равенство $\varphi^\star(f)(v) = f(\varphi(v))$ иногда переписывают в виде $(f, \varphi(v))_U = (\varphi^\star f, v)_V$, где левые и правые скобки обозначают канонические билинейные отображения $U^* \times U \to \mathbb{K}$ и $V^* \times V \to \mathbb{K}$ соответственно. Эти обозначения демонстрируют связь (подробности см. в Замечании 12.3) между линейно сопряженными отображениями, введенными выше и сопряженными отображениями евклидовых пространств, которые будут изучаться далее.

Проверка линейности $\varphi^\star$:

$$\varphi^\star(f_1 + f_2) = (f_1 + f_2) \circ \varphi = f_1 \circ \varphi + f_2 \circ \varphi = \varphi^\star(f_1) + \varphi^\star(f_2),$$

аналогично для умножения на константу.

Предложение 7.114. *Операция $\star\colon \mathcal{L}(U, V) \to \mathcal{L}(V^*, U^*)$ обладает следующими свойствами:*

1) $(\varphi_1 + \varphi_2)^\star = \varphi_1^\star + \varphi_2^\star$, $(\lambda\varphi)^\star = \lambda\varphi^\star$ *(линейность);*
2) $\mathrm{Id}_V^\star = \mathrm{Id}_{V^*}$*;*
3) *для всех линейных отображений $\varphi\colon U \to V$ диаграммы*

$$\begin{array}{ccc} V & \xrightarrow{\vartheta^V} & V^{**} \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\varphi^{\star\star}} \\ U & \xrightarrow{\vartheta^U} & U^{**} \end{array}$$

коммутативны (то есть при канонических изоморфизмах $\vartheta^U\colon U \cong U^{**}$, $\vartheta^V\colon V \cong V^{**}$ отображение $\varphi^{\star\star}$ отождествляется с φ).

4) *Если $\psi\colon V \to W$ — еще одно линейное отображение, то $(\psi \circ \varphi)^\star = \varphi^\star \circ \psi^\star$,*

Доказательство. Докажем пункт 3). $\varphi^{\star\star}(\vartheta_u^U)$ — это функция, на произвольном $f \in V^*$ принимающая значение

$$\varphi^{\star\star}(\vartheta_u^U)(f) = \vartheta_u^U(\varphi^\star f) = (\varphi^\star f)(u) = f(\varphi(u)).$$

$\vartheta_{\varphi(u)}^U$ — это функция, на произвольном $f \in V^*$ принимающая значение

$$\vartheta_{\varphi(u)}^U(f) = f(\varphi(u)).$$

Отсюда $\varphi^{\star\star}(\vartheta_u^U) = \vartheta_{\varphi(u)}^U$.

Доказательство пункта 4) дается следующей выкладкой, где $f \in W^*$, $u \in U$:

$$(\psi\varphi)^\star(f)(u) = f(\psi(\varphi(u))) = (\psi^\star f)(\varphi(u)) = \varphi^\star(\psi^\star(f))(u) = (\varphi^\star\psi^\star)(f)(u).$$

Доказательство пунктов 1) и 2) оставим читателю в качестве упражнения. ■

По поводу применения введенных понятий и результатов к нахождению инвариантных подпространств оператора см. Предложение 8.23 и следующий за ним абзац.

Замечание 7.115. В случае бесконечномерного пространства V сопряженное пространство V^* всегда имеет бóльшую размерность (в смысле мощности базиса). Например, если V — пространство финитных последовательностей, которое счетномерно, то V^* состоит из всех последовательностей, и является несчетномерным.

8 Линейные операторы

Данная глава посвящена изучению линейных операторов — основных объектов линейной алгебры. Вводятся фундаментальные понятия собственного вектора и собственного подпространства, изучаются вопросы диагонализируемости (существование базиса, в котором матрица оператора диагональна). Также изучаются инварианты линейных операторов (при этом их полная теория над полем $\mathbb{C}$ будет построена в следующем разделе). В конце главы доказывается важная теорема Гамильтона-Кэли.

8.1 Определение и простейшие свойства

Для удобства напомним определение линейного оператора (=линейного преобразования) и его матрицы, а также перечислим те их свойства, которые были доказаны ранее.

Определение 8.1. *Линейным оператором* на линейном пространстве V называется линейное отображение $\varphi\colon V \to V$.

Аналогично общему случаю линейных отображений, определяются ядро $\operatorname{Ker}\varphi$ и образ $\operatorname{Im}\varphi$ линейного оператора $\varphi\colon V \to V$. Они являются подпространствами V, причем если V конечномерно, то

$$\dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = \dim V. \tag{60}$$

Оператор $\varphi\colon V \to V$ биективен (то есть изоморфизм) тогда и только тогда, когда $\operatorname{Ker}\varphi = 0$ и $\operatorname{Im}\varphi = V$, причем если V конечномерно, то два последних условия эквивалентны (ввиду формулы (60)).

Если $\{e_1, \dots, e_n\}$ — базис в V, то матрицей φ в нем называется такая единственная матрица A порядка n, что

$$(\varphi(e_1), \dots, \varphi(e_n)) = (e_1, \dots, e_n)A.$$

Если $\overrightarrow{v}$ — координатный столбец вектора $v \in V$ в базисе $\{e_1, \ldots, e_n\}$, а A — матрица оператора φ в том же базисе, то координатный столбец вектора $\varphi(v)$ в том же базисе равен $A\overrightarrow{v}$.

Если $\{e'_1, \ldots, e'_n\}$ — новый базис в V, причем C — матрица перехода к нему от старого базиса, то $A' = C^{-1}AC$, где A' — матрица φ в новом базисе (см. (55)).

Замечание 8.2. Сразу отметим важную особенность матрицы линейного оператора: ее определитель зависит только от самогó оператора, но не от базиса, в котором она написана. Действительно,

$$\det A' = \det\left(C^{-1}AC\right) = (\det C)^{-1}(\det A)(\det C) = \det A.$$

Это говорит о том, что у линейных операторов больше инвариантов, чем у общих линейных отображений, что приводит к их более сложной теории.

Заметим, что матрица (в данном базисе) композиции операторов равна произведению их матриц, матрица тождественного оператора является единичной матрицей (в любом базисе). Оператор φ — изоморфизм тогда и только тогда, когда его матрица A (в произвольном базисе) невырождена, при этом матрицей φ^{-1} в том же базисе является A^{-1}.

Замечание 8.3. Выбор базиса в пространстве V задает изоморфизм алгебр $\mathcal{L}(V) \to \mathrm{Mat}_n(\mathbb{K})$. Вообще, можно заметить, что изоморфизм линейных пространств $\alpha\colon V \to U$ задает изоморфизм алгебр линейных операторов $\mathcal{L}(V) \to \mathcal{L}(U)$, $\varphi \mapsto \alpha\varphi\alpha^{-1}$, а для $U = \mathbb{K}^n$ любой линейный оператор является умножением столбцов на матрицу из $\mathrm{Mat}_n(\mathbb{K})$.

Из доказанного ранее также следует, что если A — матрица φ, то $\operatorname{rk} A = \dim \operatorname{Im}\varphi$ (и, таким образом, $\operatorname{rk} A$ не зависит от базиса, в котором написана A).

Рассмотрим несколько примеров линейных операторов.

Пример 8.4. Нулевой оператор, тождественный оператор Id_V, "гомотетия" $\lambda\mathrm{Id}_V$.

Пример 8.5. Пусть $V = U \oplus W$ и $\varphi\colon V \to V$ — проектор на U параллельно W, определенный в Примере 7.38. Ранее мы проверили его линейность. В Задаче 7.83 было доказано, что он удовлетворяет тождеству $\varphi^2 = \varphi$.

Докажем обратное, что любой линейный оператор $\varphi\colon V \to V$, удовлетворяющий тождеству $\varphi^2 = \varphi$, является проектором на $U := \operatorname{Im}\varphi \subset V$ параллельно $W := \operatorname{Ker}\varphi \subset V$. Действительно, любой вектор $v \in V$ представляется в виде

$$v = \varphi(v) + (v - \varphi(v)), \tag{61}$$

где первое слагаемое лежит в U, второе — в W, откуда $V = U + W$. Для доказательства того, что эта сумма прямая, можно либо воспользоваться формулой (60), либо доказать что $U \cap W = 0$ следующим образом. Пусть напротив, $0 \neq z \in U \cap W$, тогда $z = \varphi(v)$ для некоторого $v \in V$ и $\varphi(z) = 0$, откуда $0 = \varphi^2(v) = \varphi(v) = z$ — противоречие с $z \neq 0$. Теперь равенство (61) показывает, что действие нашего оператора на произвольный вектор $v \in V$ сводится к взятию его проекции на U параллельно прямому дополнению W.

Пример 8.6. Рассмотрим оператор $\varphi\colon V \to V$, удовлетворяющий тождеству $\varphi^2 = \mathrm{Id}_V$.[36] Положим

$$V^+ := \{v \in V \mid \varphi(v) = v\}, \quad V^- := \{v \in V \mid \varphi(v) = -v\}$$

(заметим, что $V^+ = \mathrm{Ker}\,(\varphi - \mathrm{Id}_V)$, $V^- = \mathrm{Ker}\,(\varphi + \mathrm{Id}_V)$). Покажем что тогда $V = V^+ \oplus V^-$. В самом деле, для всякого $v \in V$ имеем

$$v = \frac{v + \varphi(v)}{2} + \frac{v - \varphi(v)}{2},$$

где первое слагаемое лежит в V^+, а второе — в V^-, откуда $V = V^+ + V^-$. Пересечение V^+ и V^- состоит из векторов, удовлетворяющих равенству $v = -v$, откуда $V^+ \cap V^- = 0$.

Легко видеть, что если $v = u + w$ — разложение произвольного вектора $v \in V$ в соответствии с прямой суммой $V = V^+ \oplus V^-$, то действие φ на v задается формулой $\varphi(v) = u - w$. Такой оператор φ естественно назвать "отражением относительно V^+ параллельно V^-" (читателю предлагается нарисовать картинку). Легко видеть, что наоборот, любое такое отражение (связанное с разложением V в прямую сумму $V^+ \oplus V^-$ подпространств) удовлетворяет тождеству $\varphi^2 = \mathrm{Id}_V$. Примером такого линейного оператора является оператор транспонирования на пространстве квадратных матриц $\mathrm{Mat}_n(\mathbb{K})$ (какие в этом случае подпространства V^+ и V^-?). Кстати, заодно мы дали "геометрическое" описание множества решений матричного уравнения $X^2 = E$ (в квадратных матрицах данного порядка n) — они находятся в биективном соответствии с разложениями пространства $\mathbb{K}^n$ в прямую сумму своих подпространств.

Пример 8.7. Оператор поворота на плоскости (в трехмерном пространстве) на данный угол (вокруг данной оси на данный угол).

Пример 8.8. Оператор дифференцирования $\varphi = \frac{d}{dx}$ на пространстве $V = \mathbb{R}[x]_n$ многочленов степени не выше n. У этого оператора одномерное ядро (состоящее из констант) и $n-1$-мерный образ $\mathrm{Im}\,\varphi = \mathbb{R}[x]_{n-1} \subset \mathbb{R}[x]_n$. Заметим, что в этом случае $\mathrm{Ker}\,\varphi$ содержится в $\mathrm{Im}\,\varphi$.

Пример 8.9. Свойства оператора дифференцирования сильно зависят от того, на каком пространстве функций мы его рассматриваем. Рассмотрим, например, оператор $\varphi = \frac{d}{dx}$ на линейной оболочке функций

$$V := \langle \sin x,\, \cos x \rangle = \{\alpha \sin x + \beta \cos x \mid \alpha, \beta \in \mathbb{R}\}$$

над $\mathbb{R}$ (указанную линейную оболочку мы рассматриваем как подпространство пространства дифференцируемых функций на действительной прямой). Легко видеть, что функции $\sin x$, $\cos x$ линейно независимы, поэтому $\dim V = 2$. Тогда φ является изоморфизмом пространства V на себя. Любопытно отметить, что матрица φ в базисе $\{\sin x,\, \cos x\}$ совпадает с матрицей поворота плоскости на угол $\pi/2$ в ортонормированнном базисе.

[36] В этом примере мы полагаем, что $\mathrm{char}\,\mathbb{K} \neq 2$.

8.2 Инвариантные подпространства

Пусть $\varphi\colon V \to V$ — линейный оператор на V.

Определение 8.10. Подпространство $U \subset V$ называется *φ-инвариантным*, если $\forall u \in U\ \varphi(u) \in U$ (коротко: $\varphi(U) \subset U$).

Ясно, что нулевое подпространство и все V φ-инвариантны (для любого оператора φ). Далее, легко показать, что *любое подпространство, содержащееся в* $\operatorname{Ker}\varphi$, а также *любое подпространство, содержащее* $\operatorname{Im}\varphi$, *φ-инвариантны.* Кроме того, сумма и пересечение инвариантных подпространств являются инвариантными подпространствами. Несложную проверку всех этих утверждений мы оставляем читателю.

Задача 8.11. *Постарайтесь найти все инвариантные подпространства операторов из предыдущего параграфа.*

Говорят, что два оператора φ и ψ на V *коммутируют*, если $\psi\varphi = \varphi\psi$. Очевидно, это равносильно тому, что их матрицы (в произвольном базисе) коммутируют: $AB = BA$.

Предложение 8.12. *Если операторы φ и ψ коммутируют, то* $\operatorname{Ker}\varphi$ *инвариантно относительно ψ, и наоборот. То же верно и для образов.*

Доказательство. Докажем Предложение для ядер. Пусть $U := \operatorname{Ker}\varphi$. Тогда для любого $u \in U$ имеем

$$\varphi(\psi(u)) = \psi(\varphi(u)) = \psi(0) = 0,$$

откуда $\psi(u) \in U$. ∎

Вот важный для дальнейшего пример такой пары операторов: φ и $\psi := \varphi - \lambda\mathrm{Id}_V$.

Определение 8.13. Если $U \subset V$ — φ-инвариантное подпространство, то определен линейный оператор

$$\varphi|_U\colon U \to U, \quad \varphi|_U(u) = \varphi(u) \in U$$

на U, называемый *ограничением*[37] оператора φ на (инвариантное) подпространство U.

Наличие инвариантного подпространства позволяет предъявить базис, в котором матрица φ имеет специальный вид.

А именно, выберем базис $\{e_1, \ldots, e_k\}$ в подпространстве U и продолжим его до базиса $\{e_1, \ldots, e_k, e_{k+1}, \ldots, e_n\}$ во всем пространстве V. Тогда матрица A оператора φ в базисе $\{e_1, \ldots, e_n\}$ будет иметь вид

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} \tag{62}$$

[37] иногда также *сужением* оператора на подпространство U.

с квадратными матрицами B и D порядков k и $n-k$. Легко видеть, что матрица B является матрицей ограничения $\varphi|_U$ в базисе $\{e_1, \ldots, e_k\}$.

Обратно, если матрица имеет указанный выше вид, то линейная оболочка первых k базисных векторов является φ-инвариантным подпространством.

Замечание 8.14. Матрица D тоже является матрицей некоторого оператора, который строится по φ и инвариантному подпространству U, а именно *фактороператора*, но его определение выходит за рамки базового курса. Подробности см. в параграфе 8.6.

Еще лучше, если удастся найти такой базис в V, в котором A будет иметь *блочно-диагональный вид*

$$A = \begin{pmatrix} B & 0 \\ 0 & D \end{pmatrix}. \tag{63}$$

А именно, рассмотрим оператор $\varphi\colon V \to V$, для которого V является прямой суммой φ-инвариантных подпространств U и W, $V = U \oplus W$. Тогда матрица φ в базисе в V, полученном объединением базисов в U и W, будет иметь требуемый вид, причем B и D будут матрицами $\varphi|_U$ и $\varphi|_W$ в соответствующих базисах подпространств.

Обратно, если матрица A оператора φ в базисе $\{e_1, \ldots, e_n\}$ в V имеет блочно-диагональный вид (63) с блоками порядков k и $n-k$ соответственно, то линейные оболочки $U := \langle e_1, \ldots, e_k\rangle$ и $W := \langle e_{k+1}, \ldots, e_n\rangle$ будут инвариантными подпространствами V такими, что $V = U \oplus W$.

Пример 8.15. Пусть $\{e_1, e_2, e_3\}$ — ортонормированный базис в трехмерном евклидовом пространстве. В нем матрица оператора поворота φ на угол α вокруг оси e_3 имеет вид

$$\begin{pmatrix} \cos\alpha & \mp\sin\alpha & 0 \\ \pm\sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

поэтому линейные оболочки $\langle e_1, e_2\rangle$ и $\langle e_3\rangle$ φ-инвариантны.

Пример 8.16. Матрица A проектора (см. Примеры 7.38 и 8.5) на U параллельно W в объединении базисов U и W имеет вид

$$\begin{pmatrix} E_k & 0 \\ 0 & 0 \end{pmatrix},$$

где $k = \dim U$.

Пример 8.17. Матрица A отражения (см. Пример 8.6) относительно U параллельно W в объединении базисов U и W имеет вид

$$\begin{pmatrix} E_k & 0 \\ 0 & -E_{n-k} \end{pmatrix},$$

где $k = \dim U$, $n - k = \dim W$.

Более общо, если $V = V_1 \oplus \ldots \oplus V_k$ — разложение в прямую сумму φ-инвариантных подпространств, то матрица φ в объединении базисов подпространств V_i будет иметь вид

$$\begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_k \end{pmatrix},$$

где блоки A_i — матрицы ограничений $\varphi|_{V_i}$ в соответствующих базисах.

Задача 8.18. *Покажите, что для оператора $\varphi\colon V \to V$, $\dim V = n$ существует базис, в котором его матрица диагональная тогда и только тогда, когда V является прямой суммой $\oplus_{i=1}^{n} V_i$ одномерных φ-инвариантных подпространств $V_i \subset V$.*

Определение 8.19. Оператор, для которого существует базис, в котором он имеет диагональную матрицу, называется *диагонализируемым*.

Вскоре мы увидим, что не все операторы диагонализируемы (при $\dim V > 1$), и опишем препятствия к диагонализируемости.

Задача 8.20. *Покажите, что для оператора $\varphi\colon V \to V$, $\dim V = n$ существует базис, в котором его матрица верхняя треугольная тогда и только тогда, когда в V существует цепочка вложенных φ-инвариантных подпространств $0 = V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_n = V$, таких, что $\dim V_k = k$, $0 \leq k \leq n$.*

Далее мы докажем, что при $\mathbb{K} = \mathbb{C}$ для любого оператора существует базис, в котором его матрица верхняя треугольная.

При каком условии, имея вид (62) для данного φ-инвариантного $U \subset V$, можно получить вид (63), выбирая последние $n - k$ базисных векторов? Очевидно, что это можно сделать тогда и только тогда, когда для $U \subset V$ существует φ-инвариантное прямое дополнение в V. Конечно, у любого подпространства есть прямое дополнение, но в общем случае неверно, что для φ-инвариантного подпространства существует φ-инвариантное прямое дополнение. Приведем соответствующий пример.

Пример 8.21. Рассмотрим оператор $\varphi := \frac{d}{dx}$ на пространстве $V := \mathbb{R}[x]_n$. Покажите, что все его инвариантные подпространства суть подпространства $\mathbb{R}[x]_k \subset V$, $0 \leq k \leq n$ (указание: для произвольного инвариантного подпространства $U \subset V$ пусть $p \in U$ — содержащийся в нем многочлен максимальной степени, тогда покажите, что $U = \mathbb{R}[x]_k$, где $k = \deg p$). Таким образом, все инвариантные подпространства вложены в друг друга наподобие матрешки, поэтому ни у какого из них (за исключением нулевого и всего пространства) нет инвариантного прямого дополнения, а значит ни в каком базисе матрица φ не является блочно-диагональной. Тот факт, что матрица φ в базисе $\{1, x, x^2, \ldots, x^n\}$ является верхней

треугольной, связан с тем, что данный базис согласован со "структурой матрешки" в том смысле, что линейная оболочка $\{1, x, x^2, \dots, x^k\}$ для любого $0 \le k \le n$ совпадает с $\mathbb{R}[x]_k$ и, таким образом, φ-инвариантна.

Заметим, что матрица оператора дифференцирования из предыдущего примера в базисе $\{1, x, x^2, \dots, x^n\}$ не просто верхнетреугольная, а удовлетворяет более сильному условию: она является верхнетреугольной с нулями на главной диагонали. Такие матрицы называются (верхними) *нильтреугольными*.

Задача 8.22. *Как нужно усилить условие существования цепочки вложенных φ-инвариантных подпространств $0 = V_0 \subset V_1 \subset V_2 \subset \dots \subset V_n = V$ из Задачи 8.20, чтобы получить критерий существования у оператора нильтреугольной матрицы?*

В следующем Предложении мы используем понятия и обозначения из параграфа 7.6.

Предложение 8.23. *Пусть $\varphi\colon V \to V$ — линейный оператор. Тогда подпространство $U \subset V$ φ-инвариантно тогда и только тогда, когда его аннулятор $U^0 \subset V^*$ $\varphi^\star$-инвариантен.*

Доказательство. Пусть $\varphi(U) \subseteq U$. Тогда для произвольных $f \in U^0$ и $u \in U$ имеем $\varphi^\star(f)(u) = f(\varphi(u)) = 0$, откуда $\varphi^\star(f) \in U^0$. То есть $\varphi^\star(U^0) \subseteq U^0$. Для доказательства обратной импликации применим к $\varphi^\star(U^0) \subseteq U^0$ уже доказанное утверждение, получим $\varphi^{\star\star}(U^{00}) \subseteq U^{00}$, что при каноническом изоморфизме $\vartheta^V : V \to V^{**}$ отождествляется с $\varphi(U) \subseteq U$ (чтобы в этом убедиться, нужно воспользоваться Предложением 7.109 и пунктом 3) Предложения 7.114). ■

Доказанное Предложение показывает, что $n-1$-одномерные инвариантные подпространства оператора φ, заданного на n-мерном пространстве V, являются ядрами линейных функций, являющихся собственными векторами (см. следующий параграф) линейно-сопряженного преобразования $\varphi^\star$.

Задача 8.24. *Докажите, что если операторы φ, ψ на конечномерном комплексном линейном пространстве V коммутируют, то в V существует базис, в котором их матрицы одновременно являются верхними треугольными.*[38]

Решение. Требуемый результат будем доказывать индукцией по $n = \dim V$. Случай $n = 1$ тривиален. Пусть $n \ge 2$ и предположим, что результат верен для пространств размерности $\le n - 1$.

Если операторы φ, ψ коммутируют, то и $\varphi^\star$, $\psi^\star$ тоже коммутируют. Тогда у последних есть общий собственный вектор $f \in V^*$. (В самом деле, рассмотрим какое-то собственное подпространство оператора $\varphi^\star$; оно $\psi^\star$-инвариантно и значит в нем есть собственный вектор оператора $\psi^\star$). Тогда $f = 0$ задает общее для φ и ψ инвариантное подпространство $U \subset V$ размерности $n - 1$. По предположению индукции, в U для $\varphi|_U$ и $\psi|_U$ есть требуемый базис; дополняя его произвольным вектором из $V \backslash U$, получаем требуемый базис во всем V для φ и ψ. ■

8.3 Собственные векторы и подпространства

Пусть вектор $v \in V$ порождает одномерное φ-инвариантное подпространство $\langle v \rangle \subset V$. Тогда $v \ne 0$ и $\varphi(v) = \lambda v$ для некоторого скаляра $\lambda \in \mathbb{K}$. Такие векторы играют очень важную роль в изучении операторов и имеют специальное название.

[38] Заметим, что результат верен для произвольного множества таких операторов.

Определение 8.25. Пусть V — векторное пространство над полем $\mathbb{K}$. Ненулевой вектор $v \in V$ называется *собственным вектором* оператора $\varphi\colon V \to V$, отвечающим *собственному значению* $\lambda \in \mathbb{K}$, если $\varphi(v) = \lambda v$.

Легко видеть (ср. Задачу 8.18), что оператор $\varphi\colon V \to V$ диагонализируем тогда и только тогда, когда существует базис в V, состоящий из его собственных векторов.

Например, любой ненулевой вектор из ядра (если такой есть) — собственный вектор с собственным значением 0. Для $\varphi = \mathrm{Id}_V$ любой ненулевой вектор $v \in V$ является собственным с собственным значением 1.

Вот менее тривиальные примеры.

Пример 8.26. Пусть $V = U \oplus W$ и $\varphi\colon V \to V$ — проектор на U параллельно W (см. Пример 7.38). Какие у него могут быть собственные значения? Из Задачи 7.83 мы знаем, что проектор удовлетворяет тождеству $\varphi^2 = \varphi$. Поэтому если $v \in V$ — собственный вектор φ, отвечающий собственному значению λ, то

$$\lambda v = \varphi(v) = \varphi^2(v) = \varphi(\lambda v) = \lambda\varphi(v) = \lambda^2 v,$$

откуда $\lambda(\lambda - 1)v = 0$, но так как $v \neq 0$, то либо $\lambda = 0$ либо $\lambda = 1$. Соответствующие собственные векторы легко предъявить. А именно, любой ненулевой вектор из U — собственный вектор φ с собственным значением 1, а любой ненулевой вектор из W — собственный вектор φ с собственным значением 0.

Пример 8.27. Аналогично предыдущему примеру можно показать (сделайте это!), что для оператора отражения $\varphi^2 = \mathrm{Id}_V$ собственными значениями могут быть только $\lambda = \pm 1$. Если использовать обозначения Примера 8.6, то любой ненулевой вектор из V^+ — собственный вектор с собственным значением 1, а любой ненулевой вектор из V^- — собственный вектор с собственным значением -1. В частности, у оператора транспонирования на пространстве $\mathrm{Mat}_n(\mathbb{R})$ имеются два собственных значения: 1 и -1, собственные векторы для 1 — ненулевые симметричные матрицы, собственные векторы для -1 — ненулевые кососимметрические матрицы.

Пример 8.28. Оператор поворота на евклидовой плоскости на угол $\alpha \neq \pi k$ не имеет собственных векторов.

Пример 8.29. Единственным собственным значением оператора поворота трехмерного евклидова пространства V на угол $\alpha \neq \pi k$ вокруг оси $\langle a \rangle$ $(0 \neq a \in V)$ является 1, а соответствующими собственными векторами является ненулевые векторы из $\langle a \rangle \subset V$.

Пример 8.30. Рассмотрим линейную оболочку $V := \langle e^{\lambda_1 x}, \ldots, e^{\lambda_n x} \rangle$ функций над $\mathbb{R}$, где $\lambda_1, \ldots, \lambda_n$ — попарно различные вещественные числа. Легко показать, что указанные функции линейно независимы (над $\mathbb{R}$), то есть $\dim V = n$. Проще всего это сделать, записав линейную зависимость между ними, продифференцировать ее $n - 1$ раз, а затем воспользоваться невырожденностью определителя Вандермонда. Рассмотрим $\varphi := \frac{d}{dx}$ на

V. Легко видеть, что функции $e^{\lambda_k x}$ — собственные векторы оператора φ с собственными значениями λ_k и в базисе $\{e^{\lambda_1 x}, \dots, e^{\lambda_n x}\}$ пространства V оператор φ имеет диагональную матрицу $\operatorname{diag}(\lambda_1, \dots, \lambda_k)$.

Пример 8.31. Пусть $V = \mathbb{R}[x]_n$, $\varphi = \frac{d}{dx}$. В данном случае собственные векторы с собственным значением λ — такие многочлены $p \neq 0$, что $p' = \lambda p$. Так как производная любого ненулевого многочлена имеет строго меньшую степень, чем сам многочлен, то единственно возможное собственное значение — $\lambda = 0$.[39] Действительно, существуют собственные векторы с собственным значением 0: это ненулевые константы. Заметим, что при $n > 0$ в V не существует базиса из собственных векторов оператора φ, то есть он не диагонализируем.

Во всех рассмотренных примерах операторы имели конечное число собственных значений. Это верно для любого оператора в конечномерном пространстве (мы вскоре это докажем). Как искать собственные значения данного оператора φ?

Во-первых, заметим, что *скаляр $\lambda \in \mathbb{K}$ является собственным значением оператора $\varphi\colon V \to V$ тогда и только тогда, когда подпространство*

$$V_\lambda := \operatorname{Ker}(\varphi - \lambda \operatorname{Id}_V) \subset V \tag{64}$$

ненулевое, $V_\lambda \neq 0$. Действительно, любой собственный вектор оператора φ с собственным значением λ лежит в V_λ, и наоборот, любой ненулевой вектор из V_λ является собственным с собственным значением λ.

Определение 8.32. Ненулевое подпространство V_λ, определенное равенством (64), называется *собственным подпространством* оператора φ, отвечающим собственному значению λ (или, более коротко, с собственным значением λ).

Таким образом, собственное подпространство V_λ состоит из всех собственных векторов оператора φ с собственным значением λ, и нулевого вектора.

Пример 8.33. Из Примера 8.26 следует, что для проектора $\varphi\colon V \to V$ на U параллельно W подпространство U является собственным подпространством с собственным значением 1 (при $\varphi \neq 0$), а W — собственным подпространством с собственным значением 0 (при $\varphi \neq \operatorname{Id}_V$). (Заметим, что вообще, если у оператора ненулевое ядро, то оно является собственным подпространством с собственным значением 0).

Пример 8.34. Аналогично, из Примера 8.27 следует, что для оператора отражения $\varphi\colon V \to V$ подпространство V^+ является собственным подпространством с собственным значением 1 (при $\varphi \neq -\operatorname{Id}_V$), а V^- — собственным подпространством с собственным значением -1 (при $\varphi \neq \operatorname{Id}_V$). В частности, у оператора транспонирования на пространстве $\operatorname{Mat}_n(\mathbb{R})$ имеются два собственных подпространства: подпространство симметрических матриц (собственное подпространство, отвчающее собственному значению 1), и подпространство кососимметрических матриц (отвечающее собственному значению -1).

[39] Для доказательства этого можно было бы также воспользоваться соотношением $\varphi^{n+1} = 0$.

Читателю предлагается описать собственные подпространства для остальных примеров линейных операторов, рассмотренных выше.

Задача 8.35. *Докажите, что любое собственное подпространство V_λ оператора φ φ-инвариантно. (Указание: воспользуйтесь Предложением 8.12).*

Задача 8.36. *1) Покажите, что оператор $\varphi\colon V \to V$, для которого любой вектор $0 \neq v \in V$ является собственным, имеет вид $\lambda \operatorname{Id}_V$.*

2) Выведите из предыдущего пункта следующий результат: оператор, коммутирующий со всеми операторами на V, имеет вид $\lambda \operatorname{Id}_V$ (ср. с Задачей 2.12)

Решение. Пусть дан оператор φ, для которого любой ненулевой вектор является собственным; докажем, что у него единственное собственное значение. Действительно, если u, v — собственные векторы φ, отвечающие собственным значениям $\lambda \neq \mu$, то, во-первых, они неколлинеарны, а во-вторых, $\varphi(u+v) = \lambda u + \mu v$, но одновременно $u+v$ — собственный вектор φ с некоторым собственным значением ν, то есть $\varphi(u+v) = \nu(u+v)$, откуда $(\lambda-\nu)u + (\mu-\nu)v = 0$, поэтому из линейной независимости u и v получаем $\lambda = \nu = \mu$.

Для доказательства пункта 2) воспользуемся следующим соображением. Если φ коммутирует с оператором ψ, то, согласно Предложению 8.12, подпространство $\operatorname{Ker}\psi \subset V$ является φ-инвариантным. Так как любое подпространство в V является ядром какого-то оператора на V, то любое подпространство в V является φ-инвариантным. Причем из пункта 1) следует, что достаточно рассмотреть одномерные подпространства: если любое одномерное подпространство в V является φ-инвариантным, то $\varphi = \lambda \operatorname{Id}_V$.

Более конкретно, для любого $0 \neq v \in V$ существует такой оператор $\psi\colon V \to V$, для которого $\operatorname{Ker}\psi = \langle v \rangle$. Тогда если φ коммутирует со всеми операторами на V, в частности, с ψ, то, согласно Предложению 8.12, подпространство $\langle v \rangle \subset V$ является φ-инвариантным, то есть v — собственный вектор φ. Поскольку это верно для любого ненулевого вектора v, то по пункту 1) оператор φ имеет требуемый вид. ■

Равенство (64) подсказывает метод нахождения собственных подпространств. А именно, пусть в V выбран базис $\{e_1, \ldots, e_n\}$ и A — матрица оператора φ в этом базисе. Тогда оператор $\varphi - \lambda \operatorname{Id}_V$ в этом базисе имеет матрицу $A - \lambda E$. Его вырожденность (то есть условие $V_\lambda \neq 0$) равносильно вырожденности матрицы $A - \lambda E$, что, как мы знаем из теории определителей, равносильно равенству $\det(A - \lambda E) = 0$.

Таким образом, $\lambda \in \mathbb{K}$ — *собственное значение φ тогда и только тогда, когда* $\det(A - \lambda E) = 0$, где A — матрица φ (в произвольном базисе).

Для произвольной матрицы $A \in \operatorname{Mat}_n(\mathbb{K})$ порядка n рассмотрим выражение $\chi_A(t) := \det(tE - A) = (-1)^n \det(A - tE)$ от переменной t. То есть $\chi_A(t)$ — определитель матрицы

$$\begin{pmatrix} a_{11}-t & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22}-t & a_{23} & \ldots & a_{2n} \\ a_{31} & a_{32} & a_{33}-t & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn}-t \end{pmatrix}, \tag{65}$$

взятый со знáком $(-1)^n$. Так как определитель матрицы равен сумме со знаками произведений, в которые входит по одному элементу из каждой строки и из каждого столбца

(см. формулу полного разложения определителя (19)), то $\chi_A(t)$ является многочленом от t степени n с коэффициентами из поля $\mathbb{K}$, то есть $\chi_A(t) \in \mathbb{K}[t]$. Более точно,

$$\chi_A(t) = t^n - (\operatorname{tr} A)t^{n-1} + \ldots + (-1)^n \det A. \tag{66}$$

Чтобы убедиться в том, что коэффициент перед t^{n-1} действительно равен $-\operatorname{tr} A$, заметим, что если в формулу полного разложения определителя матрицы (65) входит произведение ее элементов, содержащее недиагональный элемент a_{ij}, то в это произведение не входят диагональные элементы $a_{ii} - t$ и $a_{jj} - t$, а значит оно является многочленом от t степени, не превосходящей $n-2$. Таким образом, коэффициенты перед t^{n-1} в $\chi_A(t)$ и в $(a_{11} - t)(a_{22} - t)\ldots(a_{nn} - t)$ равны, а последний, как легко видеть, равен $-\operatorname{tr} A$. Для нахождения свободного члена достаточно положить $t = 0$ в определении $\chi_A(t)$.

Из доказанного выше следует, что $\lambda \in \mathbb{K}$ является собственным значением оператора φ тогда и только тогда, когда λ — корень многочлена $\chi_A(t)$ (для матрицы A оператора φ в произвольном базисе).

Выше мы уже видели, что некоторые характеристики матриц линейных операторов не зависят от выбора базиса, в котором записывается матрица, и, таким образом, являются инвариантами самогó оператора. Таковы например $\operatorname{rk} A$ (являющийся инвариантом даже для линейных отображений) и $\det A$. Поэтому можно говорить про ранг линейного отображения $\operatorname{rk}\varphi$ (в частности, линейного оператора) и определитель линейного оператора, $\det\varphi$.

Оказывается, для всех матриц A одного оператора φ многочлены $\chi_A(t)$ совпадают. Действительно, если A' — матрица того же оператора в новом базисе, связанном с исходным матрицей перехода C, то $A' = C^{-1}AC$ и мы имеем

$$\chi_{A'}(t) = \det(tE - A') = \det(C^{-1}(tE)C - C^{-1}AC) = \det(C^{-1}(tE - A)C) = \tag{67}$$

$$= (\det C)^{-1}(\det(tE - A))\det C = \det(tE - A) = \chi_A(t).$$

Равенство $\chi_{A'}(t) = \chi_A(t)$ является равенством двух многочленов, в частности, выполнено при любом $t \in \mathbb{K}$ (напомним, мы рассматриваем случай $\mathbb{K} = \mathbb{R}$ или $\mathbb{C}$). Так как степени переменной t линейно независимы как функции, то отсюда следует, что все коэффициенты указанных многочленов равны. Поэтому многочлен $\chi_A(t)$ (и все его коэффициенты, в частности, след $\operatorname{tr} A$ и определитель $\det A$) являются инвариантами линейного оператора. Многочлен $\chi_A(t)$ называется *характеристическим многочленом* оператора φ и обозначается $\chi_\varphi(t)$. То, что этот многочлен является инвариантом оператора φ (то есть не зависит от базиса, в котором рассматривается его матрица), называется *инвариантностью характеристического многочлена.*

Замечание 8.37. Инвариантность характеристических многочленов имеет место для операторов над произвольным полем $\mathbb{K}$ (а не только $\mathbb{R}$ и $\mathbb{C}$). Причем доказательство дается той же выкладкой (67), только ее результат нужно проинтерпретировать как равенство определителей матриц с элементами в коммутативном кольце $\mathbb{K}[t]$. Теория определителей таких матриц вполне аналогична теории определителей матриц с

элементами из поля, и заинтересованный читатель легко убедится, что основные результаты об определителях непосредственно переносятся на этот случай.

Более подробно, $tE - A$, $tE - A' \in \mathrm{Mat}_n(\mathbb{K}[t])$, и тогда $\det(tE - A)$, $\det(tE - A') \in \mathbb{K}[t]$ и выкладка (67) показывает, что $\chi_A(t)$ и $\chi_{A'}(t)$ равны как формальные многочлены (а не только как функции).

Задача 8.38. *Найдите характеристические многочлены для рассмотренных выше примеров линейных операторов.*

Задача 8.39. *Верно ли, что если характеристические многочлены матриц A и B совпадают, то указанные матрицы являются матрицами одного оператора в разных базисах?*

Задача 8.40. *Пусть φ — оператор поворота в трехмерном евклидовом пространстве на угол α. Пусть A — матрица этого оператора в некотором (не обязательно ортонормированном) базисе. Выразите угол поворота α через элементы матрицы A. (Указание: воспользуйтесь инвариантностью следа).*

Задача 8.41. *Пусть φ — проектор, то есть $\varphi^2 = \varphi$. Докажите, что* $\mathrm{rk}\,\varphi = \mathrm{tr}\,\varphi$.

Задача 8.42. *Докажите, что любой многочлен $f(t) \in \mathbb{K}[t]$ степени n со старшим коэффициентом 1 является характеристическим многочленом некоторой матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$. (Указание: постарайтесь построить такую матрицу явно для произвольного такого многочлена).*

Выше мы фактически доказали следующую Теорему.

Теорема 8.43. *Элемент $\lambda \in \mathbb{K}$ является собственным значением оператора φ тогда и только тогда, когда он является корнем его характеристического многочлена $\chi_\varphi(t)$, лежащим в поле $\mathbb{K}$.*

Напомним, что у многочлена $p(t) \in \mathbb{K}[t]$ степени n не более n корней в $\mathbb{K}$ с учетом кратности (в частности, не более n различных корней), причем если поле $\mathbb{K}$ алгебраически замкнуто[40], то их в точности n с учетом кратности. Таким образом, у оператора в n-мерном пространстве не более n различных собственных значений, но может быть и меньше: корни характеристического многочлена могут быть кратными, а могут не принадлежать полю $\mathbb{K}$, если последнее не алгебраически замкнуто.

Причину последней оговорки (про поле) в формулировке предыдущей Теоремы проясняет следующий пример.

Пример 8.44. Пусть φ — оператор поворота на угол $\pi/2$ на евклидовой плоскости (это векторное пространство над полем $\mathbb{R}$). Мы знаем, что у него нет собственных векторов, а значит нет и собственных значений. В то же время в ортонормированном базисе он имеет матрицу $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и его характеристической многочлен равен $\chi_\varphi(t) = t^2 + 1$. Этот многочлен не имеет вещественных корней, в то же время имеет два комплексных корня $\pm i$.

[40] Алгебраическая замкнутость поля $\mathbb{K}$ означает, что любой многочлен $p(t) \in \mathbb{K}[t]$ положительной степени имеет корень в $\mathbb{K}$, отсюда по теореме Безу следует формулируемый далее результат.

Чтобы отличить собственные значения оператора от общих корней его характеристического многочлена (которые не обязаны лежать в поле $\mathbb{K}$), последние мы будем называть *характеристическими числами* оператора. Таким образом, собственные значения — в точности характеристические числа, которые лежат в поле $\mathbb{K}$ (напомним, что это поле, над которым определено наше векторное пространство).

Следствие 8.45. *Всякий оператор в пространстве положительной размерности над полем $\mathbb{C}$ имеет собственный вектор.*

Доказательство. Пусть $\varphi\colon V \to V$ — такой оператор и $\chi_\varphi(t) \in \mathbb{C}[t]$ — его характеристический многочлен. Из алгебраической замкнутости поля $\mathbb{C}$[41] следует, что $\chi_\varphi(t)$ имеет комплексный корень $\lambda \in \mathbb{C}$. Согласно предыдущей Теореме, он будет собственным значением оператора φ. ∎

Задача 8.46. *Пусть V — нечетномерное векторное пространство над полем $\mathbb{R}$, тогда любой линейный оператор $\varphi\colon V \to V$ имеет собственный вектор.*

Замечание 8.47. Мы знаем, что в четномерном вещественном векторном пространстве не любой оператор имеет одномерное инвариантное подпространство (которое обязательно порождается собственным вектором). Однако любой линейный оператор на конечномерном вещественном пространстве положительной размерности имеет одно- или двумерное инвариантное подпространство. Доказательство этого факта дано ниже (см. Следствие 12.63), интересующийся читатель может прочитать его прямо сейчас (или доказать этот факт самостоятельно). Отметим, что этот результат — следствие того, что любой неприводимый многочлен над $\mathbb{R}$ имеет степень 1 или 2.

Теперь мы знаем как искать собственные значения оператора φ, осталось выяснить как искать соответствующие собственные подпространства V_λ. Так как $V_\lambda = \operatorname{Ker}(\varphi - \lambda \operatorname{Id}_V)$, то в базисе, в котором φ имеет матрицу A, нахождение $V_\lambda \subset V$ сводится к решению СЛОУ с матрицей коэффициентов $A - \lambda E$. То есть ФСР указанной системы даст базис в V_λ. Заметим, что так как λ — корень характеристического многочлена, то $\det(A - \lambda E) = 0$, поэтому указанная система имеет нетривиальное решение, причем $\dim V_\lambda = \dim V - \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)$ (см. формулу (60)).

Таким образом, алгоритм решения задачи на нахождение собственных векторов оператора φ в конечномерном пространстве V над полем $\mathbb{K}$ следующий. Выбираем в V какой-то базис $\{e_1, \ldots, e_n\}$, находим матрицу A оператора φ в этом базисе. Находим его характеристический многочлен $\chi_\varphi(t) = \det(tE - A)$. Находим корни $\chi_\varphi(t)$, лежащие в поле $\mathbb{K}$, они — в точности все собственные значения φ. Пусть $\{\lambda_1, \ldots, \lambda_k\}$ — все собственные значения φ. Для каждого λ_i решаем СЛОУ с матрицей $A - \lambda_i E$, тем самым находим собственное

[41] В этом курсе мы этот факт принимаем без доказательства.

подпространство V_{λ_i}. (Точнее, выбрав базис $\{e_1, \ldots, e_n\}$, мы отождествили V с пространством столбцов $\mathbb{K}^n$, при этом изоморфизме V_{λ_i} отождествляется с пространством решений указанной системы).

8.4 Диагонализируемость

Из Задачи 8.18 (или непосредственно из определений диагонализируемости и собственного вектора) легко следует, что оператор $\varphi\colon V \to V$ диагонализируем тогда и только тогда, когда в V существует базис, состоящий из его собственных векторов. В таком базисе (если он существует) матрица φ будет диагональной с собственными значениями на главной диагонали. Главная цель данного параграфа — получить удобный критерий существования для оператора φ базиса из собственных векторов.

Вот первый важный результат в этом направлении.

Теорема 8.48. *Собственные подпространства оператора φ, отвечающие разным собственным значениям, линейно независимы.*

Доказательство. Очевидно, что одно собственное подпространство линейно независимо. Пусть $V_1, \ldots, V_k$ — набор из k собственных подпространств оператора φ, отвечающих попарно различным собственным значениям $\lambda_1, \ldots, \lambda_k$. Предположим по индукции, что набор из $k-1$ собственного подпространства $V_1, \ldots, V_{k-1}$ линейно независим; докажем, что тогда и $V_1, \ldots, V_k$ линейно независимы.

Нам нужно доказать, что если

$$v_1 + v_2 + \ldots + v_k = 0, \tag{68}$$

причем $v_i \in V_i$, то все $v_i = 0$. Применяя к обеим частям равенства (68) оператор φ, получаем

$$\lambda_1 v_1 + \ldots + \lambda_{k-1} v_{k-1} + \lambda_k v_k = 0. \tag{69}$$

Вычитая теперь из (69) умноженное на λ_k (68), получаем

$$(\lambda_1 - \lambda_k)v_1 + \ldots + (\lambda_{k-1} - \lambda_k)v_{k-1} = 0,$$

откуда с учетом индуктивного предположения имеем $(\lambda_i - \lambda_k)v_i = 0$ при $i = 1, \ldots, k-1$, но так как $\lambda_i - \lambda_k \neq 0$, то $v_1 = \ldots = v_{k-1} = 0$, откуда с учетом (68) также и $v_k = 0$, что и требовалось доказать. ■

Таким образом, $V_1 \oplus \ldots \oplus V_k \subset V$, и в V существует базис, состоящий из собственных векторов оператора φ тогда и только тогда, когда

$$V_1 \oplus \ldots \oplus V_k = V. \tag{70}$$

Мы знаем, что равенство (70) равносильно тому, что $\sum_{i=1}^{k} \dim V_i = \dim V$ (см. Предложение 7.25).

Рассмотренные ранее Примеры 8.33 и 8.34 показывают, что примерами диагонализируемых операторов являются проекторы (поскольку если $\varphi\colon V \to V$ — проектор, связанный с разложением $V = U \oplus W$, то подпространства U и W — его собственные подпространства с собственными значениями 1 и 0 соответственно) и отражения (поскольку если $\varphi\colon V \to V$ — отражение, то $V = V^+ \oplus V^-$, где V^+ и V^- — собственные подпространства с собственными значениями 1 и -1 соответственно).

Замечание 8.49. Пусть оператор $\varphi\colon V \to V$ диагонализируем и $V = V_1 \oplus \ldots \oplus V_k$ — соответствующее разложение V в прямую сумму его собственных подпространств, $V_i := V_{\lambda_i}$. Пусть $P_i\colon V \to V$ — проектор на подпространство $V_i \subset V$ параллельно прямой сумме оставшихся подпространств, $i = 1, \ldots, k$. Тогда $P_i^2 = P_i$, $P_iP_j = 0$ при $i \neq j$ и $P_1 + \ldots + P_k = \mathrm{Id}_V$. Кроме того, оператор φ равен $\sum_{i=1}^k \lambda_i P_i$, так как φ и указанная линейная комбинация проекторов одинаково действуют на произвольный вектор. Последнее выражение называется *спекральным разложением* оператора φ.

Из предыдущей Теоремы следует следующее *достаточное условие диагонализируемости.*

Следствие 8.50. *Если характеристический многочлен $\chi_\varphi(t)$ имеет $n = \dim V$ различных корней, принадлежащих полю $\mathbb{K}$, то оператор φ диагонализируем.*

Доказательство. Каждый корень $\chi_\varphi(t)$, принадлежащий полю $\mathbb{K}$, является собственным значением φ, то есть φ имеет $n = \dim V$ различных собственных значений $\lambda_1, \ldots, \lambda_n$, и каждому из них отвечает собственное подпространство $V_i \neq 0$, причем собственные подпространства образуют прямую сумму. Значит, $\dim(V_1 \oplus \ldots \oplus V_n) = \sum_{i=1}^n \dim V_i \geq n$ и значит $V = V_1 \oplus \ldots \oplus V_n$. ∎

Пример тождественного оператора (или проектора) показывает, что предыдущее достаточное условие диагнализируемости не является необходимым.

Пусть $\varphi\colon V \to V$ —линейный оператор, $U \subset V$ — φ-инвариантное подпространство, $\varphi|_U\colon U \to U$ — ограничение φ на U.

Предложение 8.51. *Характеристический многочлен ограничения оператора на инвариантное подпространство делит характеристический многочлен самого́ оператора, $\chi_{\varphi|_U}(t) \mid \chi_\varphi(t)$.*

Доказательство. Выберем базис $\{e_1, \ldots, e_k\}$ в U и продолжим его до базиса $\{e_1, \ldots, e_n\}$ в V, тогда матрица A оператора φ в нем будет иметь блочнотреугольный вид

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix},$$

где B — матрица $\varphi|_U$ в базисе $\{e_1, \ldots, e_k\}$ (см. (62)). Имеем

$$\chi_\varphi(t) = \det(tE - A) = \det \begin{pmatrix} tE - B & -C \\ 0 & tE - D \end{pmatrix} =$$

$$= \det(tE - B)\det(tE - D) = \chi_{\varphi|U}(t)\det(tE - D),$$

где мы воспользовались Теоремой 3.38. ∎

Напомним, что c называется *корнем кратности* m многочлена $p(t)$, если $p(t) = (t - c)^m q(t)$, где $q(c) \neq 0$.

Определение 8.52. Назовем *алгебраической кратностью* собственного значения λ оператора φ кратность λ как корня характеристического многочлена $\chi_\varphi(t)$. Обозначим ее $m(\lambda)$.

Определение 8.53. Назовем *геометрической кратностью* собственного значения λ оператора φ размерность соответствующего ему собственного подпространства $V_\lambda \subset V$. Обозначим ее $g(\lambda)$.

Следствие 8.54. *Для любого собственного значения λ оператора φ его геометрическая кратность не превосходит алгебраическую, $g(\lambda) \leq m(\lambda)$.*

Доказательство. Напомним (см. Задачу 8.35), что для любого собственного значения λ оператора φ соответствующее собственное подпространство V_λ φ-инвариантно. Заметим, что ограничение $\varphi|_{V_\lambda}$ оператора φ на собственное подпространство V_λ является оператором умножения на λ, то есть $\varphi|_{V_\lambda} = \lambda \operatorname{Id}_{V_\lambda}$. Поэтому $\chi_{\varphi|_{V_\lambda}}(t) = (t - \lambda)^{g(\lambda)}$. Согласно предыдущему Предложению $(t - \lambda)^{g(\lambda)} \mid \chi_\varphi(t)$. ∎

Легко привести примеры операторов, у которых геометрические кратности собственных значений равны алгебраическим (тождественный, проекторы). Следующий пример показывает, что неравенство в предыдущем Следствии может быть строгим.

Пример 8.55. Рассмотрим оператор $\varphi := \frac{d}{dx}$ на пространстве $V := \mathbb{R}[x]_n$. Легко посчитать, что $\chi_\varphi(t) = t^{n+1}$. В то же время единственному собственному значению $\lambda = 0$ отвечает одномерное собственное подпространство (состоящее из констант). Значит, $1 = g(\lambda) < m(\lambda) = n + 1$ при $n > 0$.

Напомним, что для многочлена $p(t) \in \mathbb{K}[t]$ степени n число его корней в поле $\mathbb{K}$ с учетом кратности не превосходит n, причем в точности равно n тогда и только тогда, когда все корни $p(t)$ принадлежат $\mathbb{K}$ (равносильно, когда $p(t)$ раскладывается на линейные множители над полем $\mathbb{K}$), см. Теорему 5.16.

Теперь мы в состоянии доказать обещанный ранее критерий диагонализируемости.

Теорема 8.56. *Для существования в V базиса из собственных векторов оператора $\varphi\colon V \to V$ необходимо и достаточно одновременного выполнения следующих двух условий:*

1) *все корни характеристического многочлена $\chi_\varphi(t)$ лежат в поле $\mathbb{K}$ (и, значит, являются собственными значениями φ);*

2) для каждого собственного значения λ оператора φ его геометрическая кратность равна алгебраической, $g(\lambda) = m(\lambda)$.

Доказательство. Пусть $\lambda_1, \ldots, \lambda_k$ — все различные собственные значения оператора φ, $g_1, \ldots, g_k$ — их геометрические, а $m_1, \ldots, m_k$ — алгебраические кратности. Базис из собственных векторов φ существует тогда и только тогда, когда $V = V_1 \oplus \ldots \oplus V_k$, что равносильно

$$n := \dim V = \sum_{i=1}^{k} g_i \tag{71}$$

(ср. текст после Теоремы 8.48).

С другой стороны,

$$n = \deg \chi_\varphi(t) \geq \sum_{i=1}^{k} m_i, \tag{72}$$

причем в силу замечания перед этой Теоремой, равенство имеет место тогда и только тогда, когда выполнено условие 1).

Если не выполнено условие 1), то $n > \sum_{i=1}^{k} m_i$, а так как $g_i \leq m_i$ при $i = 1, \ldots, k$, то тем более $n > \sum_{i=1}^{k} g_i$ и значит φ не диагонализируем.

Если не выполнено условие 2), то для какого-то i $g_i < m_i$, откуда $\sum_{i=1}^{k} g_i < \sum_{i=1}^{k} m_i \leq n$, и значит φ опять не диагонализируем.

Таким образом, если φ диагонализируем, то выполнены оба условия 1) и 2)[42].

С другой стороны, если выполнены и 1) и 2), то $n = \sum_{i=1}^{k} m_i$ и $g_i = m_i$ при $i = 1, \ldots, k$, а значит выполнено (71), что, как мы видели, равносильно диагонализируемости. ∎

Мы видим, что препятствия к диагонализируемости бывают двух типов. Первый тип связан с тем, что поле $\mathbb{K}$ не замкнуто алгебраически и поэтому не все корни характеристического многочлена в нем лежат. Этот случай “лечится” расширением поля (например, поля $\mathbb{R}$ до поля $\mathbb{C}$). Рассмотрим пример такого рода.

Пример 8.57. Рассмотрим оператор $\varphi := \frac{d}{dx}$ на линейной оболочке

$$V := \langle \sin x, \cos x \rangle_{\mathbb{R}} = \{\alpha \sin x + \beta \cos x \mid \alpha, \beta \in \mathbb{R}\}$$

над полем $\mathbb{R}$. Он имеет матрицу $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ в базисе $\{\sin x, \cos x\}$ и его характеристический многочлен $\chi_\varphi(t) = t^2 + 1$ не имеет вещественных корней (соответственно у φ нет собственных векторов).

Рассмотрим теперь

$$V^{\mathbb{C}} := \langle \sin x, \cos x \rangle_{\mathbb{C}} = \{\alpha \sin x + \beta \cos x \mid \alpha, \beta \in \mathbb{C}\}$$

— линейную оболочку тех же функций над полем $\mathbb{C}$ с базисом $\{\sin x, \cos x\}$. Таким образом, она является двумерным векторным пространством над полем $\mathbb{C}$, и на ней также

[42] Здесь логически мы пользуемся одним из законов Де Моргана $\neg(x \wedge y) = (\neg x) \vee (\neg y)$.

действует ($\mathbb{C}$-линейный) оператор $\varphi^{\mathbb{C}} = \frac{d}{dx}$, имеющий ту же матрицу в базисе $\{\sin x, \cos x\}$. Однако у $\varphi^{\mathbb{C}}$ уже есть собственные значения i и $-i$, являющиеся комплексными корнями многочлена $t^2 + 1$. Это приводит к тому, что у $\varphi^{\mathbb{C}}$ есть собственные векторы e^{ix} (с собственным значением i) и e^{-ix} (с собственным значением $-i$), поскольку $\frac{d}{dx}e^{\alpha x} = \alpha e^{\alpha x}$ для $\alpha \in \mathbb{C}$. Указанные экспоненты действительно лежат в $V^{\mathbb{C}}$, так как $e^{ix} = \cos x + i \sin x$ и $e^{-ix} = \cos x - i \sin x$ по формуле Эйлера. В базисе $\{e^{ix}, e^{-ix}\}$ в $V^{\mathbb{C}}$ оператор $\varphi^{\mathbb{C}}$ имеет диагональную матрицу $\operatorname{diag}(i, -i)$. Другими словами, существует матрица $C \in \operatorname{Mat}_2(\mathbb{C})$ (а именно, матрица перехода от базиса $\{\cos x, \sin x\}$ к базису $\{e^{ix}, e^{-ix}\}$ в $V^{\mathbb{C}}$) такая, что матрица

$$C^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} C$$

диагональна, но не существует такой вещественной матрицы $C \in \operatorname{Mat}_2(\mathbb{R})$.

Другой, более "злостный" тип препятствий к диагонализируемости связан с тем, что геометрическая кратность какого-то собственного значения меньше алгебраической, в этом случае расширение поля не поможет. Пример такой ситуации дает оператор дифференцирования на пространстве многочленов. Конечно, указанные типы препятствий могут встречаться вместе.

Пусть оператор $\varphi\colon V \to V$ имеет матрицу A в некотором базисе $\{e_1, \ldots, e_n\}$ в V. Из предыдущего вытекает следующий алгоритм исследования φ на диагонализируемость. Находим характеристический многочлен $\chi_\varphi(t) = \det(tE - A)$ и выясняем, все ли его корни принадлежат полю $\mathbb{K}$. Если ответ "нет", то оператор не диагонализируем, если "да", то для каждого корня λ_i (являющегося собственным значением φ) проверяем, верно ли равенство $g(\lambda_i) = m(\lambda_i)$. Так как

$$g(\lambda_i) := \dim V_{\lambda_i} = n - \operatorname{rk}(A - \lambda_i E),$$

то равенство $g(\lambda_i) = m(\lambda_i)$ равносильно $m(\lambda_i) = n - \operatorname{rk}(A - \lambda_i E)$. Если для каждого корня λ_i данное равенство справедливо, то φ диагонализируем, в противном случае — нет.

Пусть $\{v_1^i, \ldots, v_{g(i)}^i\}$ — базисы во всех собственных подпространствах $V_i := V_{\lambda_i}$, $i = 1, \ldots, k$ оператора φ. Если φ диагонализируем, то $V = V_1 \oplus \ldots \oplus V_k$, и объединение указанных базисов есть базис в V, состоящий из собственных векторов оператора φ. В нем матрица оператора φ диагональна, точнее $A' = \operatorname{diag}(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots, \lambda_n)$, где кратность вхождения λ_i равна $g(i)$. Причем $A' = C^{-1}AC$, где C — матрица перехода от исходного базиса $\{e_1, \ldots, e_n\}$ к полученному базису из собственных векторов.

Задача 8.58. *Пусть $\varphi\colon V \to V$ — линейный оператор. Докажите, что если $\operatorname{Ker}\varphi \subsetneq \operatorname{Ker}(\varphi^2)$, то φ не диагонализируем.*

Решение. Пусть $u \in \operatorname{Ker}\varphi^2 \backslash \operatorname{Ker}\varphi$. Очевидно, что подпространство $U := \langle \operatorname{Ker}\varphi, u\rangle \subset V$ является φ-инвариантным. Пусть $\{e_1, \ldots, e_k\}$ — базис в пространстве $\operatorname{Ker}\varphi$, тогда, выписывая матрицу $\varphi|_U$ в базисе $\{e_1, \ldots, e_k, u\}$ пространства U мы получаем, что $\chi_{\varphi|_U}(t) = t^{k+1}$,

где $k = \dim(\operatorname{Ker}\varphi)$, причем, согласно Предложению 8.51, $\chi_{\varphi|_U}(t) \mid \chi_\varphi(t)$. Таким образом, в этом случае алгебраическая кратность собственного значения 0 оператора φ строго больше геометрической (равной k).

Приведем также другое доказательство. Если оператор диагонализируем, то в некотором базисе его матрица диагональна. Легко видеть, что при возведении диагональной матрицы в квадрат ее диагональные элементы возводятся в квадрат, поэтому ее ранг не меняется, следовательно $\dim\operatorname{Im}\varphi = \dim\operatorname{Im}(\varphi^2)$, а значит и $\dim\operatorname{Ker}\varphi = \dim\operatorname{Ker}(\varphi^2)$. ∎

Задача 8.59. *Пусть $\varphi\colon V \to V$ — линейный оператор. Докажите, что $V = \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$ тогда и только тогда, когда $\operatorname{Ker}\varphi = \operatorname{Ker}(\varphi^2)$.*

То есть оператор, у которого ядро и образ имеют нетривиальное пересечение, недиагонализируем.

Задача 8.60. *Напишите матрицу какого-нибудь линейного оператора φ на трехмерном пространстве, если известно, что вектор с координатами $(1,2,3)^T$ лежит и в ядре и в образе φ. Будет ли такой оператор диагонализируемым?*

Задача 8.61. *Пусть $\dim V \geq 2$. Докажите, что оператор $\varphi\colon V \to V$ ранга 1 диагонализируем тогда и только тогда, когда $\operatorname{tr}\varphi \neq 0$.*

Решение. Обозначим $n := \dim V$. Пусть $U := \operatorname{Ker}\varphi$, тогда из $\operatorname{rk}\varphi = 1$ следует $\dim U = n-1$ и U является собственным подпространством φ, отвечающим собственному значению 0. Значит по Следствию 8.54 $\chi_\varphi(t) = t^{n-1}(t-\lambda)$, причем $\lambda = \operatorname{tr}\varphi \in \mathbb{K}$ (см. формулу (66)). Если $\lambda = 0$, то алгебраическая кратность собственного значения 0 (равная n) строго больше геометрической (равной $n-1$), поэтому такой оператор не диагонализируем. Если $\lambda \neq 0$, то у φ есть еще одно собственное значение λ, значит помимо $V_0 = U$ есть еще одно собственное подпространство V_λ, следовательно $V = V_0 \oplus V_\lambda$, и тогда φ диагонализируем. ∎

Задача 8.62. *Пусть φ — линейный оператор на V, $\{\lambda_1, \ldots, \lambda_k\}$ — набор его различных собственных значений, принадлежащих основному полю, $V_{\lambda_j} \subset V$ — соответствующие собственные подпространства. Пусть $U \subset V$ — φ-инвариантное подпространство. Докажите, что если для $\mathbf{u} \in U$ существует представление*

$$\mathbf{u} = \mathbf{v}_1 + \ldots + \mathbf{v}_k, \tag{73}$$

где $\mathbf{v}_j \in V_{\lambda_j}$, то $\mathbf{v}_j \in U \ \forall\, j,\ 1 \leq j \leq k$.

Решение. Воспользуемся индукцией по числу l ненулевых слагаемых в разложении (73). Для $l = 1$ утверждение очевидно. Допустим, что требуемое утверждение верно для разложений вида (73) с числом ненулевых компонент $\mathbf{v}_j$, не превосходящим $l-1$, докажем, что тогда утверждение верно для разложений с l ненулевыми компонентами. Без ограничения общности можно считать, что ненулевыми являются первые l компонент в (73). Пусть

$$U \ni \mathbf{u} = \mathbf{v}_1 + \ldots + \mathbf{v}_l, \tag{74}$$

где все $\mathbf{v}_j \neq \mathbf{0}$. Тогда $\varphi(\mathbf{u}) = \lambda_1\mathbf{v}_1 + \ldots + \lambda_l\mathbf{v}_l$. Вычитая из последнего тождества равенство, полученное умножением обеих частей (74) на λ_l, имеем

$$\varphi(\mathbf{u}) - \lambda_l\mathbf{u} = (\lambda_1 - \lambda_l)\mathbf{v}_1 + \ldots + (\lambda_{l-1} - \lambda_l)\mathbf{v}_{l-1}.$$

Мы получили разложение вида (73), содержащее $l-1$ ненулевую компоненту, следовательно, по предположению индукции, $\mathbf{v}_j \in \in U \cap V_{\lambda_j}$, $1 \leq j \leq l-1$. Но тогда из (74) и $\mathbf{v}_l \in U$, что и требовалось доказать. ■

Положив в условии предыдущей задачи $U = \{\mathbf{0}\}$, снова приходим к Теореме 8.48.

Задача 8.63. *a) Докажите, что два диагонализируемых оператора коммутируют тогда и только тогда, когда они имеют общий базис из собственных векторов.*

b) Распространите этот результат на произвольное множество коммутирующих диагонализируемых операторов.

Задача 8.64. *Докажите, что если оператор $\varphi\colon V \to V$ диагонализируем, то и его ограничение $\varphi|_U$ на любое инвариантное подпространство $U \subset V$ диагонализируемо.*

Решение. Очевидно, что оператор φ диагонализируем $\Leftrightarrow V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_k}$. В предыдущей задаче доказано, что если подпространство $U \subset V$ φ-инвариантно, то для представления произвольного вектора $\mathbf{u} \in U$ вида

$$\mathbf{u} = \mathbf{v}_1 + \ldots + \mathbf{v}_k,$$

где $\mathbf{v}_j \in V_{\lambda_j}$, следует $\mathbf{v}_j \in U$ $\forall j$. Другими словами, $U = (U \cap V_{\lambda_1}) \oplus \ldots \oplus (U \cap V_{\lambda_k})$. Отсюда следует диагонализируемость оператора $\varphi|_U$, так как $U \cap V_{\lambda_j}$ — его собственные подпространства.

Другое решение приведено в Задаче 8.77. ■

Задача 8.65. *Пусть оператор $\varphi\colon V \to V$ диагонализируем. Тогда любое его φ-инвариантное подпространство $U \subset V$ имеет φ-инвариантное прямое дополнение $W \subset V$, то есть такое φ-инвариантное подпространство $W \subset V$, что $V = U \oplus W$.*

Решение. В предыдущих обозначениях пусть

$$V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_k}, \quad U = (U \cap V_{\lambda_1}) \oplus \ldots \oplus (U \cap V_{\lambda_k}).$$

Для каждого подпространства $U \cap V_{\lambda_i} \subset V_{\lambda_i}$ выберем произвольное прямое дополнение $W_i \subset V_{\lambda_i}$. Тогда подпространство $W = W_1 \oplus \ldots \oplus W_k \subset V$ является φ-инвариантным и $V = U \oplus W$. ■

Ясно, что утверждение предыдущей задачи можно обратить при условии, что характеристический многочлен оператора φ раскладывается на линейные множители над полем $\mathbb{K}$.

Задача 8.66. *Приведите пример, показывающий, что в линейном пространстве сколь угодно большой размерности над полем $\mathbb{Q}$ у оператора может не быть нетривиальных инвариантных подпространств.*

Решение. Воспользуемся неприводимостью над $\mathbb{Q}$ многочленов "деления круга на p частей" $f_p(t) := \frac{t^p-1}{t-1}$, где p — простое (см. [11], §6 гл. 3). Заметим, что задав произвольный многочлен $g(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1}t + a_n \in \mathbb{Q}[t]$ можно построить линейный оператор φ, для которого $g(t)$ является характеристическим многочленом. А именно, достаточно задать действие φ на базисных векторах следующим образом:

$$\varphi(e_1) = e_2,\ \varphi(e_2) = e_3, \ldots, \varphi(e_{n-1}) = e_n,\ \varphi(e_n) = -a_n e_1 - a_{n-1} e_2 - \ldots - a_1 e_n.$$

Таким образом, оператор на $p-1$-мерном пространстве V над полем $\mathbb{Q}$, действующий на базисе

$$\varphi(e_1) = e_2,\ \varphi(e_2) = e_3,\ \ldots,\ \varphi(e_{p-2}) = e_{p-1},\ \varphi(e_{p-1}) = -e_1 - e_2 - \ldots - e_{p-1}$$

имеет характеристический многочлен $f_p(t)$. Если бы у φ было инвариантное подпространство $U \neq 0, V$, то характеристический многочлен его ограничения $\varphi|_U$ делил бы $f_p(t)$ в кольце $\mathbb{Q}[t]$, что противоречило бы неприводимости $f_p(t)$. ■

8.5 Теорема Гамильтона-Кэли

В предыдущем параграфе мы видели, что не любой оператор диагонализируем даже в случае алгебраически замкнутого поля $\mathbb{K}$ (такого как поле комплексных чисел $\mathbb{C}$). Однако в последнем случае всегда можно найти базис, в котором матрица оператора имеет так называемую жорданову нормальную форму, которую мы рассмотрим в следующей главе. Здесь же мы докажем ослабленную версию теоремы о жордановой нормальной форме, а именно существование у оператора матрицы треугольного вида.

Предложение 8.67. *Для оператора φ в конечномерном пространстве V над алгебраически замкнутым полем $\mathbb{K}$ существует такой базис в V, в котором матрица φ является верхнетреугольной.*

Доказательство. Докажем Предложение индукцией по $n := \dim V$. Если $n = 1$, то Предложение очевидно. Пусть $n > 1$. Так как поле $\mathbb{K}$ алгебраически замкнуто, у φ существует собственное значение $\lambda \in \mathbb{K}$, то есть $V_\lambda := \operatorname{Ker}(\varphi - \lambda \operatorname{Id}_V) \neq 0$. Тогда $\operatorname{Im}(\varphi - \lambda \operatorname{Id}_V) \neq V$ и, значит, $\dim(\operatorname{Im}(\varphi - \lambda \operatorname{Id}_V)) \leq n-1$. Пусть $U \subset V$ — какое-либо $n-1$-мерное подпространство в V, содержащее $\operatorname{Im}(\varphi - \lambda \operatorname{Id}_V)$. Покажем, что оно φ-инвариантно. Действительно, $\forall\, u \in U$

$$\varphi(u) = \varphi(u) - \lambda u + \lambda u = (\varphi - \lambda \operatorname{Id}_V)(u) + \lambda u \in U,$$

поскольку $(\varphi - \lambda \operatorname{Id}_V)(u) \in U$ и $\lambda u \in U$.

Так как $\dim U = n - 1 < n$, то по предположению индукции существует базис $\{e_1, \ldots, e_{n-1}\}$ в U, в котором матрица B оператора $\varphi|_U$ верхнетреугольная. Дополним его произвольным образом до базиса $\{e_1, \ldots, e_{n-1}, e_n\}$ в V. В нем матрица A оператора φ будет иметь вид $\begin{pmatrix} B & C \\ 0 & d \end{pmatrix}$, где C — столбец высоты $n-1$, а d — матрица порядка 1, и A, очевидно, является верхнетреугольной. ∎

Замечание 8.68. Заметим, что геометрический смысл доказанного Предложения состоит в существовании у оператора φ цепочки вложенных φ-инвариантных подпространств[43]

$$0 = V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_{n-1} \subset V_n = V$$

таких, что $\dim V_k = k$, $0 \leq k \leq n$ (см. Задачу 8.20). С этой точки зрения шаг индукции состоит в доказательстве того, что у оператора φ на n-мерном пространстве V существует $n-1$-мерное инвариантное подпространство V_{n-1}, после этого индуктивное предположение можно применить к оператору $\varphi|_{V_{n-1}}$ на V_{n-1}.

Как обстоят дела с существованием треугольной матрицы у преобразования вещественного векторного пространства? Нетрудно заметить, что необходимым условием этого является вещественность всех характеристических чисел (корней характеристического

[43] Такая цепочка называется *флагом*.

многочлена) такого преобразования. Действительно, у треугольной матрицы на главной диагонали стоят характеристические числа. Оказывается, это условие является и достаточным.

Задача 8.69. *Докажите, что если у преобразования φ вещественного пространства V все характеристические числа вещественны, то в V существует базис, в котором φ имеет верхнетреугольную матрицу. (Указание: для доказательства шага индукции воспользуйтесь Предложением 8.51).*

Оператор $\varphi\colon V \to V$ называется *нильпотентным*, если для некоторого натурального N $\varphi^N = 0$. Например, нулевой оператор нильпотентен так же как и оператор дифференцирования на пространстве $\mathbb{R}[x]_n$.

Задача 8.70. *Докажите, что если $\varphi\colon V \to V$ — нильпотентный оператор на конечномерном пространстве V, $\dim V = n$, то в V существует базис $\{e_1, \dots, e_n\}$, в котором φ имеет верхненильтреугольную матрицу (то есть верхнетреугольную матрицу с нулями на главной диагонали).*

Решение (см. также доказательство Леммы 9.3). Доказывать будем индукцией по $n = \dim V$. Если $n = 1$, то нильпотентный оператор на V нулевой и доказываемое утверждение, очевидно, верно. Пусть $n > 1$, положим $V_1 := \varphi(V)$. Из нильпотентности φ следует, что $V_1 \subsetneq V$. Выберем произвольное подпространство $U \subset V$ размерности $n-1$, содержащее V_1. Тогда U φ-инвариантно и ограничение $\varphi|_U$ нильпотентно. По предположению индукции в U найдется базис $\{e_1, \dots, e_{n-1}\}$, в котором $\varphi|_U$ имеет верхненильтреугольную матрицу. Пусть $\{e_1, \dots, e_{n-1}, e_n\}$ — произвольное дополнение до базиса в V. Поскольку $\varphi(e_n) \in U$, то матрица φ в нем также нильтреугольна и шаг индукции доказан. ■

В доказательстве следующей Теоремы нам пригодится следующая Задача.

Пусть φ — оператор на V, $U \subset V$ — его инвариантное подпространство, а $p(t)$ — некоторый многочлен. Тогда можно вычислить многочлен $p(\varphi)$ от оператора φ, это снова будет оператор на V, причем легко убедиться, что U будет его инвариантным подпространством. Затем можно оператор $p(\varphi)$ ограничить на U и получить оператор $p(\varphi)|_U\colon U \to U$. А можно выбрать другой порядок действий: сначала ограничить φ на U, а потом вычислить многочлен $p(\varphi|_U)$, снова получив некоторый оператор на U.

Задача 8.71. *Пусть $\varphi\colon V \to V$ — линейный оператор, $U \subset V$ — φ-инвариантное подпространство. Пусть $p(t) \in \mathbb{K}[t]$ — многочлен. Тогда $p(\varphi)|_U = p(\varphi|_U)$ как линейные операторы на U.*

Доказательство следует непосредственно из определений.

Оказывается, что если подставить матрицу оператора в его характеристический многочлен, получится нулевая матрица. Говорят, что многочлен $p(t)$ *аннулирует* (квадратную!) матрицу A, если $p(A) = 0$ (справа стоит нулевая матрица того же порядка, что и A). Заметим, что если $p(t)$ аннулирует матрицу A оператора φ в каком-то базисе, то он аннулирует его матрицу и в любом другом базисе, так как $p(C^{-1}AC) = C^{-1}p(A)C$ для любой невырожденной матрицы C. Поэтому корректно говорить об аннулирующем многочлене самого́ оператора.

Теорема 8.72. *(Гамильтон-Кэли) Характеристический многочлен $\chi_\varphi(t)$ аннулирует оператор φ.*

Доказательство. Теорему докажем сначала для алгебраически замкнутого поля $\mathbb{K}$.

Снова будем пользоваться индукцией по $n := \dim V$. При $n = 1$ Теорема очевидна: $t - \lambda$ аннулирует $\varphi = \lambda \operatorname{Id}_V$. Пусть $n > 1$. Выберем базис $\{e_1, \dots, e_n\}$ в V, в котором φ имеет верхнетреугольную матрицу $\begin{pmatrix} \mu_1 & * & * & \dots & * \\ 0 & \mu_2 & * & \dots & * \\ 0 & 0 & \mu_3 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \mu_n \end{pmatrix}$. Заметим, что $\mu_1, \dots, \mu_n$ — все собственные значения φ, только не обязательно попарно различные. Характеристический многочлен $\chi_\varphi(t)$ равен $(t - \mu_1) \dots (t - \mu_n)$.

Пусть $U := \langle e_1, \dots, e_{n-1} \rangle \subset V$. Из вида матрицы (конкретно из того, что в последней строчке все элементы кроме μ_n равны нулю) следует, что подпространство $U \subset V$ φ-инвариантно. Легко также видеть, что $\operatorname{Im}(\varphi - \mu_n \operatorname{Id}_V) \subset U$. Так как оператору $\varphi|_U$ отвечает левый верхний блок порядка $n-1$ приведенной выше треугольной матрицы, то $\chi_\varphi(t) = \chi_{\varphi|_U}(t)(t - \mu_n)$, и $\chi_\varphi(\varphi)$ является композицией двух операторов, $\varphi - \mu_n \operatorname{Id}_V$ и $\chi_{\varphi|_U}(\varphi)$, причем образ первого содержится в U, а ограничение второго на U есть $\chi_{\varphi|_U}(\varphi)|_U = \chi_{\varphi|_U}(\varphi|_U)$ (см. Задачу 8.71), что равно нулю по предположению индукции. Значит $\operatorname{Im}(\varphi - \mu_n \operatorname{Id}_V) \subset \operatorname{Ker}(\chi_{\varphi|_U}(\varphi))$, поэтому $\chi_\varphi(\varphi) = \chi_{\varphi|_U}(\varphi) \circ (\varphi - \mu_n \operatorname{Id}_V) = 0$, и шаг индукции тем самым доказан.

Если поле $\mathbb{K}$ не является алгебраически замкнутым (например $\mathbb{K} = \mathbb{R}$), то воспользуемся тем, что его всегда можно вложить в алгебраически замкнутое поле $\mathbb{L}$. Например, вещественную матрицу A можно рассматривать также как комплексную, и для нее Теорема верна (то есть $\chi_A(A) = 0$). Но характеристический многочлен $\chi_A(t)$ не зависит от того, рассматриваем мы A как вещественную или как комплексную матрицу, а значит Теорема верна и для исходного поля $\mathbb{K}$. ∎

Замечание 8.73. Дадим набросок другого доказательства теоремы Гамильтона-Кэли, основанного на формуле (23) для присоединенной матрицы, которое работает для произвольного поля $\mathbb{K}$.

Рассмотрим алгебру $\operatorname{Mat}_n(\mathbb{K}[t])$ матриц порядка n с коэффициентами в алгебре многочленов $\mathbb{K}[t]$. Заметим, что любую матрицу $B \in \operatorname{Mat}_n(\mathbb{K}[t])$ можно однозначно записать в виде многочлена от переменной t с коэффициентами в $\operatorname{Mat}_n(\mathbb{K})$. Поэтому рассмотрим алгебру $\operatorname{Mat}_n(\mathbb{K})[t]$, состоящую из формальных выражений $M(t) = M_0 + M_1 t + M_2 t^2 + \dots + M_k t^k$, $M_i \in \operatorname{Mat}_n(\mathbb{K})$, с умножением

$$M(t)N(t) = \left(\sum_{i=1}^{k} M_i t^i \right) \left(\sum_{j=1}^{l} N_j t^j \right) = \sum_{i,\,j} (M_i N_j) t^{i+j}.$$

Лемма 8.74. Имеет место изоморфизм $\mathbb{K}$-алгебр $\operatorname{Mat}_n(\mathbb{K}[t]) \cong \operatorname{Mat}_n(\mathbb{K})[t]$.

Доказательство. Рассмотрим матрицы $E_{ij}^k \in \operatorname{Mat}_n(\mathbb{K}[t])$, у которых на i,j-м месте стоит t^k, а в остальных местах нули.

Легко видеть, что матрицы E_{ij}^k, где $1 \le i,\, j \le n$, $k \ge 0$, образуют базис в $\mathrm{Mat}_n(\mathbb{K}[t])$ над $\mathbb{K}$. Отобразим его в базис $E_{ij}t^k$ в $\mathrm{Mat}_n(\mathbb{K})[t]$. Также легко видеть, что элементы обоих базисов перемножаются по одинаковому закону

$$E_{ij}^k \cdot E_{pq}^r = \delta_{jp} E_{iq}^{k+r}, \quad E_{ij}t^k \cdot E_{pq}t^r = \delta_{jp} E_{iq} t^{k+r}$$

(где δ_{jp} — дельта-символ Кронекера). Умножение базисных элементов однозначно определяет умножение их линейных комбинаций по дистрибутивности (билинейности), и тем самым однозначно задает умножение во всей алгебре, и, значит, две данные алгебры действительно оказываются изоморфными. ■

Далее, заметим, что определение и все теоремы об определителях работают (с очевидными модификациями)[44], если заменить поле $\mathbb{K}$ на произвольное коммутативное ассоциативное кольцо с единицей R, например $\mathbb{Z}$ или $\mathbb{K}[t]$.

Итак, рассмотрим матрицу $tE - A$, где $A \in \mathrm{Mat}_n(\mathbb{K})$, как матрицу с элементами из кольца $\mathbb{K}[t]$, то есть как элемент $\mathrm{Mat}_n(\mathbb{K}[t])$. Для нее продолжает оставаться верной формула (23)

$$(tE - A)\widehat{(tE - A)} = \det(tE - A)E = \chi_A(t)\, E, \tag{75}$$

понимаемая как тождество в кольце $\mathrm{Mat}_n(\mathbb{K}[t]) \cong \mathrm{Mat}_n(\mathbb{K})[t]$.

Вот иллюстрация для случая $n = 2$:

$$tE - A = \begin{pmatrix} t - a_{11} & -a_{12} \\ -a_{21} & t - a_{22} \end{pmatrix}, \qquad \widehat{tE - A} = \begin{pmatrix} t - a_{22} & a_{12} \\ a_{21} & t - a_{11} \end{pmatrix},$$

$$\begin{pmatrix} t - a_{11} & -a_{12} \\ -a_{21} & t - a_{22} \end{pmatrix} \begin{pmatrix} t - a_{22} & a_{12} \\ a_{21} & t - a_{11} \end{pmatrix} = (t^2 - (a_{11} + a_{22})t + a_{11}a_{22} - a_{12}a_{21})E.$$

Далее мы хотим в многочлен $M(t) = \sum_{i=0}^k M_i t^i \in \mathrm{Mat}_n(\mathbb{K})[t]$ вместо переменной t подставить матрицу $A \in \mathrm{Mat}_n(\mathbb{K})$, но эта операция в общем случае не обладает хорошими свойствами (не задает гомоморфизм алгебр, и, более того, не определена корректно — поскольку зависит от того, с какой стороны от коэффициентов мы пишем символ t). Последнее связано с тем, что переменная $t \in \mathrm{Mat}_n(\mathbb{K})[t]$ по определению коммутирует со всеми числовыми матрицами, что не выполнено для произвольной матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$.

Для матрицы A рассмотрим подалгебру

$$Z(A) := \{B \in \mathrm{Mat}_n(\mathbb{K}) \mid AB = BA\} \subset \mathrm{Mat}_n(\mathbb{K}),$$

которая называется *централизатором* матрицы A. Несложную проверку того, что для любой матрицы A $Z(A)$ в самом деле является подалгеброй, оставим читателю. Заметим, что $A \in Z(A)$ и, более того, A лежит в *центре* $Z(A)$, то есть коммутирует со всеми элементами $Z(A)$.

Теперь мы хотим показать, что коэффициенты матричных многочленов, участвующих в (75), лежат в $Z(A)$. Во-первых, A коммутирует с E и A. Во-вторых, как и в случае числовых матриц, присоединенная матрица $\widehat{tE - A}$ коммутирует с $tE - A$. Ясно, что элементы матрицы $\widehat{tE - A}$ — многочлены степени не выше $n - 1$, поэтому существует представление $\widehat{tE - A} = B_0 + B_1 t + \ldots + B_{n-1}t^{n-1}$, где $B_i \in \mathrm{Mat}_n(\mathbb{K})$. Тогда

$$(tE - A)(B_0 + B_1 t + \ldots + B_{n-1}t^{n-1}) = (B_0 + B_1 t + \ldots + B_{n-1}t^{n-1})(tE - A),$$

откуда, приравнивая коэффициенты перед одинаковыми степенями t, получаем $AB_0 = B_0A$, $AB_1 = B_1A, \ldots, AB_{n-1} = B_{n-1}A$.

[44] Например, матрица A из $\mathrm{Mat}_n(R)$ обратима тогда и только тогда, когда ее определитель является обратимым элементом кольца R.

Таким образом, коэффициенты матричных многочленов, входящих в (75), действительно содержатся в подалгебре $Z(A) \subset \mathrm{Mat}_n(\mathbb{K})$, то есть (75) можно рассматривать как тождество между многочленами из $Z(A)[t]$. Легко видеть, что подстановка матрицы A вместо t задает гомоморфизм алгебр

$$Z(A)[t] \to Z(A), \quad M(t) \mapsto M(A), \quad \text{где } M(t) = \sum_{i=0}^{k} M_i t^i.$$

Значит, подстановка A вместо t в левую и правую части (75) сохраняет равенство, причем слева она дает нулевую матрицу (поскольку таков первый множитель $AE - A$). Поэтому коэффициент $\chi_A(A)$ перед E в правой части равен нулю (нулевой матрице).

Задача 8.75. *Докажите, что если оператор φ невырожден, то его обратный φ^{-1} является многочленом от φ.*

Ненулевой многочлен минимальной степени со старшим коэффициентом 1, аннулирующий данный оператор φ, называется *минимальным многочленом* оператора φ и обозначается $\mu_\varphi(t)$.

Используя алгоритм Евклида (деления с остатком) легко показать, что $\mu_\varphi(t) \mid \chi_\varphi(t)$ (более точно, минимальный многочлен делит любой аннулирующий).

Заметим, что минимальный многочлен может как совпадать с характеристическим, так и отличаться от него. Например, для тождественного оператора Id_V на n-мерном пространстве V характеристический многочлен равен $(t-1)^n$, в то время как минимальный равен $t-1$. Еще пример: характеристические многочлены нулевого оператора и оператора дифференцирования на пространстве $\mathbb{R}[x]_n$ равны t^{n+1}, в то время как минимальный в первом случае t, а во втором — совпадает с характеристическим.

Последний пример подсказывает, что наличие кратных корней у минимального многочлена — препятствие к диагонализируемости. Это действительно так.

Предложение 8.76. *Оператор φ над алгебраически замкнутым полем $\mathbb{K}$ диагонализируем тогда и только тогда, когда его минимальный многочлен $\mu_\varphi(t)$ не имеет кратных корней.*

Доказательство. Пусть $\mu_\varphi(t) = (t-\lambda)^m g(t)$, где $m > 1$. Тогда существует $v \in V$ такой, что $(\varphi - \lambda \,\mathrm{Id}_V)^2(v) = 0$, но $(\varphi - \lambda \,\mathrm{Id}_V)(v) \neq 0$. Согласно Задаче 8.58 оператор $\varphi - \lambda \mathrm{Id}_V$ тогда не диагонализируем, а значит и φ не диагонализируем.

Обратно, пусть $\mu_\varphi(t) = (t-\lambda_1)\dots(t-\lambda_k)$, где λ_i попарно различны. Имеем

$$V = \mathrm{Ker}\,((\varphi - \lambda_1 \mathrm{Id}_V)\dots(\varphi - \lambda_k \mathrm{Id}_V)).$$

Пусть

$$g_i := \dim \mathrm{Ker}\,(\varphi - \lambda_i \mathrm{Id}_V) = \dim V_i$$

— размерности собственных подпространств.

Полагая $\varphi_i := \varphi - \lambda_i \mathrm{Id}_V$ в обозначениях п. 2) Задачи 7.87, имеем

$$n = \dim V = \dim \mathrm{Ker}(\varphi_k \circ \dots \circ \varphi_1) \leq \dim \mathrm{Ker}(\varphi_1) + \dots + \dim \mathrm{Ker}(\varphi_k) = g_1 + \dots + g_k,$$

откуда (поскольку $V_1 \oplus \dots \oplus V_k \subseteq V$) $n = g_1 + \dots + g_k$ и значит $V = V_1 \oplus \dots \oplus V_k$. ■

Заметим, что если потребовать, чтобы корни $\mu_\varphi(t)$ лежали в $\mathbb{K}$, то результат предыдущей Задачи верен без предположения об алгебраической замкнутости $\mathbb{K}$.

Например, мы знаем, что проекторы — в точности операторы, удовлетворяющие тождеству $\varphi^2 = \varphi$. Если исключить тривиальные случаи $\varphi = 0$ или Id, то легко видеть, что аннулирующий многочлен $t^2 - t = t(t-1)$ является также минимальным. Отсюда с учетом доказанного выше Предложения следует, что проектор диагонализируем (что, впрочем, мы ранее доказали другим способом). То же относится и к операторам отражения, удовлетворяющим тождеству $\varphi^2 = \mathrm{Id}_V$.

Задача 8.77. *Используя предыдущее Предложение докажите, что ограничение диагонализируемого оператора на инвариантное подпространство диагонализируемо.*

Решение. Нам уже известен этот результат из Задачи 8.64. Докажем его другим способом. Так как φ по условию диагонализируем, его минимальный многочлен $\mu_\varphi(t)$ раскладывается на линейные множители над $\mathbb{K}$ и не имеет кратных корней. Пусть $U \subset V$ — произвольное φ-инвариантное подпространство. В силу того, что для любого многочлена $p(t) \in \mathbb{K}[t]$ линейные операторы $p(\varphi)|_U = p(\varphi|U)\colon U \to U$ равны (см. Задачу 8.71), многочлен $\mu_\varphi(t)$ является аннулирующим для $\varphi|_U$ и поэтому $\mu_{\varphi|_U}(t) \mid \mu_\varphi(t)$, а значит тоже не имеет кратных корней. ■

Задача 8.78. *Пусть $\varphi\colon V \to V$ — линейный оператор на конечномерном векторном пространстве V над полем $\mathbb{C}$ такой, что $\varphi^k = \mathrm{Id}_V$ для некоторого натурального k. Докажите, что φ диагонализируем.*

Задача 8.79. *Рассмотрим 4 точки, являющиеся вершинами квадрата; пусть V — пространство вещественнозначных функций на множестве этих точек. Действие группы D_4 симметрий квадрата на множестве его вершин задает ее действие на V.*

a) Разложите пространство V в прямую сумму минимальных инвариантных подпространств группы D_4.

Оператор $\varphi\colon V \to V$ ставит в соответствие функции $f \in V$ функцию $\varphi(f) \in V$, значение которой в произвольной вершине квадрата равно полусумме значений функции f в двух соседних вершинах.

b) Проверьте, что найденные в пункте a) подпространства совпадают с собственными подпространствами оператора φ.

c) Объясните, почему собственные подпространства φ инвариантны относительно преобразований V, индуцированных симметриями квадрата.

Для читателей, немного знакомых с теорией представлений конечных групп, наметим более концептуальный подход к предыдущей задаче. Любое линейное представление конечной группы над полем характеристики 0 является прямой суммой неприводимых. V является прямой суммой инвариантных относительно D_4 подпространств, состоящих из постоянных функций, четных функций (относительно центральной симметрии) с суммой значений, равной нулю и нечетных функций. Им отвечают неприводимые представления группы D_4 размерностей соответственно 1, 1, 2, которые, очевидно, попарно неэквивалентны. Так как оператор φ коммутирует со всеми групповыми операторами (поскольку симметрии квадрата сохраняют соседство вершин), то он определяет эндоморфизм представления V, а поскольку V является прямой суммой попарно неэквивалентных неприводимых представлений, то все прямые слагаемые φ-инвариантны. Далее, чтобы показать, что ограничение φ на каждое неприводимое представление является скалярным оператором, хотелось бы воспользоваться леммой Шура, но ее стандартная формулировка верна над алгебраически замкнутым полем. В данном случае проще всего непосредственно проверить, что ограничение φ на каждое неприводимое представление является скалярным оператором, то есть каждое неприводимое представлене целиком содержится в некотором собственном подпространстве оператора

φ, и только что проведенное вычисление показывает, что перечисленные ранее неприводимые представления отвечают соответственно собственным значениям 1, -1, 0 оператора φ.Таким образом, в данном случае неприводимые компоненты представления D_4 в V совпадают с собственными подпространствами φ. Подробности см. например в [6].

В заключении параграфа рассмотрим следующий вопрос (ниже мы используем язык матриц, хотя можно было бы то же самое изложить на языке операторов). Напомним, что алгебра $\mathrm{Mat}_n(\mathbb{K})$ матриц порядка n как линейное пространство имеет размерность n^2, и для данной матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$ рассмотрим подмножество $L(A) := \{f(A) \mid f(t) \in \mathbb{K}[t]\} \subset \mathrm{Mat}_n(\mathbb{K})$, состоящее из всех матриц, представимых как многочлены от A. Легко видеть, что $L(A)$ — подпространство в $\mathrm{Mat}_n(\mathbb{K})$ и даже (коммутативная) подалгебра. Например, для $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $\mathbb{K} = \mathbb{R}$

$$L(A) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \cong \mathbb{C}$$

Какова размерность $L(A)$ в общем случае?

Задача 8.80. *Докажите, что размерность $L(A)$ равна степени минимальноого многочлена матрицы A. (Указание: используйте наличие алгоритма деления с остатком в $\mathbb{K}[t]$).*

Предыдущая задача показывает, что для любой матрицы A порядка n $\dim L(A) \leq n$.

Задача 8.81. *Покажите, что для $A = \mathrm{diag}\,(\lambda_1, \ldots, \lambda_n)$, где $\lambda_i \neq \lambda_j$ при $i \neq j$, алгебра $L(A)$ совпадает с алгеброй всех диагональных матриц порядка n.*

Задача 8.82. *Чему равна размерность $L(J_n(\lambda))$, где $J_n(\lambda)$ — жорданова клетка порядка n? Опишите алгебру $L(J_n(\lambda))$ как алгебру матриц явно.*

Задача 8.83. *Изоморфны ли алгебры $L(A)$ из двух последних задач?*

8.6 Факторпространство и фактороператор

Пусть V — линейное пространство над полем $\mathbb{K}$, а $U \subset V$ — его подпространство. Рассмотрим на V следующее отношение: $v \sim v' \Leftrightarrow v' - v \in U$. Очевидно, что это — отношение эквивалентности. Класс эквивалентности вектора $v \in V$ обозначим $v+U$. Из определения следует, что $v+U = v'+U \Leftrightarrow v'-v \in U$. Множество классов эквивалентности обозначим V/U.

На множестве V/U определим операции сложения и умножения на элементы поля $\mathbb{K}$ по формулам $(v_1 + U) + (v_2 + U) = (v_1 + v_2) + U$, $\lambda(v + U) = \lambda v + U$ (где $\lambda \in \mathbb{K}$). Непосредственно проверяется, что $(V/U, +, \cdot)$ является линейным пространством над полем $\mathbb{K}$. Оно называется *факторпространством* пространства V по подпространству U и обозначается V/U.

Наглядно элементы V/U можно представлять себе как сдвиги подпространства U на всевозможные векторы из V. Читателю предлагается нарисовать картинку и дать наглядную интерпретацию введенных операций. Например, роль нулевого вектора факторпространства играет само подпространство $U = 0+U$.

Факторпространство задано вместе с линейным отображением $\pi\colon V \to V/U$, $\pi(v) = v + U$, называемым *канонической проекцией*. Ясно, что π сюръективно и $\mathrm{Ker}\,\pi = U$. Применяя известную теорему о сумме размерностей ядра и образа линейного отображения, получаем, что для конечномерного V $\dim(V/U) = \dim V - \dim U$. Кардинал $\dim(V/U)$ называется *коразмерностью* подпространства U в V (обозначение: $\mathrm{codim}_V U$). В математике и ее приложениях важную роль играют случаи подпространств конечной коразмерности в бесконечномерных пространствах (см. Задачи 8.86, 8.88 и Пример 8.87).

Предложение 8.84. *Пусть W — произвольное прямое дополнение к подпространству U в V. Тогда ограничение $\pi|_W : W \to V/U$ — изоморфизм линейных пространств.*

Доказательство. В самом деле, по определению прямого дополнения $\forall v \in V\ \exists!\, u \in U$ и $w \in W$ такие, что $v = u + w$. То есть $\forall v \in V\ \exists!\, w \in W$ такой, что $v + U = w + U$, что влечет биективность $\pi|_W$. ■

Из доказанного Предложения можно легко вывести такое следствие.

Следствие 8.85. *Система $\{e_{k+1} + U, \dots, e_n + U\}$ является базисом в V/U тогда и только тогда, когда векторы $\{e_{k+1}, \dots, e_n\}$ образуют базис в некотором прямом дополнении W к U в V.*

Доказательство: при изоморфизме базис переходит в базис. ■

Задача 8.86. *Пусть f — ненулевая линейная функция на векторном пространстве V (не обязательно конечномерном) над полем $\mathbb{K}$, $U := \ker f$. Докажите, что*

1) $V = U \oplus \langle v \rangle$ для любого $v \notin U$;

2) U — максимальное подпространство в V, т.е. оно не содержится ни в каком другом подпространстве в V отличном от V;

3) $\dim (V/U) = 1$.

Решение. 1) Пусть $v \in V$ — произвольный вектор такой, что $f(v) \neq 0$; пусть $w \in V$ — еще какой-то вектор. Тогда $f(w - \frac{f(w)}{f(v)}v) = 0$, то есть $w - \frac{f(w)}{f(v)}v \in U$. Иными словами, для произвольного $w \in V$ существует $\lambda \in \mathbb{K}$ такое, что $w = u + \lambda v$, где $u \in U$. Поэтому $V = U + \langle v \rangle$. Легко видеть, что последняя сумма прямая.

2) Если $W \subset V$ — такое подпространство, что $U \subsetneq W \subset V$, то из пункта 1) следует, что $W = V$.

3) теперь следует из Предложения 8.84. ■

Пример 8.87. [45] Пусть $C^\infty(S^1)$ — линейное пространство вещественнозначных бесконечно дифференцируемых функций на единичной окружности S^1. В качестве параметра на окружности будем рассматривать угловую координату $\vartheta \in \mathbb{R}$, причем ϑ_1 и ϑ_2 отвечают одной и той же точке окружности $\Leftrightarrow \vartheta_2 - \vartheta_1 \in 2\pi\mathbb{Z}$. Функция f на окружности — то же, что 2π-периодическая функция от ϑ, то есть $f\colon \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{R}$. Примером такой функции является ограничение функции x (абсциссы точки плоскости) на окружность, это дает функцию $\cos\vartheta$ на окружности.

Дифференцируемость функции f на окружности — то же, что дифференцируемость функции f по переменной ϑ. Заметим, что сама ϑ *не является* функцией на окружности: ее значение в точке окружности определено только с точностью до целочисленного кратного 2π. Однако дифференциал $d\vartheta$ корректно определен (причина этого состоит в том, что дифференциал от локально постоянной функции равен нулю). Например, переходя к декартовым координатам (x, y), получим $d\vartheta = \frac{xdy - ydx}{x^2+y^2}$ (это выражение определено во всех точках плоскости с выброшенным началом координат).

Мы будем рассматривать выражения вида $f(\vartheta)d\vartheta$, где $f \in C^\infty(S^1)$. Такие выражения называются "дифференциальными 1-формами". Самое важное их свойство состоит в том, что эти выражения можно интегрировать по окружности. Например, $\int_{S^1} d\vartheta = 2\pi$. Дифференциальные 1-формы образуют бесконечномерное линейное пространство над полем $\mathbb{R}$

$$\Omega^1(S^1) := \{f(\vartheta)d\vartheta \mid f \in C^\infty(S^1)\}$$

(точнее, свободный модуль ранга 1 над кольцом $C^\infty(S^1)$). В пространстве $\Omega^1(S^1)$ содержится подпространство дифференциалов функций на окружности $dF(\vartheta) = F'(\vartheta)d\vartheta$, $F \in C^\infty(S^1)$. Дифференциальные

[45] Этот пример заметно сложнее остальных, но мы его включили из-за его важности для ряда математических и физических теорий.

формы, являющиеся дифференциалами функций, называются “точными 1-формами”. Ясно, например, что $d\vartheta$ не является дифференциалом функции (окружность — компакт, поэтому для любой дифференцируемой функции на окружности найдется точка, в которой ее дифференциал равен нулю, в то время как $d\vartheta$ не равна нулю во всех точках окружности). Как понять, является ли дифференциальная 1-форма $f(\vartheta)d\vartheta$ дифференциалом функции или нет?

Рассмотрим линейную функцию

$$\int_{S^1} : \Omega^1(S^1) \to \mathbb{R}, \quad f(\vartheta)d\vartheta \mapsto \int_{S^1} f(\vartheta)d\vartheta.$$

Из формулы Ньютона-Лейбница следует, что если $f(\vartheta)d\vartheta = F'(\vartheta)d\vartheta$, то интеграл от нее по окружности равен нулю. Обратно, если $\int_{S^1} f(\vartheta)d\vartheta = 0$, рассмотрим выражение $F(\vartheta) := \int_0^\vartheta f(t)dt$ как функцию от ϑ. Из предположения следует, что она является 2π-периодической, то есть является функцией на окружности, и $dF(\vartheta) = f(\vartheta)d\vartheta$. Как мы уже видели, $\int_{S^1} d\vartheta = 2\pi$, что еще раз свидетельствует о том, что 1-форма $d\vartheta$ не является точной (т.е. дифференциалом функции). Таким образом, точные формы образуют ядро линейной функции $\int_{S^1}$. Мы получаем, что для окружности факторпространство дифференциальных 1-форм по подпространству точных 1-форм является одномерным. В качестве базиса в нем можно выбрать класс формы $d\vartheta$ (или любой другой формы с ненулевым интегралом). В частности, для любой 1-формы $f(\vartheta)d\vartheta$ существует единственное $\lambda \in \mathbb{R}$ (а именно $\lambda = \frac{1}{2\pi}\int_{S^1} f(\vartheta)d\vartheta$) такое, что $f(\vartheta)d\vartheta - \lambda d\vartheta = dF(\vartheta)$, где $F \in C^\infty(S^1)$. Это факторпространство называется *группой одномерных когомологий Де Рама окружности*. То, что оно ненулевое, отражает тот факт, что окружность имеет нетривиальную топологию — не стягиваема по себе в точку (в отличие, например, от интервала прямой).

Задача 8.88. *Пусть $V := \mathbb{R}[t]$ — линейное пространство многочленов над полем $\mathbb{R}$.*

a) Зададим подпространство

$$U := \{p(t) \in \mathbb{R}[t] \mid p(0) = p'(0) = p''(0) = \ldots = p^{(k-1)}(0) = 0\} \subset V.$$

Найдите размерность факторпространства V/U и какой-нибудь базис в нем.

b) Тот же вопрос, что и в предыдущем пункте, для подпространства

$$W = \{p(t) \in \mathbb{R}[t] \mid p(\alpha_1) = p(\alpha_2) = \ldots = p(\alpha_n) = 0\} \subset V,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — набор попарно различных точек из $\mathbb{R}$.

Задача 8.89. *Последовательность*

$$K: \quad 0 \xrightarrow{d_0} V_1 \xrightarrow{d_1} V_2 \xrightarrow{d_2} \ldots \xrightarrow{d_{n-1}} V_n \xrightarrow{d_n} 0$$

конечномерных линейных пространств и линейных отображений называется компле́ксом, если композиция любых двух соседних отображений в нем равна нулю, $d_{i+1} \circ d_i = 0$. Факторпространство $H^i(K) := \operatorname{Ker} d_i / \operatorname{Im} d_{i-1}$ называется i-м пространством когомологий этого комплекса. Число

$$\chi(K) := \sum_{i=1}^{n} (-1)^i \dim V_i$$

называется эйлеровой характеристикой этого комплекса. Докажите, что

$$\chi(K) = \sum_{i=1}^{n} (-1)^i \dim H^i(K).$$

Задача 8.90. *Докажите следующий аналог формулы Грассмана:*

$$\operatorname{codim}_V (U+W) + \operatorname{codim}_V (U\cap W) = \operatorname{codim}_V U + \operatorname{codim}_V W,$$

где U и W — подпространства конечной коразмерности не обязательно конечномерного линейного пространства V.

Решение задачи разобьем на три шага.

1) Рассмотрим отображение $\varphi\colon V \to (V/U)\oplus(V/W)$, заданное формулой $\varphi(v) = (v+U,\, v+W)$. Ясно, что оно линейно. Покажем, что $\operatorname{Ker}\varphi = U\cap W$. В самом деле, $(v+U,\, v+W) = (0+U,\, 0+W) \Leftrightarrow v\in U\cap W$. Значит, корректно определено линейное отображение

$$i\colon V/(U\cap W) \to (V/U)\oplus(V/W), \quad i(v+(U\cap W)) = (v+U, v+W),$$

которое к тому же инъективно.

2) Рассмотрим сюръективное линейное отображение

$$\pi\colon (V/U)\oplus(V/W) \to V/(U+W), \quad \pi(v_1+U,\, v_2+W) = v_1 - v_2 + (U+W).$$

Нетрудно поверить, что $\operatorname{Ker}\pi = \operatorname{Im} i$.

3) Теперь требуемое равенство $\dim((V/U)\oplus(V/W)) = \dim V/(U+W) + \dim V/(U\cap W)$ следует из такого легко проверяемого утверждения: пусть дана последовательность $L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ конечномерных линейных пространств и линейных отображений такая, что φ инъективно, ψ сюръективно и $\operatorname{Im}\varphi = \operatorname{Ker}\psi$, то $\dim M = \dim L + \dim N$. ■

Перейдем теперь к определению фактороператора.

Пусть $\varphi\colon V\to V$ — линейный оператор, $U\subset V$ — φ-инвариантное подпространство. Фактороператором $\overline{\varphi} = \overline{\varphi}_{V/U}\colon V/U \to V/U$ называется линейный оператор, определенный формулой $\overline{\varphi}(v+U) = \varphi(v)+U \ \ \forall v\in V$.

Проверим корректность определения: если $v+U = v'+U$, то

$$\overline{\varphi}(v+U) = \varphi(v)+U = \varphi(v')+U = \overline{\varphi}(v'+U),$$

поскольку $\varphi(v')-\varphi(v) = \varphi(v'-v)\in U$ в силу φ-инвариантности U.

Проверка линейности:

$$\overline{\varphi}((v_1+U)+(v_2+U)) = \overline{\varphi}((v_1+v_2)+U) = \varphi(v_1+v_2)+U =$$

$$(\varphi(v_1)+\varphi(v_2))+U = (\varphi(v_1)+U)+(\varphi(v_2)+U) = \overline{\varphi}(v_1+U)+\overline{\varphi}(v_2+U),$$

аналогично проверяется $\overline{\varphi}(\lambda(v+U)) = \lambda\overline{\varphi}(v+U)$.

Задача 8.91. $\overline{\mathrm{Id}_V} = \mathrm{Id}_{V/U}$. *Если $\psi\colon V\to V$ — еще один оператор, для которого подпространство $U\subset V$ ψ-инвариантно, то $\overline{\psi\varphi} = \overline{\psi}\,\overline{\varphi}$.*

Мы знаем, что если $\{e_1,\dots,e_n\}$ — базис в V, первые k элементов $\{e_1,\dots,e_k\}$ которого образуют базис в φ-инвариантном подпространстве U, то φ имеет в нем матрицу вида

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix},$$

в которой блок B является матрицей ограничения $\varphi|_U$ в базисе $\{e_1,\dots,e_k\}$.

Задача 8.92. *Докажите, что блок D является матрицей $\overline{\varphi}$ в базисе $\{e_{k+1}+U,\dots,e_n+U\}$ факторпространства V/U.*

Используя предыдущую задачу, легко построить пример линейного оператора, имеющего инвариантное подпространство такое, что ограничение на него и фактороператор нулевые, а сам оператор — нет.

Из предыдущей задачи также следует, что

$$\chi_\varphi(t)=\chi_{\varphi|_U}(t)\chi_{\overline{\varphi}_{V/U}}(t). \tag{76}$$

Предположим теперь, что к φ-инвариантному подпространству U мы в V смогли найти φ-инвариантное прямое дополнение W (мы знаем, что такое прямое дополнение не всегда существует). Тогда имеет место следующее утверждение.

Предложение 8.93. *Диаграмма*

$$\begin{array}{ccc} W & \xrightarrow{\varphi|_W} & W \\ {\scriptstyle \pi|_W}\downarrow\cong & & \cong\downarrow{\scriptstyle \pi|_W} \\ V/U & \xrightarrow{\overline{\varphi}_{V/U}} & V/U \end{array}$$

коммутативна, то есть $\overline{\varphi}_{V/U}\circ\pi|_W=\pi|_W\circ\varphi|_W$.

Доказательство. Имеем

$$(\overline{\varphi}_{V/U}\circ\pi|_W)(w)=\overline{\varphi}_{V/U}(w+U)=\varphi(w)+U,$$
$$(\pi|_W\circ\varphi|_W)(w)=\pi|_W(\varphi(w))=\varphi(w)+U. \quad \blacksquare$$

Доказанное предложение показывает, что при отождествлении факторпространства V/U с W посредством изоморфизма $\pi|_W$ действие оператора $\overline{\varphi}_{V/U}$ на V/U отождествляется с действием ограничения $\varphi|_W$ на W.

В качестве примера использования понятия фактороператора докажем с помощью него теорему Гамильтона-Кэли.

Лемма 8.94. Пусть $\varphi,\psi\colon V\to V$ — линейные операторы, для которых подпространство $U\subset V$ инвариантно. Тогда

1) $\overline{\varphi+\psi}=\overline{\varphi}+\overline{\psi}$;
2) $\overline{\lambda\varphi}=\lambda\overline{\varphi}$;
3) $\overline{\varphi}^m=\overline{\varphi^m}$ для $m\in\mathbb{N}$.

Доказательство. 1)

$$(\overline{\varphi+\psi})(v+U)=(\varphi+\psi)(v)+U=(\varphi(v)+\psi(v))+U=$$
$$=(\varphi(v)+U)+(\psi(v)+U)=\overline{\varphi}(v+U)+\overline{\psi}(v+U)=(\overline{\varphi}+\overline{\psi})(v+U).$$

2)

$$\overline{\lambda\varphi}(v+U)=(\lambda\varphi)(v)+U=\lambda\varphi(v)+U=\lambda(\varphi(v)+U)=\lambda\overline{\varphi}(v+U).$$

3) Индукция по m. Случай $m=1$ очевиден, пусть $m>2$ и пусть результат верен для $m-1$. Имеем

$$\overline{\varphi^m}(v+U)=\varphi^m(v)+U=\varphi(\varphi^{m-1}(v))+U=\overline{\varphi}(\varphi^{m-1}(v)+U)=$$
$$\overline{\varphi}(\overline{\varphi^{m-1}}(v+U))=(\overline{\varphi}\,\overline{\varphi^{m-1}})(v+U)=(\overline{\varphi}\,\overline{\varphi}^{m-1})(v+U)=(\overline{\varphi}^m)(v+U). \quad \blacksquare$$

Пусть $p(t)\in\mathbb{K}[t]$ — произвольный многочлен. Тогда если подпространство U является φ-инвариантным, то оно и $p(\varphi)$-инвариантно, и значит на V/U определены операторы $p(\overline{\varphi})$ и $\overline{p(\varphi)}$.

Лемма 8.95. $p(\overline{\varphi}) = \overline{p(\varphi)}$.

Доказательство. Пусть $p(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$. Тогда используя предыдущую лемму, имеем

$$\overline{p(\varphi)} = \overline{a_n\varphi^n + a_{n-1}\varphi^{n-1} + \ldots + a_1\varphi + a_0\mathrm{Id}_V} = \overline{a_n\varphi^n} + \overline{a_{n-1}\varphi^{n-1}} + \ldots + \overline{a_1\varphi} + \overline{a_0\mathrm{Id}_V} =$$

$$= a_n\overline{\varphi^n} + a_{n-1}\overline{\varphi^{n-1}} + \ldots + a_1\overline{\varphi} + a_0\overline{\mathrm{Id}_V} = a_n\overline{\varphi}^n + a_{n-1}\overline{\varphi}^{n-1} + \ldots + a_1\overline{\varphi} + a_0\mathrm{Id}_{V/U} = p(\overline{\varphi}). \quad \blacksquare$$

Теорема 8.96. *(Гамильтон-Кэли) (см. Теорему 8.72) Пусть V — конечномерное пространство над алгебраически замкнутым полем $\mathbb{K}$, $\varphi\colon V \to V$ — линейный оператор. Тогда его характеристический многочлен $\chi_\varphi(t)$ аннулирует φ, то есть $\chi_\varphi(\varphi)$ — нулевой оператор.*

Доказательство. Проведем доказательство индукцией по $n = \dim V$. Если $n = 1$, то $\varphi = \lambda\mathrm{Id}_V$ для некоторого скаляра $\lambda \in \mathbb{K}$, $\chi_\varphi(t) = t - \lambda$ и $\varphi - \lambda\mathrm{Id}_V = 0$. Пусть $n > 1$. Так как поле $\mathbb{K}$ алгебраически замкнуто, то у φ есть собственный вектор e с некоторым собственным значением λ. Положим $U := \langle e\rangle \subset V$. Тогда U — одномерное φ-инвариантное подпространство, $\chi_{\varphi|_U}(t) = t - \lambda$. Пусть $\overline{\varphi} = \overline{\varphi}_{V/U}$ — соответствующий фактороператор. Тогда $\chi_\varphi(t) = \chi_{\varphi|_U}(t)\chi_{\overline{\varphi}_{V/U}}(t)$ (см. (76)).

Так как $\dim V/U = n - 1$, работает предположение индукции, и мы имеем $\chi_{\overline{\varphi}_{V/U}}(\overline{\varphi}_{V/U}) = 0$ как оператор на V/U. По предыдущей лемме $\chi_{\overline{\varphi}_{V/U}}(\overline{\varphi}_{V/U}) = \overline{\chi_{\overline{\varphi}_{V/U}}(\varphi)}_{V/U}$ и значит

$$0 + U = \chi_{\overline{\varphi}_{V/U}}(\overline{\varphi}_{V/U})(v + U) =$$

$$= \overline{\chi_{\overline{\varphi}_{V/U}}(\varphi)}(v + U) = \chi_{\overline{\varphi}_{V/U}}(\varphi)(v) + U,$$

откуда $\chi_{\overline{\varphi}_{V/U}}(\varphi)(v) \in U \ \ \forall\, v \in V$. Так как $\chi_{\varphi|_U}(\varphi) = \varphi - \lambda\mathrm{Id}_V$ — нулевой оператор на U, то композиция $\chi_{\varphi|_U}(\varphi) \circ \chi_{\overline{\varphi}_{V/U}}(\varphi)$ — нулевой оператор на всем V (поскольку образ $\chi_{\overline{\varphi}_{V/U}}(\varphi)$ содержится в ядре $\chi_{\varphi|_U}(\varphi)$), а это согласно (76) есть $\chi_\varphi(\varphi)$. Тем самым шаг индукции доказан. $\blacksquare$

Задача 8.97. *Докажите, что фактороператор $\overline{\varphi}\colon V/U \to V/U$ диагонализируемого оператора φ диагонализируем.*

Решение. Согласно Задаче 8.65, для φ-инвариантного подпространства $U \subset V$ в V есть φ-инвариантное прямое дополнение W. Согласно Задаче 8.64, ограничение $\varphi|_W$ диагонализируемо, а тогда из Предложения 8.93 легко выводится, что диагонализируем и $\overline{\varphi}$.

Другое решение можно получить, используя Предложение 8.76 (ср. Задачу 8.77). Если φ диагонализируем, то его минимальный многочлен $\mu_\varphi(t)$ раскладывается на линейные множители над $\mathbb{K}$ и не имеет кратных корней. Так как по Лемме 8.95 $\mu_\varphi(\overline{\varphi}) = \overline{\mu_\varphi(\varphi)} = 0$ (как операторы $V/U \to V/U$), то $\mu_{\overline{\varphi}}(t)$ делит $\mu_\varphi(t)$, а значит тоже не имеет кратных корней. $\blacksquare$

Задача 8.98. *Докажите, что если два оператора на конечномерном пространстве над полем $\mathbb{C}$ коммутируют, то для них существует общий базис, в котором их матрицы верхние треугольные.*

9 Жорданова нормальная форма

Ни один курс линейной алгебры не может считаться сколько-нибудь полным без классификации всех линейных операторов на конечномерных пространствах хотя бы в простейшем случае алгебраически замкнутого поля.

Мы видели, что препятствия к диагонализируемости операторов над полем $\mathbb{K}$ бывают двух видов: во-первых, корни характеристического многочлена могут не принадлежать полю $\mathbb{K}$, во-вторых, даже если

корень лежит в $\mathbb{K}$, его геометрическая кратность может оказаться строго меньше алгебраической. В первом случае проблема недиагонализируемости решается переходом к расширению поля $\mathbb{K}$, содержащему все корни характеристического многочлена, в случае же препятствий второго типа оператор останется недиагонализируемым даже после расширения поля.

Так как не все линейные операторы диагонализируемы, нужно определить "простейший вид" матриц линейных операторов более общий чем диагональный. Диагональный вид возникает тогда, когда все пространство представляется в виде прямой суммы инвариантных одномерных (порожденных собственными векторами) подпространств. В общем случае одномерные инвариантные подпространства нужно заменить более общими, отвечающими так называемым жордановым цепочкам, причем жорданова цепочка длины 1 состоит из одного собственного вектора.

Более подробно, рассмотрим оператор $\varphi\colon V \to V$ на конечномерном пространстве V, и пусть λ — его собственное значение. Рассмотрим оператор $\psi := \varphi - \lambda\,\mathrm{Id}_V$ и пусть $0 \neq e \in V$ — такой вектор, что для некоторого $m \geq 1$ $\psi^m(e) = 0$, но $\psi^{m-1}(e) \neq 0$ (например, собственный вектор φ с собственным значением λ удовлетворяет этому условию при $m = 1$). Тогда легко проверяется, что система векторов $\{\psi^{m-1}(e), \dots, \psi(e), e\}$ линейно независима (см. доказательство Леммы 9.5 ниже) и ее линейная оболочка $\langle\psi^{m-1}(e), \dots, \psi(e), e\rangle$ φ-инвариантна. Система векторов $\{\psi^{m-1}(e), \dots, \psi(e), e\}$ и называется *жордановой цепочкой* для оператора φ, отвечающей собственному значению λ, так как применение оператора $\psi = \varphi - \lambda\mathrm{Id}_V$ сдвигает векторы цепочки на одну позицию влево, при этом переводя $\psi^{m-1}(e)$ в 0[46]. Матрица ограничения φ на $\langle\psi^{m-1}(e), \dots, \psi(e), e\rangle$ в базисе $\{\psi^{m-1}(e), \dots, \psi(e), e\}$ имеет вид

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$$

и называется *жордановой клеткой* порядка m с собственным значением λ.

Далее мы докажем, что если характеристический многочлен оператора φ раскладывается на линейные множители над полем $\mathbb{K}$, то в V существует базис, состоящий из жордановых цепочек оператора φ (отвечающих разным его собственным значениям). Такой базис называется *жордановым базисом* для оператора φ. В этом базисе матрица φ имеет блочно-диагональный вид, с жордановыми клетками в качестве блоков. Такая матрица и называется *жордановой нормальной формой* (кратко ЖНФ) оператора φ. Заметим, что диагональный вид является частным случаем ЖНФ, а именно когда все жордановы клетки имеют порядок 1 (соответственно все жордановы цепочки имеют длину 1 и, значит, состоят из собственных векторов). Более того, ЖНФ данного оператора определена однозначно с точностью до перестановки клеток в блочно-диагональном виде. То есть число клеток данного порядка с собственным значением λ в ЖНФ φ не зависит от выбора жорданова базиса.

Подобно тому, как собственные векторы, отвечающие одному собственному значению λ, порождают соответствующее собственное подпространство, жордановы цепочки, отвечающие конкретному собственному значению λ, порождают так называемое корневое подпространство. Причем все пространство, на котором действует оператор, при условии, что его характеристический многочлен раскладывается над полем $\mathbb{K}$ на линейные множители, всегда является суммой корневых подпространств (хотя, как мы знаем, не всегда является суммой собственных).

[46] таким образом, система $\{\psi^{m-1}(e), \dots, \psi(e), e\}$ также будет жордановой цепочкой для оператора ψ, отвечающей собственному значению 0.

Заметим, что в данном тексте мы не планируем излагать алгоритм практического нахождения жорданова базиса, который подробно изложен в решебнике [12].

9.1 Корневые подпространства

Пусть V — векторное пространство над полем $\mathbb{K}$.

Определение 9.1. Вектор e называется *корневым вектором* оператора φ, отвечающим скаляру $\lambda \in \mathbb{K}$, если существует такое натуральное N, что $(\varphi - \lambda \operatorname{Id}_V)^N e = 0$. Наименьшее из таких N называется *высотой* корневого вектора e и обозначается $\operatorname{ht} e$.

Очевидно, что корневые векторы высоты 1 — в точности собственные векторы. Удобно считать нулевой вектор корневым вектором высоты 0 (отвечающим любому $\lambda \in \mathbb{K}$).

Пример 9.2. Для оператора дифференцирования на пространстве $V = C^\infty(\mathbb{R})$ бесконечно дифференцируемых функций собственные векторы с собственным значением λ — это ненулевые функции, пропорциональные $e^{\lambda x}$, а корневые векторы — это функции вида $p(x)e^{\lambda x}$, где $p(x)$ — многочлен. При этом высота такого корневого вектора равна $\deg p + 1$. В частности, корневые векторы, отвечающие $\lambda = 0$ — суть в точности многочлены.

Легко проверить, что множество всех корневых векторов, отвечающих данному λ, образуют подпространство $V^\lambda \subset V$, называемое *корневым подпространством* оператора φ, отвечающим λ. Если e — корневой вектор высоты $m > 0$, отвечающий λ, то $(\varphi - \lambda \operatorname{Id}_V)e$ — корневой вектор высоты $m-1$, отвечающий тому же λ. Отсюда следует, что корневое подпространство V^λ инвариантно относительно $(\varphi - \lambda \operatorname{Id}_V)$, а значит, и относительно φ. (Последнее можно доказать даже проще: если $(\varphi - \lambda \operatorname{Id}_V)^N e = 0$, то, так как $\varphi - \lambda \operatorname{Id}_V$ и φ коммутируют, то и $(\varphi - \lambda \operatorname{Id}_V)^N(\varphi(e)) = 0$).

Заметим, что если e — корневой вектор оператора φ высоты $\operatorname{ht} e = m > 0$, отвечающий λ, то $(\varphi - \lambda \operatorname{Id}_V)^{m-1} e$ — собственный вектор φ с собственным значением λ. Таким образом, ненулевые корневые подпространства отвечают тем скалярам, которые являются собственными значениями, и в этом случае $V_\lambda \subseteq V^\lambda$.

Напомним, что оператор $\varphi\colon V \to V$ называется *нильпотентным*, если существует натуральное N такое, что $\varphi^N = 0$. Наименьшее среди таких N называется *высотой* оператора φ и обозначается $\operatorname{ht} \varphi$. Например, для оператора $\varphi = \frac{d}{dx}\colon \mathbb{R}[x]_n \to \mathbb{R}[x]_n$ его высота $\operatorname{ht}\left(\frac{d}{dx}\right) = \dim \mathbb{R}[x]_n = n+1$.

Далее мы по умолчанию считаем пространство V конечномерным.

Лемма 9.3. Пусть $\varphi\colon V \to V$ — нильпотентный оператор, $\dim V = n$. Тогда $\chi_\varphi(t) = t^n$.

Доказательство легко следует из Задачи 8.70. Приведем также немного другое рассуждение. Пусть $\operatorname{ht} \varphi = m$. Тогда имеем цепочку вложенных подпространств

$$0 \subsetneq \operatorname{Ker} \varphi \subsetneq \operatorname{Ker} \varphi^2 \subsetneq \ldots \subsetneq \operatorname{Ker} \varphi^{m-1} \subsetneq \operatorname{Ker} \varphi^m = V. \tag{77}$$

(В самом деле, если для некоторого $0 \leq k \leq m-1$ имеет место равенство $\operatorname{Ker} \varphi^k = \operatorname{Ker} \varphi^{k+1}$, то $\operatorname{Ker} \varphi^{k+1} = \operatorname{Ker} \varphi^{k+2} = \ldots$, что при $\operatorname{Ker} \varphi^k \neq V$ противоречит нильпотентности φ, а при $\operatorname{Ker} \varphi^k = V$ — определению высоты нильпотентного оператора). Выберем согласованный с этой цепочкой базис в V. Другими словами, выберем базис в $\operatorname{Ker} \varphi$, затем дополним его до базиса в $\operatorname{Ker} \varphi^2$ и т.д. В таком базисе матрица φ будет верхнетреугольной с нулями на главной диагонали. Отсюда следует требуемое. ■

Поскольку длина цепочки подпространств (77) не превосходит $\dim V + 1$, для нильпотентного оператора φ его высота $\operatorname{ht} \varphi \leq \dim V$ (причем все значения высоты от 1 до $\dim V$ возможны — читателю предлагается привести примеры соответствующих нильпотентных матриц).

Пусть $V^\lambda \neq 0$ — корневое подпространство оператора φ, отвечающее его собственному значению λ.

Лемма 9.4. Оператор $(\varphi - \lambda \operatorname{Id}_V)|_{V^\lambda}$ нильпотентен.

Доказательство. По определению корневого подпространства все векторы из V^λ имеют конечную высоту. Поскольку V^λ конечномерно (будучи подпространством конечномерного пространства), высота оператора $(\varphi - \lambda \operatorname{Id}_V)|_{V^\lambda}$ равна максимуму высот векторов произвольного базиса в V^λ. ■

Для нильпотентного оператора $(\varphi - \lambda \operatorname{Id}_V)|_{V^\lambda}$ существует базис в V^λ, в котором он имеет верхнюю треугольную матрицу с нулями на главной диагонали, а значит $\varphi|_{V^\lambda}$ в том же базисе имеет верхнюю треугольную матрицу с λ на главной диагонали. Поэтому если $d := \dim V^\lambda$, то $\chi_{\varphi|_{V^\lambda}}(t) = (t-\lambda)^d$; в частности, согласно Предложению 8.51, $d \leq m$, где m — кратность корня λ характеристического многочлена φ (вскоре мы покажем, что на самом деле $d = m$). Если $\mu \neq \lambda$, то оператор $(\varphi - \mu \operatorname{Id}_V)|_{V^\lambda}$ невырожден, так как в некотором базисе он имеет верхнюю треугольную матрицу с $\lambda - \mu \neq 0$ на главной диагонали.

Лемма 9.5. Пусть m — кратность корня λ многочлена $\chi_\varphi(t)$. Тогда $V^\lambda = \operatorname{Ker}((\varphi - \lambda \operatorname{Id}_V)^m)$.[47]

Доказательство. Из определения V^λ следует, что $\operatorname{Ker}((\varphi - \lambda \operatorname{Id}_V)^m) \subset V^\lambda$. Обратное включение следует из того, что, как было отмечено выше, высота нильпотентного оператора $(\varphi - \lambda \operatorname{Id}_V)|_{V^\lambda} \colon V^\lambda \to V^\lambda$ не превосходит $d = \dim V^\lambda$, причем как мы уже знаем $d \leq m$.

Второе доказательство. Покажем, что высота любого вектора $e \in V^\lambda$ не превосходит m, откуда, очевидно, следует требуемое. Предположим противное: пусть существует $e \in V^\lambda$ такой, что $\operatorname{ht} e = N > m$. Пусть для краткости ψ обозначает оператор $(\varphi - \lambda \operatorname{Id}_V)$. Тогда векторы $\{e, \psi(e), \ldots, \psi^{N-1}(e)\}$ линейно независимы. Действительно, если

$$\lambda_0 e + \lambda_1 \psi(e) + \ldots + \lambda_{N-1}\psi^{N-1}(e) = 0$$

— произвольная линейная зависимость, то, применяя к ней ψ^{N-1} и используя $\psi^N(e) = 0$, получим $\lambda_0 = 0$; с учетом этого, применяя к исходной зависимости ψ^{N-2}, получим $\lambda_1 = 0$ и т.д.

Очевидно, что $\langle e, \psi(e), \ldots, \psi^{N-1}(e)\rangle \subset V^\lambda$, откуда $\dim V^\lambda \geq N > m$, что противоречит тому, что m — максимальная степень множителя $(t-\lambda)$, на которую делится $\chi_\varphi(t)$. ■

Пусть $\chi_\varphi(t) = (t-\lambda_1)^{m_1} \ldots (t-\lambda_s)^{m_s}$, где λ_i попарно различны, причем все $\lambda_i \in \mathbb{K}$. Обозначим для краткости $\psi_i := (\varphi - \lambda_i \operatorname{Id}_V)^{m_i}$. Операторы ψ_i, $i = 1, \ldots, s$ попарно коммутируют, и по Теореме Гамильтона-Кэли $V = \operatorname{Ker}(\psi_1 \ldots \psi_s)$. Кроме того, по предыдущей Лемме $V^{\lambda_i} = \operatorname{Ker}\psi_i$. Отсюда, в частности, следует, что подпространство $V^{\lambda_i} \subset V$ инвариантно для всех ψ_j (см. Предложение 8.12). Мы также знаем (см. предшествующий Лемме 9.5 абзац), что $\psi_j|_{V^{\lambda_i}}$ — изоморфизм при $j \neq i$.

Предложение 9.6. *Корневые подпространства, отвечающие разным собственным значениям, линейно независимы.*

Доказательство. Пусть $V^{\lambda_1}, \ldots, V^{\lambda_k}$ — набор корневых подпространств оператора φ, отвечающих разным собственным значениям $\lambda_1, \ldots, \lambda_k$. Воспользуемся индукцией по k. При $k = 1$ требуемое утверждение очевидно; предположим что $k > 1$. Пусть $v_1 + \ldots + v_{k-1} + v_k = 0$, где $v_i \in V^{\lambda_i}$. Применяя к линейной зависимости ψ_k, получим $\psi_k(v_1) + \ldots + \psi_k(v_{k-1}) = 0$, причем $\psi_k(v_i) \in V^{\lambda_i}$. По предположению индукции $\psi_k(v_i) = 0$, $i = 1, \ldots, k-1$. Но так как $\psi_k|_{V^{\lambda_i}}$ — изоморфизм при $i \neq k$, то и сами $v_i = 0$ при $i = 1, \ldots, k-1$, а значит и $v_k = 0$. ■

Предложение 9.7. *Предположим, что характеристический многочлен оператора φ раскладывается на линейные множители над полем $\mathbb{K}$. Тогда V является прямой суммой корневых подпространств.*

[47] На всякий случай отметим, что кратность корня m — не обязательно наименьшее среди натуральных чисел, удовлетворяющих условию Леммы.

Доказательство. Будем использовать введенные выше обозначения. Пусть $v \in V = \operatorname{Ker}(\psi_s \dots \psi_1)$ — произвольный вектор. Тогда $(\psi_{s-1} \dots \psi_1)(v) \in \operatorname{Ker} \psi_s = V^{\lambda_s}$, причем $(\psi_{s-1} \dots \psi_1)|_{V^{\lambda_s}}$ — композиция изоморфизмов и значит тоже изоморфизм. Поэтому существует (единственный!) $v_s \in V^{\lambda_s}$ такой, что $(\psi_{s-1} \dots \psi_1)(v) = (\psi_{s-1} \dots \psi_1)(v_s)$. Тогда $(\psi_{s-1} \dots \psi_1)(v - v_s) = 0$, откуда $(\psi_{s-2} \dots \psi_1)(v - v_s) \in \operatorname{Ker} \psi_{s-1}$. Так как $(\psi_{s-2} \dots \psi_1)|_{V^{\lambda_{s-1}}}$ — изоморфизм, то найдется (снова единственный) $v_{s-1} \in V^{\lambda_{s-1}}$ такой, что $(\psi_{s-2} \dots \psi_1)(v - v_s) = (\psi_{s-2} \dots \psi_1)(v_{s-1})$. Тогда $(\psi_{s-3} \dots \psi_1)(v - v_s - v_{s-1}) \in V^{\lambda_{s-2}}$. Продолжая в том же духе, в конце концов мы придем к $\psi_1(v - v_s - \dots - v_3 - v_2) = 0$, где $v_i \in V^{\lambda_i}$, откуда $v = v_1 + \dots + v_s$ для некоторого $v_1 \in V^{\lambda_1}$. Значит, $V = V^{\lambda_1} + \dots + V^{\lambda_s}$, а из предыдущего Предложения мы знаем, что сумма справа — прямая.[48]

По-другому доказать Предложение можно с помощью Задачи 7.87 (ср. также Предложение 8.76). ■

Следствие 9.8. $\dim V^{\lambda_i} = m_i$, *где* m_i — *кратность корня* λ_i *многочлена* $\chi_\varphi(t)$.

Доказательство. Для $i = 1, \dots, s$ имеем $\dim V^{\lambda_i} \le m_i$, но $\sum_{i=1}^s \dim V^{\lambda_i} = n = \sum_{i=1}^s m_i$. ■

Таким образом, в случае, когда характеристический многочлен оператора φ раскладывается на линейные множители над полем $\mathbb{K}$ (что, в частности, всегда верно для $\mathbb{K} = \mathbb{C}$), все пространство представляется в виде прямой суммы корневых подпространств, $V = V^{\lambda_1} \oplus \dots \oplus V^{\lambda_s}$, которые φ-инвариантны. Заметим, что корневое подпространство V^λ совпадает с собственным V_λ тогда и только тогда, когда геометрическая кратность собственного значения λ равна его алгебраической кратности, в случае же строгого неравенства имеет место строгое включение $V_\lambda \subsetneq V^\lambda$ (рекомендуем читателю еще раз вернуться к Теореме 8.56; теперь должно быть ясно, что условие 1) в ней обеспечивает разложимость пространства в сумму корневых, а условие 2) — что корневые совпадают с собственными). Заметим еще, что в последнем случае ограничение φ на V^λ не диагонализируемо (а значит, согласно Задаче 8.64, и сам оператор φ не диагонализируем).

Из инвариантности корневых подпространств следует, что в базисе пространства V, полученном объединением базисов всех корневых подпространств, матрица оператора φ будет иметь блочно-диагональный вид, блоки которого являются матрицами ограничения φ на корневые подпространства V^{λ_i}. Поэтому для исследования оператора достаточно изучить его ограничение на одно корневое подпространство.

Итак, пусть $\varphi\colon V \to V$ — линейный оператор, для которого $V = V^\lambda$ — корневое (под)пространство, отвечающее некоторому скаляру $\lambda \in \mathbb{K}$. Тогда $\psi := \varphi - \lambda \operatorname{Id}_V\colon V \to V$ — нильпотентный оператор. Если A — матрица ψ в некотором базисе пространства V, то матрицей φ в том же базисе будет $A + \lambda E$. Поэтому задача свелась к изучению нильпотентного оператора.

9.2 Случай нильпотентного оператора

Пусть V — n-мерное векторное пространство. Примером нильпотентного оператора φ на V является оператор, который в некотором базисе $\{e_1, \dots, e_n\}$ действует, сдвигая его векторы влево и переводя e_1 в 0, то есть $\varphi(e_i) = e_{i-1}$ при $i \ge 2$ и $\varphi(e_1) = 0$. Например, так задается действие оператора $\frac{d}{dx}$ на пространстве $V = \mathbb{R}[x]_{n-1}$ в базисе $\{1, \frac{x}{1!}, \frac{x^2}{2!}, \dots, \frac{x^{n-1}}{(n-1)!}\}$. Напомним, что такая система векторов называется жордановой цепочкой. Читателю предлагается написать соответствующую матрицу; она называется *нильпотентной жордановой клеткой* (или жордановой клеткой с собственным значением 0) *порядка* n.

Задача 9.9. *Найдите минимальный и характеристический многочлены нильпотентной жордановой клетки порядка* n.

[48] На самом деле анализ приведенного доказательства показывает, что в нем мы еще раз доказали, что указанная сумма прямая, поскольку выбор v_s, $v_{s-1}, \dots, v_1$ на каждом шаге единственен.

Заметим, что не для любого нильпотентного оператора существует базис, состоящий из одной жордановой цепочки (эквивалентно, не для всякого нильпотентного оператора существует вектор $e \in V$, $\operatorname{ht} e = \dim V$): сразу видно необходимое (как следует из дальнейшего, также являющееся достаточным) условие для этого: $\operatorname{rk}\varphi = \dim V - 1$.

Однако для любого нильпотентного оператора φ верен следующий результат: пространство V является прямой суммой φ-инвариантных подпространств, в каждом из которых базис — жорданова цепочка. Рассмотрим пример.

Пример 9.10. Пусть $\varphi := \frac{d^3}{dx^3} \colon \mathbb{R}[x]_{12} \to \mathbb{R}[x]_{12}$. Обозначим $e_k := \frac{x^k}{k!}$, $k = 0, \dots, 12$. Тогда действие φ на базисных векторах записывается в виде жордановых цепочек

$$\begin{array}{ccccccccccc} e_{12} & \mapsto & e_9 & \mapsto & e_6 & \mapsto & e_3 & \mapsto & e_0 & \mapsto & 0 \\ & & e_{10} & \mapsto & e_7 & \mapsto & e_4 & \mapsto & e_1 & \mapsto & 0 \\ & & e_{11} & \mapsto & e_8 & \mapsto & e_5 & \mapsto & e_2 & \mapsto & 0 \end{array}$$

Заметим, что k-й столбец этой таблицы, если считать справа, состоит из корневых векторов высоты $k-1$. Ясно, что линейная оболочка векторов из каждой жордановой цепочки φ-инвариантна, и φ в базисе $\{e_0, e_3, e_6, e_9, e_{12}, e_2, e_5, e_8, e_{11}, e_1, e_4, e_7, e_{10}\}$ имеет блочно-диагональную матрицу, блоки которой являются нильпотентными жордановыми клетками порядков $5, 4, 4$.

Напомним, что базис, в котором матрица оператора имеет блочно-диагональный вид с жордановыми клетками в качестве блоков, называется *жордановым базисом.*

Очевидно, что максимальная длина жордановой цепочки для нильпотентного оператора φ равна высоте этого оператора. Поэтому возникает следующая идея доказательства существования жорданова базиса: найти для φ вектор v максимальной высоты (равной $\operatorname{ht}\varphi$) и попытаться доказать, что для линейной оболочки порожденной им жордановой цепочки существует φ-инвариантное прямое дополнение. Далее можно было бы применить индуктивное предположение о существовании жорданова базиса к этому прямому дополнению и ограничению φ на него. Эта идея действительно может быть реализована, см. [11], Гл. 6, § 4, Предложение 4. Мы, однако, приведем несколько другое рассуждение.

Предложение 9.11. *У нильпотентного оператора φ на конечномерном пространстве V существует жорданов базис.*

Доказательство. Нам нужно доказать следующее. Если $\varphi \colon V \to V$ — линейный оператор на конечномерном векторном пространстве V такой, что $\varphi^m = 0$ для некоторого $m \geq 1$, то в V существует такой набор векторов $v_1, \dots, v_r$ и отвечающий им набор натуральных чисел $k_1, \dots, k_r$, что система векторов

$$\varphi^{k_1-1}(v_1),\ \varphi^{k_1-2}(v_1),\ \dots,\ \varphi(v_1),\ v_1,\ \dots,\ \varphi^{k_r-1}(v_r),\ \varphi^{k_r-2}(v_r),\ \dots,\ \varphi(v_r),\ v_r, \tag{78}$$

где $\varphi^{k_i}(v_i) = 0$ для всех $1 \leq i \leq r$, является базисом в V[49]. Легко видеть, что это — жорданов базис для φ, и обратно, любой жорданов базис имеет такой вид.

Для доказательства Предложения воспользуемся индукцией по $\dim V$. Если $\dim V = 1$, то $\varphi = 0$ и требуемый результат, очевидно, верен. Для доказательства шага индукции предположим, что $\dim V \geq 2$. Ясно, что $\varphi(V) := \operatorname{Im}\varphi \subset V$, но при этом $\varphi(V) \neq V$, ибо тогда $\varphi^m(V) = \varphi^{m-1}(V) = \dots = \varphi(V) = V$, что противоречит равенству $\varphi^m = 0$. Кроме того, в случае $\varphi = 0$ требуемый результат тривиален. Таким образом, мы можем предположить, что

$$0 \subsetneq \varphi(V) \subsetneq V.$$

По предположению индукции (примененному к пространству $U := \varphi(V)$ и ограничению на него оператора φ) в U существует набор векторов $u_1, \dots, u_s$ такой, что

$$u_1, \varphi(u_1), \dots, \varphi^{l_1-1}(u_1),\ \dots,\ u_s, \varphi(u_s), \dots, \varphi^{l_s-1}(u_s) \tag{79}$$

[49] Заметим, что высота φ тогда равна $\max_{1 \leq i \leq r}(k_i)$.

— базис в U и $\varphi^{l_i}(u_i) = 0$ для $1 \leq i \leq s$.

Для $1 \leq i \leq s$ выберем такие векторы $v_i \in V$, что $\varphi(v_i) = u_i$ (такие v_i существуют, поскольку $u_i \in \varphi(V)$). Подпространство $\operatorname{Ker}\varphi \subset V$ содержит линейно независимые векторы $\varphi^{l_1-1}(u_1), \ldots, \varphi^{l_s-1}(u_s)$. Дополним эти векторы до базиса в $\operatorname{Ker}\varphi$ векторами $w_1, \ldots, w_p$ (этим векторам будут отвечать жордановы цепочки длины 1 в (78)). Мы докажем, что

$$v_1, \varphi(v_1), \ldots, \varphi^{l_1}(v_1), \ \ldots\ , v_s, \varphi(v_s), \ldots, \varphi^{l_s}(v_s), w_1, \ldots, w_p \tag{80}$$

— требуемый (с точностью до перестановки векторов) базис в V.

Для доказательства линейной независимости системы (80) применим φ к произвольной линейной комбинации указанных векторов, равной нулю. Тогда в силу линейной независимости системы (79) получим, что коэффициенты перед векторами

$$v_1, \ldots, \varphi^{l_1-1}(v_1), \ \ldots\ , v_s, \ldots, \varphi^{l_s-1}(v_s)$$

равны нулю. Теперь линейная независимость (80) следует из того, что

$$\varphi^{l_1}(v_1), \ldots, \varphi^{l_s}(v_s), w_1, \ldots, w_p$$

— базис в $\operatorname{Ker}\varphi$.

Проверим теперь, что число векторов в (80) равно $\dim V$. Действительно, из (79) $\dim \operatorname{Im}\varphi = l_1 + \ldots + l_s$; кроме того, $\dim \operatorname{Ker}\varphi = s + p$. Тогда

$$\dim V = \dim \operatorname{Im}\varphi + \dim \operatorname{Ker}\varphi = (l_1 + 1) + \ldots + (l_s + 1) + p,$$

а это — в точности число элементов в системе (80). ■

Как найти ЖНФ нильпотентного оператора φ? Легко видеть, что число жордановых клеток (включая клетки порядка 1) равно размерности ядра φ (то есть собственного подпространства, отвечающего собственному значению 0). Максимальный размер жордановой клетки равен высоте оператора. Далее полезны следующие соображения. Рассмотрим нильпотентную клетку J_k порядка k. Ранги $J_k^0 = E,\ J_k,\ J_k^2,\ \ldots\ , J_k^{k-1},\ J_k^k = 0$ образуют строго убывающую последовательность $k, k-1, k-2, \ldots, 1, 0$. Так как ранг матрицы оператора не зависит от базиса, то для нахождения ЖНФ достаточно знать ранги степеней матрицы A, где A — матрица φ в произвольном базисе.

Поясним сказанное на примере оператора из Примера 9.10. Размерность его ядра равна 3 (оно равно $\mathbb{R}[x]_2 \subset \mathbb{R}[x]_{12}$), значит в ЖНФ имеются 3 жордановы клетки. Размерность ядра $\varphi^2 = \frac{d^6}{dx^6}$ равна 6, значит все жордановы клетки имеют порядок больше 1 (если бы были клетки порядка 1, то так как они уже нулевые, то при возведении в квадрат их ранг не меняется, и в этом случае падение ранга всего оператора было бы меньше чем на 3). Размерность ядра $\varphi^3 = \frac{d^9}{dx^9}$ равна 9, значит все жордановы клетки имеют порядок больше 2. Размерность ядра $\varphi^4 = \frac{d^{12}}{dx^{12}}$ равна 12, значит все жордановы клетки имеют порядок больше 3. Размерность ядра $\varphi^5 = 0$ равна 13, значит только одна жорданова клетка имеет порядок больше 4, равный 5. Значит, размеры клеток в ЖНФ $5, 4, 4$ и $5 + 4 + 4 = 13 = \dim V$.

Задача 9.12. *Характеристический и минимальный многочлены оператора φ равны соответственно t^5 и t^2. Опишите возможные ЖНФ оператора φ.*

Как искать жорданов базис нильпотентного оператора? Для изложения алгоритма нам будет полезно следующее понятие.

Определение 9.13. Система векторов $e_1, \ldots, e_k \in V$ называется *линейно независимой над подпространством $U \subset V$*, если из $\lambda_1 e_1 + \ldots + \lambda_k e_k \in U$ следует $\lambda_1 = \ldots = \lambda_k = 0$.

Читателю предлагается убедиться, что система $e_1, \ldots, e_k \in V$ линейно независима над U тогда и только тогда, когда система $e_1 + U, \ldots, e_k + U$ векторов из V/U линейно независима (в обычном смысле). Более того, $e_1, \ldots, e_k \in V$ — *максимальная* линейно независимая система над U тогда и только тогда, когда $e_1 + U, \ldots, e_k + U$ является базисом в факторпространстве V/U.

Изложим теперь сам алгоритм. Пусть дан нильпотентный оператор $\varphi\colon V \to V$, $\operatorname{ht}\varphi = m$. Во-первых, найдем максимальную систему векторов $e_1, \ldots, e_k$ из $V = \operatorname{Ker}\varphi^m$, линейно независимую над $\operatorname{Ker}\varphi^{m-1} \subset V$. Такие векторы зададут жордановы цепочки максимальной длины m. Тогда система векторов $\varphi(e_1), \ldots, \varphi(e_k) \in \operatorname{Ker}\varphi^{m-1}$ линейно независима над $\operatorname{Ker}\varphi^{m-2}$. В самом деле, если $\lambda_1\varphi(e_1) + \ldots + \lambda_k\varphi(e_k) \in \operatorname{Ker}\varphi^{m-2}$ — линейная зависимость, то $\lambda_1 e_1 + \ldots + \lambda_k e_k \in \operatorname{Ker}\varphi^{m-1}$, что противоречит предположению. Дополним систему $\varphi(e_1), \ldots, \varphi(e_k) \in \operatorname{Ker}\varphi^{m-1}$ до максимальной линейно независимой над $\operatorname{Ker}\varphi^{m-2}$ системы $\varphi(e_1), \ldots, \varphi(e_k), e_{k+1}, \ldots, e_{k+l}$ в $\operatorname{Ker}\varphi^{m-1}$. Последние l векторов в ней будут порождать жордановы цепочки длины $m-1$. В свою очередь, система $\varphi^2(e_1), \ldots, \varphi^2(e_k), \varphi(e_{k+1}), \ldots, \varphi(e_{k+l})$ векторов из $\operatorname{Ker}\varphi^{m-2}$ линейно независима над $\operatorname{Ker}\varphi^{m-3}$. Дополним ее до максимальной линейно независимой системы $\varphi^2(e_1), \ldots, \varphi^2(e_k), \varphi(e_{k+1}), \ldots, \varphi(e_{k+l})$, $e_{k+l+1}, \ldots, e_{k+l+p}$ из $\operatorname{Ker}\varphi^{m-2}$ над $\operatorname{Ker}\varphi^{m-3}$, и т.д.

Почему в результате мы получим линейно независимую систему? Пусть дана нетривиальная линейная зависимость между построенными в результате описанного выше процесса векторами. Применяя к ней φ^{m-1}, получим некоторую зависимость $\lambda_1 e_1 + \ldots + \lambda_k e_k \in \operatorname{Ker}\varphi^{m-1}$, а значит $\lambda_1 = \ldots = \lambda_k = 0$. Таким образом, коэффициенты перед $e_1, \ldots, e_k$ в данной линейной зависимости равны 0. Теперь применяя к ней φ^{m-2}, получаем, что $\mu_1\varphi(e_1) + \ldots + \mu_k\varphi(e_k) + \mu_{k+1}e_{k+1} + \ldots + \mu_{k+l}e_{k+l} \in \operatorname{Ker}\varphi^{m-2}$, а значит в ней также равны нулю коэффициенты перед $\varphi(e_1), \ldots, \varphi(e_k), e_{k+1}, \ldots, e_{k+l}$, и т.д.

Почему полученная система будет базисом в V? Для доказательства достаточно сравнить размерности: в самом деле,

$$\sum_{i=1}^{m} \dim\left(\operatorname{Ker}\varphi^i/\operatorname{Ker}\varphi^{i-1}\right) = \dim V.$$

9.3 Основная теорема

Теорема 9.14. *Пусть $\varphi\colon V \to V$ — линейный оператор на конечномерном пространстве V над полем $\mathbb{K}$. Предположим, что его характеристический многочлен раскладывается на линейные множители над $\mathbb{K}$. Тогда в V существует базис, состоящий из жордановых цепочек оператора φ, отвечающих его собственным значениям (то есть жорданов базис для φ). Для каждого собственного значения λ набор длин соответствующих ему базисных жордановых цепочек не зависит от выбора жорданова базиса.*

Приведем переформулировку Теоремы в терминах матриц.

Теорема 9.15. *В условиях предыдущей Теоремы для оператора существует базис, в котором он имеет жорданову матрицу (то есть блочно-диагональную матрицу, блоками которой являются жордановы клетки). Набор порядков жордановых клеток, отвечающих собственному значению λ, не зависит от выбора такого базиса.*

Доказательство. Доказательство существования жорданова базиса следует из предыдущего. Напомним его основные моменты. В условии Теоремы все пространство V представляется в виде прямой суммы корневых подпространств оператора φ, которые к тому же φ-инвариантны. Значит, достаточно доказать существование базиса из жордановых цепочек для отдельного корневого подпространства V^λ, поскольку тогда базис в V можно получить как объединение базисов в корневых подпространствах. Оператор $\psi = (\varphi - \lambda\operatorname{Id}_V)$ на V^λ нильпотентен, и для него существование базиса из жордановых цепочек доказано в Предложении 9.11. При этом жордановы цепочки ψ, отвечающие его собственному значению 0 — в точности жордановы цепочки оператора φ, отвечающие собственному значению λ.

Доказательство единственности проведем для матричной формулировки. Заметим, что число и порядок жордановых клеток с собственным значением λ однозначно определяются набором рангов степеней оператора $\varphi - \lambda \operatorname{Id}_V$. А именно, число таких клеток равно $\dim V - \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)$. Число клеток порядка больше 1 равно $\operatorname{rk}(\varphi - \lambda \operatorname{Id}_V) - \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^2$, число клеток порядка больше 2 равно $\operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^2 - \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^3$ и т.д. Если $\operatorname{ht}((\varphi - \lambda \operatorname{Id}_V)|_{V^\lambda}) = m$, то число клеток максимального порядка m равно $\operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^{m-1} - \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^m$, далее $\operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^m = \operatorname{rk}(\varphi - \lambda \operatorname{Id}_V)^{m+1} = \ldots = \dim V - \dim V^\lambda$. ■

В частности, для $\mathbb{K} = \mathbb{C}$ условие о разложимости на линейные множители выполнено для любого многочлена, значит любой оператор в комплексном линейном пространстве в некотором базисе задается жордановой матрицей.

Заметим, что размерность собственного подпространства оператора φ, отвечающего собственному значению λ, равна числу жордановых цепочек с данным собственным значением в жордановом базисе (числу жордановых клеток с собственным значением λ в ЖНФ), а размерность соответствующего корневого подпространства равна сумме длин жордановых цепочек с собственным значением λ в жордановом базисе (сумме порядков жордановых клеток с собственным значением λ в ЖНФ).

На множестве всех матриц из $\operatorname{Mat}_n(\mathbb{C})$ рассмотрим следующее отношение эквивалентности. Две матрицы A, $A' \in \operatorname{Mat}_n(\mathbb{C})$ назовем эквивалентными, если существует такая невырожденная матрица $C \in \operatorname{GL}_n(\mathbb{C})$, что $A' = C^{-1}AC$. То есть две матрицы эквивалентны тогда и только тогда, когда они являются матрицами одного и того же оператора в n-мерном пространстве над полем $\mathbb{C}$ в разных базисах. Из доказанной Теоремы следует, что в каждом классе эквивалентности есть жорданова матрица, причем две жордановы матрицы эквивалентны тогда и только тогда, когда одна из другой получается перестановкой жордановых клеток.

Следующая задача уточняет Предложение 8.76.

Задача 9.16. *Пусть $\mu_\varphi(t)$ — минимальный многочлен оператора φ. Докажите, что кратность его корня λ равна максимальному порядку жордановой клетки оператора φ с собственным значением λ.*

Задача 9.17. *Пусть для оператора φ известны его характеристический $\chi_\varphi(t) = t^4(t-1)^3$ и минимальный $\mu_\varphi(t) = t^2(t-1)^2$ многочлены. Что по этой информации можно сказать про ЖНФ оператора φ, а также про размерности его собственных и корневых подпространств?*

Задача 9.18. *Оператор φ удовлетворяет тождеству $\varphi^5 = \varphi^3$. Что можно сказать про его ЖНФ?*

Задача 9.19. *Найдите жорданову форму оператора $D = \frac{\partial}{\partial x} + \frac{\partial}{\partial y}$ на пространстве $\mathbb{R}[x, y]_4$ многочленов степени не выше 4 от переменных x, y.*

Замечание 9.20. В заключении данного раздела упомянем об одном недостатке жордановой нормальной формы. Допустим, у нас есть семейство комплексных матриц данного порядка, непрерывно зависящее от каких-то параметров. Каждую индивидуальную матрицу семейства можно привести к жордановой форме некоторой заменой базиса, но, вообще говоря, для матриц всего семейства нельзя добиться того, чтобы жорданова форма и приводящая к ней замена базиса непрерывно зависели от параметров.

Вот простейший пример описанной ситуации. Рассмотрим семейство матриц $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$, непрерывно зависящих от параметра ε. При $\varepsilon = 0$ ЖНФ матрицы семейства есть $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, в то время как при $\varepsilon \neq 0$ — $\begin{pmatrix} \sqrt{\varepsilon} & 0 \\ 0 & -\sqrt{\varepsilon} \end{pmatrix}$.

9.4 Применение ЖНФ к линейным дифференциальным уравнениям

Предложение 9.21. *Пусть L — конечномерное пространство комплекснозначных дифференцируемых функций вещественной переменной x, обладающее тем свойством, что если $f \in L$, то $\frac{df}{dx} \in L$. Тогда существуют такие попарно различные комплексные числа $\lambda_1, \dots, \lambda_s$ и целые числа $r_1, \dots, r_s \geq 1$, что $L = \oplus L_i$, где L_i — пространство функций вида $e^{\lambda_i x} P(x)$, где $P(x)$ — произвольный многочлен степени $\leq r_i - 1$.*

Доказательство. Так как пространство L инвариантно относительно $\frac{d}{dx}$, то этот оператор можно ограничить на L (причем поскольку $\frac{d}{dx}$ к функциям из L можно применять неограниченное число раз, все функции из L бесконечно дифференцируемы). Идея заключается в том, чтобы рассмотреть жорданов базис для оператора $\frac{d}{dx}$ на L и последовательно вычислить вид входящих в него функций, начиная с собственных векторов, затем корневых векторов высоты 2 и т.д.

А именно, предположим что линейный оператор $\frac{d}{dx}$ на комплексном пространстве L имеет жорданову форму с клетками, отвечающими собственным значениям $\lambda_1, \dots, \lambda_s$ размеров $r_1, \dots, r_s$ и рассмотрим соответствующие жордановы цепочки

$$\begin{array}{lllllll}
v^1_{r_1-1} & \xrightarrow{\frac{d}{dx}-\lambda_1 \mathrm{Id}} & v^1_{r_1-2} & \to \dots \to & v^1_0 & \xrightarrow{\frac{d}{dx}-\lambda_1 \mathrm{Id}} & 0 \\
v^2_{r_2-1} & \xrightarrow{\frac{d}{dx}-\lambda_2 \mathrm{Id}} & v^2_{r_2-2} & \to \dots \to & v^2_0 & \xrightarrow{\frac{d}{dx}-\lambda_2 \mathrm{Id}} & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
v^s_{r_s-1} & \xrightarrow{\frac{d}{dx}-\lambda_s \mathrm{Id}} & v^s_{r_s-2} & \to \dots \to & v^s_0 & \xrightarrow{\frac{d}{dx}-\lambda_s \mathrm{Id}} & 0
\end{array}$$

Тогда можно положить $v^i_0 = e^{\lambda_i x}$. Действительно, это — ненулевое (поскольку собственный вектор) решение дифференциального уравнения $\frac{df}{dx} = \lambda_i f$, которое определено однозначно с точностью до умножения на ненулевое число. (В самом деле, если f — решение указанного уравнения, то дифференцирование выражения $fe^{-\lambda_i x}$ дает 0, то есть это — некоторая константа). В частности, мы видим, что λ_i, $1 \leq i \leq s$, попарно различны, то есть каждому собственному значению отвечает ровно одна жорданова клетка. В следующей строчке стоят решения уравнений $\frac{df}{dx} - \lambda_i f = e^{\lambda_i x}$ (для тех i, для которых $r_i > 1$). Произвольное решение линейного неоднородного уравнения является суммой его частного решения и общего решения соответствующего однородного уравнения. Легко видеть, что в качестве частного решения подходит $\frac{x}{1!} e^{\lambda_i x}$. Поэтому положим $v^i_1 = \frac{x}{1!} e^{\lambda_i x}$ для i таких, что $r_i > 1$.

Далее положим по индукции $v^i_{k-1} = \frac{x^{k-1}}{(k-1)!} e^{\lambda_i x}$ при $0 \leq k-1 < r_i - 1$. Тогда $\frac{x^k}{k!} e^{\lambda_i x}$ является решением уравнения $\frac{df}{dx} - \lambda_i f = v^i_{k-1}$, что доказывает индуктивное предположение. Очевидно, что линейная оболочка векторов $v^i_0, \dots, v^i_{r_i-1}$ совпадает с пространством, состоящим из всех функций $P(x)e^{\lambda_i x}$, где $\deg P(x) \leq r_i - 1$. ■

Доказанное Предложение объясняет роль квазимногочленов (то есть функций вида $P(x)e^{\lambda x}$, где $P(x)$ — многочлен) в теории обыкновенных линейных дифференциальных уравнений с постоянными коэффициентами. Действительно, если $y(x)$ — функция вещественной переменной x, являющаяся решением однородного дифференциального уравнения

$$\frac{d^n y}{dx^n} + \sum_{i=0}^{n-1} a_i \frac{d^i y}{dx^i} = 0, \quad a_i \in \mathbb{C}, \tag{81}$$

то $y(x)$ по крайней мере n раз дифференцируема и индукция, использующая выражение (81) n-й производной через производные меньшего порядка показывает, что на самом деле она бесконечно дифференцируема, а также что линейная оболочка функций $\frac{d^i y}{dx^i}$, $i \geq 0$, конечномерна и оператор $\frac{d}{dx}$ переводит

ее в себя. Как показывает предыдущее Предложение, из этого вытекает, что $y(x)$ представляется в виде $\sum P_i(x)e^{\lambda_i x}$, где $P_i(x)$ — многочлены.

По уравнению (81) определим многочлен $f(t) := t^n + \sum_{i=0}^{n-1} a_i t^i$. Очевидно, что $f(t)$ — аннулирующий многочлен оператора $\frac{d}{dx}$ на линейном пространстве L всех решений уравнения (81).

Предложение 9.22. *Многочлен $f(t)$ является характеристическим и минимальным многочленом оператора $\frac{d}{dx}$ на пространстве L всех решений уравнения (81). В частности,* $\dim L = n$ *и λ_i — его корни кратностей r_i, $\sum_i r_i = n$.*

Доказательство. Если L бесконечномерно, то тем не менее произвольный его элемент (в силу соотношения (81)) принадлежит конечномерному $\frac{d}{dx}$-инвариантному подпространству. Любое такое подпространство представляется в виде прямой суммы корневых подпространств оператора $\frac{d}{dx}$, в которых (как мы видели в предыдущем Предложении) квазиодночлены $\{e^{\lambda x}, xe^{\lambda x}, \dots, \frac{x^k}{k!}e^{\lambda x}\}$ (для некоторого k) образуют базис. Подставляя $e^{\lambda x}$ в (81) получаем, что λ — корень $f(t)$.

Пусть $f(t) = \prod_{i=1}^{s}(t-\lambda_i)^{r_i}$, причем $\lambda_i \neq \lambda_j$ при $i \neq j$. Поскольку оператор $\frac{d}{dx} - \lambda_i \mathrm{Id}_L$ понижает степень $\frac{x^k}{k!}e^{\lambda_i x}$, $k \geq 1$ на 1 и определяет изоморфизм при ограничении на пространство квазимногочленов с $\lambda \neq \lambda_i$ мы видим, что для каждого корня λ_i многочлена $f(t)$ в L имеется r_i-мерное корневое подпространство оператора $\frac{d}{dx}$ и все L является их прямой суммой. В частности, многочлен $f(t)$ является минимальным многочленом оператора $\frac{d}{dx}$, а поскольку для каждого собственного значения λ_i имеется единственная жорданова клетка, то и характеристическим. ■

Таким образом, в обозначениях из предыдущего доказательства пространство решений уравнения (81) является линейной оболочкой квазимногочленов

$$P_i(x)e^{\lambda_i x}, \quad \deg P_i(x) \leq r_i - 1, \quad 1 \leq i \leq s.$$

Задача 9.23. *Найдите все решения дифференциального уравнения*

$$y''' + 2y'' - 4y' - 8y = 0.$$

Решение. Характеристическое уравнение

$$t^3 + 2t^2 - 4t - 8 = (t+2)(t^2 - 4) = 0.$$

Его корни $\lambda_1 = 2$ кратности 1 и $\lambda_2 = -2$ кратности 2. Таким образом, функции e^{2x}, e^{-2x}, xe^{-2x} образуют базис в пространстве решений (называемый также фундаментальной системой решений) рассматриваемого уравнения. ■

9.5 Применение ЖНФ к рекуррентным последовательностям

У изложенной выше теории линейных дифференциальных уравнений есть красивый дискретный аналог — теория рекуррентных последовательностей. Чтобы подчеркнуть указанную аналогию (в основе которой лежит общая математическая основа — теория операторов в конечномерных линейных пространствах, в частности, ЖНФ), изложение в этом параграфе совершенно параллельно предыдущему.

Пусть V — бесконечномерное комплексное линейное пространство, состоящее из всех последовательностей комплексных чисел $V = \{(x_0, x_1, \dots,) \mid x_i \in \mathbb{C}\}$ с покомпонентным сложением и умножением на скаляры. На нем действует линейный оператор левого сдвига

$$d\colon V \to V, \quad d(x_0, x_1, x_2, \dots) = (x_1, x_2, x_3, \dots).$$

Он является аналогом оператора дифференцирования на пространстве бесконечно дифференцируемых функций.

Напомним, что последовательность — функция на множестве натуральных чисел (в нашем случае включая ноль). Для удобства дальнейших ссылок для фиксированного $\lambda \in \mathbb{C}$ сразу определим набор последовательностей v_0, v_1, $v_2, \ldots$ следующим образом:

$$v_0(n) = \lambda^n, \;\; n \geq 0; \quad v_1(n) = n\lambda^{n-1} \;\text{ при }\; n \geq 1, \;\; v_1(0) = 0;$$
$$v_2(n) = \binom{n}{2}\lambda^{n-2} \;\text{ при }\; n \geq 2, \;\; v_2(n) = 0 \;\text{ при }\; n = 0, 1; \tag{82}$$
$$v_k(n) = \binom{n}{k}\lambda^{n-k} \;\text{ при }\; n \geq k, \;\; v_k(n) = 0 \;\text{ при }\; 0 \leq n \leq k-1.$$

Задача 9.24. *Докажите, что при* $\lambda \neq 0$

$$\langle v_0, \ldots, v_k\rangle_{\mathbb{C}} = \{p(n)\lambda^n \mid p(t) \in \mathbb{C}[t], \; \deg p(t) \leq k\}.$$

Если $\lambda = 0$, *то* $\langle v_0, \ldots, v_k\rangle_{\mathbb{C}}$ *состоит из всех последовательностей, обращающихся в нуль начиная с* $k+1$*-го члена (напомним, что нумерация у нас начинается с нуля).*

(Указание: используйте, что при фиксированном k, $k \leq n$, $\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}$ *является многочленом степени* k *от* n*).*

Через V_k^λ обозначим пространство последовательностей $\langle v_0, \ldots, v_k\rangle_{\mathbb{C}}$ из предыдущей задачи, отвечающее данному λ. Ясно, что $\dim V_k^\lambda = k+1$.

Следующее Предложение является аналогом Предложения 9.21.

Предложение 9.25. *Для конечномерного* d*-инвариантного подпространства* $L \subset V$ *существуют такие попарно различные комплексные числа* $\lambda_1, \ldots, \lambda_s$ *и целые числа* $r_1, \ldots, r_s \geq 1$, *что* $L = \oplus L_i$, *где* $L_i = V_{r_i-1}^{\lambda_i}$.

Доказательство. Приведенное ниже доказательство совершенно аналогично доказательству Предложения 9.21.

Так как пространство L инвариантно относительно оператора сдвига d, то этот оператор можно ограничить на L; положим $\delta := d|_L$. Идея заключается в том, чтобы рассмотреть жорданов базис для оператора δ на L и последовательно вычислить вид входящих в него последовательностей, начиная с собственных векторов, затем корневых векторов высоты 2 и т.д.

А именно предположим, что линейный оператор δ на комплексном пространстве L имеет жорданову форму с клетками, отвечающими собственным значениям $\lambda_1, \ldots, \lambda_s$ размеров $r_1, \ldots, r_s$ и рассмотрим соответствующие жордановы цепочки

$$\begin{array}{lllllllll}
v_{r_1-1}(\lambda_1) & \overset{\delta-\lambda_1\mathrm{Id}}{\longrightarrow} & v_{r_1-2}(\lambda_1) & \to & \ldots & \to & v_0(\lambda_1) & \overset{\delta-\lambda_1\mathrm{Id}}{\longrightarrow} & 0 \\
v_{r_2-1}(\lambda_2) & \overset{\delta-\lambda_2\mathrm{Id}}{\longrightarrow} & v_{r_2-2}(\lambda_2) & \to & \ldots & \to & v_0(\lambda_2) & \overset{\delta-\lambda_2\mathrm{Id}}{\longrightarrow} & 0 \\
\ldots\ldots & & \ldots\ldots & & \ldots\ldots & & \ldots\ldots & & \ldots\ldots \\
v_{r_s-1}(\lambda_s) & \overset{\delta-\lambda_s\mathrm{Id}}{\longrightarrow} & v_{r_s-2}(\lambda_s) & \to & \ldots & \to & v_0(\lambda_s) & \overset{\delta-\lambda_s\mathrm{Id}}{\longrightarrow} & 0.
\end{array}$$

Далее читатель легко убедится самостоятельно, что как и подсказывают обозначения, для $\lambda = \lambda_i$ роль жордановых цепочек играют последовательности (82). Например, геометрическая прогрессия $v_0(\lambda) = (1, \lambda, \lambda^2, \ldots)$ играет роль собственного вектора оператора δ с собственным значением λ, причем пространство собственных векторов, отвечающих данному собственному значению, одномерно, а это показывает, что каждому собственному значению отвечает ровно одна жорданова клетка. В следующей строчке стоят решения неоднородного уравнения $\delta y - \lambda y = v_0(\lambda)$; легко проверяется, что в качестве его частного решения подходит последовательность $y = v_1(\lambda)$ и т.д. Доказательство завершается с помощью индукции с использованием тождества Паскаля $\binom{n+1}{k} - \binom{n}{k} = \binom{n}{k-1}$ для биномиальных коэффициентов.

Теперь из Задачи 9.24 получаем, что соответствующее корневое подпространство L действительно совпадает с V^{λ}_{r-1}. ■

Пусть $L \subset V$ — пространство решений однородного рекуррентного соотношения

$$x_{k+n} + a_{n-1}x_{k+n-1} + \ldots + a_1 x_{k+1} + a_0 x_k = 0, \quad k = 0, 1, 2, \ldots. \tag{83}$$

Тогда пространство L d-инвариантно и имеет размерность n (поскольку очевидно, что рекуррента определяется однозначно первыми n членами). Более того, соотношения (83) означают, что $L = \operatorname{Ker} f(\delta)$, где $f(t) := t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$. Далее так же, как в Предложении 9.22 доказывается, что аннулирующий многочлен $f(t)$ оператора δ — характеристический и минимальный.

Таким образом, в обозначениях Задачи 9.24, корневое подпространство $V^{\lambda}_{r-1} \subset L$ r-кратного корня $\lambda \neq 0$ многочлена $f(t)$ состоит из всех последовательностей вида $(p(0), p(1)\lambda, p(2)\lambda^2, \ldots, p(k)\lambda^k, \ldots)$, где $p(t) \in \mathbb{C}[t]$, $\deg p(t) \leq r - 1$.

Задача 9.26. *Найдите все решения однородного рекуррентного соотношения*

$$x_{k+3} - 8x_{k+2} + 21x_{k+1} - 18x_k = 0.$$

Решение. Характеристическое уравнение

$$t^3 - 8t^2 + 21t - 18 = (t-3)^2(t-2) = 0.$$

Его корни $\lambda_1 = 3$ кратности 2 и $\lambda_2 = 2$ кратности 1. Таким образом, последовательности

$$(1, 3, 3^2, 3^3, 3^4, \ldots), \quad (0, 1, 2 \cdot 3, 3 \cdot 3^2, 4 \cdot 3^3, \ldots), \quad (1, 2, 2^2, 2^3, 2^4, \ldots)$$

образуют базис в пространстве решений рассматриваемой рекурренты. Задавая конкретные значения $x_0 = a$, $x_1 = b$, $x_2 = c$ можно получить соответствующее частное решение. ■

9.6 Пространство с оператором как модуль над кольцом многочленов

В этом разделе мы наметим более концептуальный подход к изучению линейных операторов, подробности см., например, в [11], Гл. 9.

В вводной главе отмечалось, что существуют обобщения линейных пространств над произвольным ассоциативным кольцом R с единицей вместо поля $\mathbb{K}$, они называются R-модулями. Более точно, *(левым) R-модулем* M называется абелева группа $(M, +)$, на которой задана операция $R \times M \to M$, $(r, m) \mapsto rm$ умножения (слева) на элементы кольца R, удовлетворяющая следующим условиям:

- $1m = m$ для любого $m \in M$ ($1 \in R$ — единица кольца);
- $s(rm) = (sr)m$ для любых r, $s \in R$ и $m \in M$;
- $(r + s)m = rm + sm$, $r(m_1 + m_2) = rm_1 + rm_2$ для любых r, $s \in R$ и m, m_1, $m_2 \in M$.

Рассмотрим несколько примеров модулей над разными кольцами R.

Пример 9.27. Из определений сразу следует, что если $\mathbb{K}$ — поле, то $\mathbb{K}$-модуль — это векторное пространство над $\mathbb{K}$.

Пример 9.28. $\mathbb{Z}$-модуль A по-существу то же, что абелева группа. Действительно, любую абелеву группу A можно рассматривать как $\mathbb{Z}$-модуль, если положить

$$na = \begin{cases} a + \ldots + a, & \text{если } n \in \mathbb{N}; \\ 0, & \text{если } n = 0; \\ (-a) + \ldots + (-a), & \text{если } n \text{ — целое отрицательное число.} \end{cases}$$

Обратно, из определения модуля легко вывести (сделайте это!), что в произвольном $\mathbb{Z}$-модуле умножение на целые числа связано с операцией сложения в абелевой группе описанным выше образом.

Пример 9.29. Любое линейное пространство V над полем $\mathbb{K}$ можно рассматривать не только как $\mathbb{K}$-модуль, но и как модуль над кольцом $\mathcal{L}(V)$ всех линейных операторов на V. Свойства V как $\mathcal{L}(V)$-модуля совсем не похожи на свойства V как $\mathbb{K}$-векторного пространства: например, любой ненулевой элемент $v \in V$ порождает все V как $\mathcal{L}(V)$-модуль (но только одномерное подпространство $\langle v \rangle$ в V как в $\mathbb{K}$-векторном пространстве).

Пример 9.30. Модуль над кольцом многочленов $\mathbb{K}[t]$ — то же, что пара (V, φ), состоящая из $\mathbb{K}$-линейного пространства V и линейного оператора $\varphi\colon V \to V$, такого, что $tv = \varphi(v)$, $\forall\, v \in V$.

В самом деле, поскольку поле $\mathbb{K}$ содержится в $\mathbb{K}[t]$ в качестве подкольца многочленов степени не выше 0, произвольный $\mathbb{K}[t]$-модуль является $\mathbb{K}$-модулем (то есть векторным пространством над полем $\mathbb{K}$) с некоторой дополнительной структурой. Из аксиом модуля следует, что умножение на t должно действовать как линейный оператор на V, который мы обозначим φ. Тогда произведение вектора $v \in V$ на произвольный многочлен $f(t) \in \mathbb{K}[t]$ должно быть равно $f(\varphi)(v)$ (результату применения линейного оператора $f(\varphi)$ к вектору v).

Обратно, имея пару (V, φ), читатель легко определит соответствующий $\mathbb{K}[t]$-модуль.

Ясно, что свойства линейного оператора отражаются на свойствах соответствующего модуля и поэтому неудивительно, что изучение $\mathbb{K}[t]$-модулей дает еще один способ изучения линейных операторов.

Пример 9.31. Для того, чтобы на вещественном векторном пространстве V задать структуру $\mathbb{C}$-модуля (то есть комплексного векторного пространства) нужно на V задать $\mathbb{R}$-линейный оператор $I\colon V \to V$ такой, что $I^2 = -\mathrm{Id}_V$. (Докажите, что такой оператор I существует только при условии что $\dim_{\mathbb{R}} V$ четна). Действительно, в этом случае мы можем определить умножение элементов V на комплексные числа по формуле $(a + bi)v := av + bI(v)$. Читателю предлагается проверить, что тем самым мы действительно получаем линейное пространство над $\mathbb{C}$.

И обратно, комплексное векторное пространство можно (оставив умножение только на $\mathbb{R} \subset \mathbb{C}$) рассматривать как вещественное векторное пространство, на котором вдобавок задан $\mathbb{R}$-линейный оператор I умножения на $i \in \mathbb{C}$, который в силу $i^2 = -1$ должен удовлетворять соотношению $I^2 = -\mathrm{Id}_V$.

Пример 9.32. Для заинтересованного читателя упомянем еще один важный пример модулей. Для любой конечной группы G и поля $\mathbb{K}$ можно построить т.н. *групповую алгебру* $\mathbb{K}[G]$ (см. Замечание 5.8). В учебниках алгебры доказывается, что $\mathbb{K}[G]$-модули — в точности линейные представления группы G над полем $\mathbb{K}$.

Задача 9.33. *Определите понятие подмодуля R-модуля M. Покажите, что подмодуль $\mathbb{K}[t]$-модуля (V, φ) — пара $(U, \varphi|_U)$, состоящая из φ-инвариантного подпространства $U \subset V$ и ограничения оператора φ на него.*

В частности, результат о том, что у произвольного оператора φ на линейном пространстве V конечной положительной размерности над алгебраически замкнутым полем $\mathbb{K}$ обязательно есть собственный вектор в терминах модулей можно сформулировать как существование в соответствующем $\mathbb{K}[t]$-модуле (V, φ) подмодуля, одномерного как линейное пространство.

Важную роль в этой теории играют ненулевые модули, у которых нет собственных (отличных от нулевого и самого модуля) подмодулей. Они называются *простыми*. Например, если поле $\mathbb{K}$ алгебраически замкнуто, то нет простых $\mathbb{K}[t]$-модулей кроме одномерных (как линейные пространства над $\mathbb{K}$). Над кольцом $\mathbb{R}[t]$ есть 1 и 2-мерные простые модули (например, модуль, отвечающий повороту евклидовой плоскости на угол $\neq \pi k$, прост). Пространство V является простым модулем над кольцом всех линейных операторов $\mathcal{L}(V)$.

Очевидным образом определяется прямая сумма модулей над данным кольцом R. Существование для данного подмодуля $(U, \varphi|_U)$ $\mathbb{K}[t]$-модуля (V, φ) подмодуля $(W, \varphi|_W)$ такого, что $V \cong U \oplus W$ (прямая сумма подмодулей) равносильно существованию для φ-инвариантного подпространства U φ-инвариантного прямого дополнения W.

Если для кольца R выполняется условие, что всякий подмодуль произвольного R-модуля является прямым слагаемым, то любой R-модуль является прямой суммой простых. Так обстоит дело в случае $R = \mathbb{K}$ (произвольное поле) или $R = \mathbb{K}[G]$, где $\mathbb{K}$ — поле характеристики 0, а G — конечная группа (теорема Машке). Простейший пример оператора на двумерном пространстве с матрицей $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ показывает, что данное условие не выполняется для $R = \mathbb{K}[t]$. (В самом деле, одномерный подмодуль, отвечающий левому верхнему углу матрицы, не имеет прямого дополнения). Это делает теорию $\mathbb{K}[t]$-модулей более сложной (в частности, приводит к тому, что даже над алгебраически замкнутым полем не любой оператор диагонализируем). Похожим образом дело обстоит и для кольца $R = \mathbb{Z}$.

Роль отображений между модулями, аналогичных линейным, играют *гомоморфизмы модулей*. Более подробно, пусть $M,\ N$ — два R-модуля. По определению, гомоморфизм между ними — такой гомоморфизм абелевых групп $\alpha\colon (M, +) \to (N, +)$, для которого $\alpha(r * m) = r \circ \alpha(m)$ для любых $m \in M$ и $r \in R$ (здесь мы специально умножение на элементы кольца R в модулях M и N обозначили разными символами — соответственно $*$ и $\circ$).

Задача 9.34. *Проверьте, что гомоморфизм между двумя $\mathbb{K}[t]$-модулями (V, φ) и (U, ψ) — это такое линейное отображение $\alpha\colon V \to U$ $\mathbb{K}$-линейных пространств V и U, для которого диаграмма*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ U & \xrightarrow[\psi]{} & U \end{array}$$

коммутативна, то есть $\forall\, v \in V\ \ \psi(\alpha(v)) = \alpha(\varphi(v))$.

Задача 9.35. *Пусть V — вещественное векторное пространство, а $\varphi\colon V \to V$ — $\mathbb{R}$-линейный оператор. Покажите, что φ определяет $\mathbb{C}$-линейный оператор $(V, I) \to (V, I)$ (см. Пример 9.31) тогда и только тогда, когда $\varphi \circ I = I \circ \varphi$.*

Как и в случае линейных отображений, биективный гомоморфизм модулей называется изоморфизмом, а модули, между которыми существует изоморфизм — изоморфными. Заметим, что изоморфизмы — в точности обратимые гомоморфизмы.

Задача 9.36. *Покажите, что два $\mathbb{K}[t]$-модуля вида (V, φ) и (V, ψ) (то есть φ и ψ — два (вообще говоря) разных линейных оператора на одном пространстве V) изоморфны тогда и только тогда, когда операторы φ и ψ сопряжены (то есть существует такой линейный изоморфизм $\alpha\colon V \to V$, что $\psi = \alpha \circ \varphi \circ \alpha^{-1}$).*

Из предыдущей задачи и изложенной выше теории жордановой нормальной формы следует, что в случае $\mathbb{K} = \mathbb{C}$ два оператора φ и ψ определяют на V изоморфные структуры $\mathbb{C}[t]$-модуля тогда и только тогда, когда эти операторы имеют одинаковую ЖНФ. Можно двигаться в обратном направлении: сначала классифицировать $\mathbb{C}[t]$-модули с точностью до изоморфизма, а затем применить полученную классификацию для нахождения нормальной формы операторов.

Задача классификации модулей над произвольным кольцом R выходит за пределы возможностей человеческой математики, однако для некоторых интересных классов колец такая классификация существует. В частности, существует теорема, описывающая классификацию конечнопорожденных модулей

над евклидовыми кольцами, к которым в частности относятся кольцо целых чисел $\mathbb{Z}$ и кольца многочленов $\mathbb{K}[t]$. Заинтересованный читатель может найти и соответствующую теорему, и вывод из нее жордановой нормальной формы в учебнике [11], Гл. 9, § 3.

10 Билинейные и квадратичные функции

Билинейные функции — важный класс объектов, определенных на линейных пространствах. Задание такой функции на данном линейном пространстве (как правило симметричной или кососимметричной) часто приводит к интересной геометрии. Так, например, для билинейной симметричной положительно определенной функции на вещественном пространстве мы получаем евклидову геометрию (которой будет посвящена отдельная глава). С точки зрения специальной теории относительности интерес представляют также знаконеопределенные функции. В различных теориях (в гамильтоновой механике например) важную роль также играют пространства, снабженные невырожденной кососимметрической функцией. В данном разделе мы рассмотрим классификацию симметричных и кососимметричных билинейных функций (главным образом над полями $\mathbb{R}$ и $\mathbb{C}$), в частности, познакомимся с их инвариантами, а также с важным критерием положительной определенности вещественной симметричной билинейной функции.

10.1 Основные определения

Пусть V — векторное пространство над полем $\mathbb{K}$[50].

Определение 10.1. *Билинейной функцией* (или *билинейной формой*) на векторном пространстве V называется отображение $\alpha\colon V \times V \to \mathbb{K}$, линейное по каждому из двух своих аргументов.

Пример 10.2. Скалярное произведение геометрических векторов на евклидовой плоскости или в евклидовом трехмерном пространстве.

Пример 10.3. Из свойств интеграла Римана, доказывемых в курсе анализа, следует, что функция $\alpha(f, g) = \int_a^b f(x)g(x)\,dx$ является билинейной функцией на (бесконечномерном!) пространстве $C[a, b]$.

Пример 10.4. Функция $\alpha(A,\, B) = \operatorname{tr}(AB)$ является билинейной функцией на пространстве матриц $\mathrm{Mat}_n(\mathbb{K})$.

Пример 10.5. Как следует из свойств умножения матриц, для любой матрицы $A \in \mathrm{Mat}_n(\mathbb{K})$ функция $\alpha(x, y) = x^T Ay$ является билинейной на пространстве $\mathbb{K}^n$ столбцов высоты n.

Пример 10.6. Ориентированная площадь параллелограмма, построенного на упорядоченной паре векторов $\{u,\, v\}$ (псевдоскалярное произведение) на ориентированной евклидовой плоскости является билинейной функцией от u и v.

[50] при этом мы считаем, что в поле $2 \neq 0$, такие поля имеют характеристику $\neq 2$.

Пример 10.7. Пусть $C^1[a,b]$ — бесконечномерное линейное пространство непрерывно дифференцируемых функций на отрезке $[a,b]$, а $C^1_0[a,b] \subset C^1[a,b]$ — линейное подпространство в нем, состоящее из функций, принимающих нулевые значения в концах отрезка. Для $f,\ g \in C^1_0[a,b]$ выражение $\int_a^b f(x)g'(x)\,dx$ задает билинейную функцию на $C^1_0[a,b]$.

Легко проверяется, что сумма билинейных функций на V снова является билинейной функцией на V, произведение билинейной функции на скаляр снова билинейная функция и более того, билинейные функции на V образуют линейное пространство, которое мы обозначим $\mathcal{B}(V)$.

Сейчас мы покажем, что при отождествлении n-мерного пространства V с пространством столбцов $\mathbb{K}^n$ с помощью выбора базиса билинейная функция на V отождествляется с билинейной функцией из Примера 10.5 (для своей матрицы A).

Лемма 10.8. Пусть $\{e_1,\dots,e_n\}$ — фиксированный базис в V. Тогда для любого набора n^2 скаляров $a_{ij},\ 1 \le i,j \le n$ существует единственная билинейная функция $\alpha \in \mathcal{B}(V)$ такая, что $\alpha(e_i,e_j) = a_{ij},\ 1 \le i,j \le n$.

Доказательство. Сначала предположим, что такая билинейная функция α существует. Тогда по билинейности для произвольных $u,\ v \in V$ получаем:

$$\alpha(u,v) = \alpha\left(\sum_i u_i e_i, \sum_j v_j e_j\right) = \sum_{i,j} u_i v_j \alpha(e_i,e_j) = \sum_{i,j} a_{ij} u_i v_j.$$

Значит, существует не более одной билинейной функции, удовлетворяющей поставленному условию.

Теперь осталось лишь заметить, что функция $\alpha\colon V \times V \to \mathbb{K}$, для произвольных векторов $u,\ v \in V$ определенная равенством

$$\alpha(u,v) = \sum_{i,j} a_{ij} u_i v_j, \tag{84}$$

в самом деле билинейна, и для нее $\alpha(e_i,e_j) = a_{ij}$. ∎

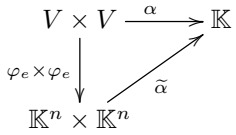
Матрица $A = (a_{ij}) \in \mathrm{Mat}_n(\mathbb{K})$ называется *матрицей билинейной функции* α *в базисе* $\{e_1,\dots,e_n\}$.

Заметим, что формула (84) означает, что значение билинейной функции α с матрицей $A = (a_{ij})$ в базисе $\{e_1,\dots,e_n\}$ на векторах u и v с координатными столбцами x и y в том же базисе вычисляется как

$$\alpha(u,v) = x^T A y. \tag{85}$$

Замечание 10.9. Попробуем пояснить формулу (85). Мы знаем, что выбор базиса $\{e_1,\dots,e_n\}$ в V определяет изоморфизм $\varphi_e\colon V \to \mathbb{K}^n$, сопоставляющий вектору $v \in V$ его координатный столбец $\varphi_e(v) \in \mathbb{K}^n$. Пусть A — матрица билинейной функции $\alpha\colon V \times V \to \mathbb{K}$ в базисе $\{e_1,\dots,e_n\}$. Зададим билинейную функцию $\widetilde{\alpha}\colon \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ на пространстве столбцов $\mathbb{K}^n$ формулой $\widetilde{\alpha}(x,y) = x^T A y$ для произвольных $x,\ y \in \mathbb{K}^n$.

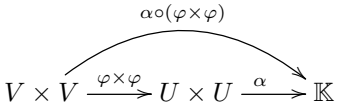
Тогда равенство (85) равносильно $\alpha(u,\,v) = \widetilde{\alpha}(\varphi_e(u), \varphi_e(v))$ для любых $u,\, v \in V$. Иначе говоря, диаграмма



(86)

коммутативна. То есть, как и утверждалось выше, при отождествлении n-мерного пространства V с пространством столбцов $\mathbb{K}^n$ с помощью выбора базиса билинейная функция на V отождествляется с билинейной функцией из Примера 10.5 (для соответствующей матрицы A).

Вообще, можно заметить, что изоморфизм линейных пространств $\varphi\colon V \to U$ определяет изоморфизм линейных пространств $\mathcal{B}(U) \to \mathcal{B}(V)$, $\alpha \mapsto \alpha(\varphi(\ldots), \varphi(\ldots))$ (наглядно это видно из диаграммы



— билинейная функция α определяет билинейную функцию $\alpha \circ (\varphi \times \varphi)$).

Рассматривая $\mathbb{K}^n$ в качестве U и используя данное в Примере 10.5 описание всех билинейных функций на $\mathbb{K}^n$ как задаваемых матрицами $A \in \mathrm{Mat}_n(\mathbb{K})$, мы снова приходим к приведенному выше результату.

Таким образом, мы определили отображение

$$\psi = \psi_e\colon \mathcal{B}(V) \to \mathrm{Mat}_n(\mathbb{K}), \quad \psi(\alpha) = (a_{ij}), \;\; \text{где} \;\; a_{ij} = \alpha(e_i, e_j). \tag{87}$$

Предложение 10.10. *Отображение (87) является биекцией.*

Доказательство. Следует непосредственно из доказанной выше Леммы. ■

В действительности ψ — не просто биекция, а изоморфизм линейных пространств. В самом деле, если $\alpha,\, \beta \in \mathcal{B}(V)$ — билинейные функции с матрицами A и B в выбранном базисе и $C = (c_{ij})$ обозначает матрицу билинейной функции $\alpha + \beta$ в том же базисе, то

$$c_{ij} = (\alpha + \beta)(e_i, e_j) = \alpha(e_i, e_j) + \beta(e_i, e_j) = a_{ij} + b_{ij}.$$

Аналогично проверяется та часть определения линейности, которая связана с умножением на скаляр.

Таким образом, мы действительно построили некоторый линейный изоморфизм (87) (зависящий от базиса e). В частности, $\dim \mathcal{B}(V) = (\dim V)^2$.

Выясним теперь, как матрица билинейной функции зависит от базиса[51]. Пусть $\{e_1, \ldots, e_n\}$ и $\{e'_1, \ldots, e'_n\}$ — два базиса в V и C — матрица перехода от первого базиса ко второму. Тогда координатные столбцы x, x' вектора $u \in V$ в этих базисах связаны соотношением $x = Cx'$. Имеем (см. (85))

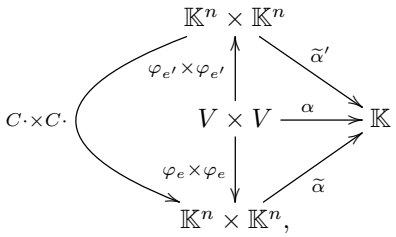
$$\alpha(u, v) = x^T A y = (Cx')^T A (Cy') = x'^T (C^T A C) y'.$$

[51] То есть как от базиса зависит построенный изоморфизм ψ_e.

С другой стороны, если A' — матрица α в базисе $\{e'_1, \dots, e'_n\}$, то $\alpha(u, v) = x'^T A' y'$. То есть билинейные функции с матрицами $C^T AC$ и A' в базисе $\{e'_1, \dots, e'_n\}$ совпадают (обе равны α), а тогда в силу доказанного выше эти матрицы равны, то есть матрица α во втором базисе есть

$$A' = C^T AC. \tag{88}$$

Замечание 10.11. Формулу (88) иллюстрирует коммутативная диаграмма



составленная из диаграмм (86) и (50) (ср. (56)). В самом деле, из ее коммутативности следует, что $\widetilde{\alpha}'(x', y') = \widetilde{\alpha}(Cx', Cy')$, то есть $x'^T A' y' = (Cx')^T ACy' = x'^T C^T ACy'$.

Полезно сопоставить формулу (88) с аналогичной формулой (55) для матрицы линейного оператора. Мы видим, что хотя и линейный оператор и билинейная функция в базисе задаются матрицей, эти матрицы по-разному преобразуются при замене базиса (одинаково только когда матрица перехода ортогональна). Это имеет важные следствия. Например, мы видели, что определитель и след матрицы линейного оператора не зависят от базиса; для матриц билинейных функций это уже не так (читателю предлагается в этом убедиться).

В частности, если оператор в каком-либо базисе имеет единичную матрицу, то он тождественный и в любом другом базисе он также имеет единичную матрицу. А если билинейная функция имеет в некотором базисе единичную матрицу, то в базисе, полученном из исходного с помощью матрицы перехода C она будет иметь матрицу $C^T C$, которая является единичной тогда и только тогда, когда C ортогональна.

Еще одной особенностью закона преобразования матриц билинейных функций является то, что сохраняется условие симметричности (кососимметричности) матрицы. То есть если в некотором базисе матрица билинейной функции симметрична (кососимметрична), то это верно и для любого другого базиса (убедитесь в этом).

Определение 10.12. *Ядром* билинейной функции $\alpha\colon V \times V \to \mathbb{K}$ называется подпространство

$$\operatorname{Ker} \alpha := \{v \in V \mid \alpha(u, v) = 0 \ \forall\, u \in V\} \subset V.$$

Функция α называется *невырожденной*, если $\operatorname{Ker} \alpha = 0$.

Например, скалярное произведение из Примера 10.2 является невырожденной билинейной функцией, поскольку для любого ненулевого вектора его скалярный квадрат положителен. По этой же причине невырождена билинейная функция из Примера 10.3. Невырожденность билинейной функции из Примера 10.5 равносильна невырожденности матрицы A.

Задача 10.13. *Докажите невырожденность функций из Примеров 10.4 и 10.6.*

Предложение 10.14. *Пусть A — матрица α в некотором базисе $\{e_1, \dots, e_n\}$ пространства V. Тогда*

$$\dim \operatorname{Ker} \alpha = n - \operatorname{rk} A.$$

Доказательство. Легко видеть, что

$$\operatorname{Ker} \alpha = \{v \in V \mid \alpha(e_i, v) = 0,\ i = 1, \dots, n\},$$

то есть при отождествлении V с пространством столбцов $\mathbb{K}^n$ при помощи выбранного базиса подпространство $\operatorname{Ker} \alpha$ отождествляется с пространством решений СЛОУ с матрицей коэффициентов A. ∎

В частности, $\operatorname{Ker} \alpha = 0$ тогда и только тогда, когда $\operatorname{rk} A = n$, то есть когда матрица A невырождена.

Следствие 10.15. *Ранг матрицы билинейной функции не зависит от базиса.*

Доказательство. Действительно, подпространство $\operatorname{Ker} \alpha$ ни от каких базисов не зависит (а зависит только от самой α). ∎

Заметим, что предыдущее следствие можно вывести и непосредственно из формулы (88), поскольку последняя показывает, что матрица A' получается из A некоторой конечной последовательностью элементарных преобразований строк и столбцов.

Доказанное следствие влечет корректность следующего определения.

Определение 10.16. *Рангом* билинейной функции α называется ранг ее матрицы в произвольном базисе. Он обозначается $\operatorname{rk} \alpha$.

Пример 10.17. Пусть $f_1,\ f_2 \colon V \to \mathbb{K}$ — ненулевые линейные функции на пространстве V. Тогда билинейная функция $f_1 \otimes f_2$, заданная равенством $(f_1 \otimes f_2)(u, v) := f_1(u) f_2(v)\ \forall\, u,\ v \in V$, имеет ранг 1. (В самом деле, ее матрица в данном базисе является произведением столбца, транспонированного к координатной строке функции f_1, на координатную строку функции f_2). Операция $\otimes$ называется *тензорным произведением* линейных функций. Подробнее она будет рассмотрена в § 15.2.

Задача 10.18. *Докажите что наоборот, любая билинейная функция ранга* 1 *является тензорным произведением ненулевых линейных функций.*

Решение. Ядро, которое определено в Определении 10.12, естественно назвать правым ядром. Аналогично можно определить левое ядро

$$\operatorname{Ker}' \alpha := \{u \in V \mid \alpha(u,\, v) = 0\ \forall\, v \in V\} \subset V.$$

Обозначим $U := \operatorname{Ker} \alpha,\ W := \operatorname{Ker}' \alpha$. Ясно, что $\dim U = \dim W$, причем если $\operatorname{rk} \alpha = 1$, то размерности обоих ядер равны $n - 1$. Могут представиться две ситуации: 1) $U = W$ или 2) $U \neq W$, в этом случае $U + W = V$.

В случае 1) выберем вектор $v \notin U (= W)$ и линейную функцию $f\colon V \to \mathbb{K}$, такую что $\operatorname{Ker} f = U$, $f(v) = 1$. Тогда, используя представление любого вектора из V в виде $\lambda v + z$, где $z \in U = W$, легко проверить, что $\alpha = \alpha(v, v) f \otimes f$ (в частности, $\alpha(v, v) \neq 0$).

В случае 2) выберем векторы $u \in U \setminus W$ и $w \in W \setminus U$ (они вместе с $U \cap W$ порождают V), а также линейные функции f_1, $f_2, : V \to \mathbb{K}$, такие что $\operatorname{Ker} f_1 = W$, $f_1(u) = 1$, $\operatorname{Ker} f_2 = U$, $f_2(w) = 1$. Теперь с использованием того, что любой вектор из V представляется в виде $\beta u + \gamma w + z$, где $z \in U \cap W$ (в самом деле, для любого $v \in V$ $v - f_1(v)u - f_2(v)w \in U \cap W$), легко проверяется, что $\alpha = \alpha(u, w) f_1 \otimes f_2$. ■

Из предыдущей Задачи следует, что любая билинейная функция ранга r является суммой r попарных тензорных произведений некоторых линейных функций.

Замечание 10.19. Заметим, что с использованием тензорного произведения линейных функций, введенного в Примере 10.17, билинейную функцию (84) можно также записать в виде $\alpha = \sum_{i,j} a_{ij} \varepsilon_i \otimes \varepsilon_j$, где $\{\varepsilon_1, \dots, \varepsilon_n\}$ — биортогональный базис к выбранному базису $\{e_1, \dots, e_n\}$ в V (см. Определение 7.99), ср. аналогичное выражение (58) для линейных функций. Однако в дальнейшем мы в основном (за исключением § 10.7) будем придерживаться более традиционного обозначения (84), принятого в учебниках по линейной алгебре.

В дальнейшем мы будем интересоваться не всеми билинейными функциями, а только теми, которые либо симметричны, либо кососимметричны.

Заметим, что для билинейной функции $\alpha\colon V \times V \to \mathbb{K}$ можно определить *транспонированную билинейную функцию* $\alpha^T\colon V \times V \to \mathbb{K}$ по формуле $\alpha^T(u, v) = \alpha(v, u) \ \ \forall\, u,\, v \in V$. Ясно, что матрицы функций α и α^T в фиксированном базисе являются транспонированными друг другу.

Определение 10.20. Билинейная функция $\alpha\colon V \times V \to \mathbb{K}$ называется *симметричной* (соответственно *кососимметричной*), если $\alpha^T = \alpha$ (соответственно $\alpha^T = -\alpha$).

Очевидно, билинейная функция симметрична (кососимметрична) тогда и только тогда, когда ее матрица в некотором (а значит в любом) базисе симметрична (кососимметрична).

Например, билинейные функции из Примеров 10.2, 10.3, 10.4 симметричны, из Примеров 10.6 и 10.7 кососимметричны (для доказательства кососимметричности последней нужно воспользоваться формулой интегрирования по частям), а из Примера 10.5 симметрична (кососимметрична) тогда и только тогда, когда матрица A симметрична (кососимметрична).

Также очевидно, что симметричные (кососимметричные) функции образуют подпространство в $\mathcal{B}(V)$. Подпространство симметричных (соотв. кососимметричных) функций мы обозначим $\mathcal{B}^+(V)$ (соотв. $\mathcal{B}^-(V)$). При изоморфизме (87) они отождествляются с подпространствами симметричных (соотв. кососимметричных) матриц.

Равенство

$$\alpha = \frac{1}{2}\left(\alpha + \alpha^T\right) + \frac{1}{2}\left(\alpha - \alpha^T\right) \tag{89}$$

показывает, что любая билинейная функция единственным образом представляется в виде суммы симметричной α^+ и кососимметричной α^- (это также следует из существования

разложения пространства матриц порядка n в прямую сумму подпространств симметричных и кососимметричных). То есть $\mathcal{B}(V) = \mathcal{B}^+(V) \oplus \mathcal{B}^-(V)$.

Пример 10.21. Если $\alpha = f_1 \otimes f_2$ — билинейная функция ранга 1 (см. Пример 10.17), то

$$\alpha^+ := \frac{1}{2}(f_1 \otimes f_2 + f_2 \otimes f_1) \tag{90}$$

(то есть $\alpha^+(u, v) = \frac{1}{2}(f_1(u)f_2(v) + f_2(u)f_1(v))$) будет симметричной, а

$$\alpha^- := \frac{1}{2}(f_1 \otimes f_2 - f_2 \otimes f_1) \tag{91}$$

(то есть $\alpha^-(u, v) = \frac{1}{2}(f_1(u)f_2(v) - f_2(u)f_1(v))$) — кососимметричной билинейными функциями. Из того, что любая билинейная функция является суммой функций ранга 1 следует, что любая симметричная (соответственно кососимметричная) билинейная функция является суммой функций вида (90) (соответственно вида (91)).

Чтобы мотивировать следующее определение, обратимся к конкретному примеру билинейной функции — скалярному произведению в евклидовом пространстве. Вместо того, чтобы рассматривать скалярное произведение как функцию двух аргументов, можно рассмотреть функцию "скалярный квадрат вектора" $v \mapsto (v, v) = |v|^2$ от одного аргумента. Заметим, что если нам известны скалярные квадраты всех векторов, мы можем восстановить и их попарные скалярные произведения, используя теорему косинусов. Как мы вскоре увидим, это — общее свойство симметричных билинейных функций и отвечающих им "скалярных квадратов". По-научному, скалярные квадраты называются квадратичными функциями.

Определение 10.22. *Квадратичной функцией* на векторном пространстве V называется функция $q\colon V \to \mathbb{K}$, для которой существует билинейная функция $\alpha\colon V \times V \to \mathbb{K}$ такая, что $q(v) = \alpha(v, v)\ \forall\, v \in V$.

То есть любая билинейная функция α задает квадратичную функцию q_α, которая получается из α ограничением области определения с $V \times V$ на диагональ $\Delta_V := \{(v, v) \mid v \in V\} \subset V \times V$. Из определения непосредственно следует, что для любой квадратичной функции q на пространстве V и любого скаляра $\lambda \in \mathbb{K}$ верно равенство $q(\lambda v) = \lambda^2 q(v)\ \forall v \in V$. В базисе квадратичная функция является выражением вида $q(v) = \sum_{i,j} a_{ij} v_i v_j$, то есть однородным многочленом степени 2 от координат вектора.

Заметим, что если α кососимметрична, то ей отвечает нулевая квадратичная функция. Более общо, если две билинейные функции отличаются на кососимметричную функцию, то они определяют одну и ту же квадратичную функцию. Сейчас мы докажем, что по квадратичной функции q_α однозначно восстанавливается симметричная компонента билинейной функции α (см. формулу (89)).

Действительно, если α — билинейная функция, то для соответствующей квадратичной функции q_α и для любой пары векторов $u,\, v \in V$ имеем

$$q_\alpha(u+v) = \alpha(u+v, u+v) = \alpha(u,u) + \alpha(u,v) + \alpha(v,u) + \alpha(v,v) =$$

$$= q_\alpha(u) + \alpha(u,v) + \alpha(v,u) + q_\alpha(v),$$

откуда

$$\alpha(u,v) + \alpha(v,u) = q_\alpha(u+v) - q_\alpha(u) - q_\alpha(v).$$

В частности, если α симметрична, то

$$\alpha(u,v) = \frac{1}{2}(q_\alpha(u+v) - q_\alpha(u) - q_\alpha(v)). \tag{92}$$

Положим по определению $\alpha_q(u,\, v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$. Очевидно, что так определенная билинейная функция α_q симметрична.

Предложение 10.23. *Сопоставления*

$$\alpha \mapsto q_\alpha, \quad q \mapsto \alpha_q$$

определяют взаимно обратные биекции между множествами симметричных билинейных $\mathcal{B}^+(V)$ и квадратичных функций $Q(V)$.

Доказательство. Во-первых, проверим, что композиция

$$\mathcal{B}^+(V) \to Q(V) \to \mathcal{B}^+(V), \quad \alpha \mapsto q_\alpha \mapsto \alpha_{q_\alpha}$$

тождественна. Действительно, $q_\alpha(v) = \alpha(v,v)$ и

$$\alpha_{q_\alpha}(u,v) = \frac{1}{2}(q_\alpha(u+v) - q_\alpha(u) - q_\alpha(v)) = \frac{1}{2}(\alpha(u+v,u+v) - \alpha(u,u) - \alpha(v,v)) =$$

$$= \frac{1}{2}(\alpha(u,u) + \alpha(u,v) + \alpha(v,u) + \alpha(v,v) - \alpha(u,u) - \alpha(v,v)) = \alpha(u,v) \ \ \forall u,\, v \in V.$$

Во-вторых, проверим, что композиция

$$Q(V) \to \mathcal{B}^+(V) \to Q(V), \quad q \mapsto \alpha_q \mapsto q_{\alpha_q}$$

тождественна. Действительно,

$$q_{\alpha_q}(v) = \alpha_q(v,v) = \frac{1}{2}(q(2v) - 2q(v)) = \frac{1}{2}(4q(v) - 2q(v)) = q(v), \ \ \forall v \in V.$$

Заметим теперь, что для произвольных множеств X, Y отображения $f\colon X \to Y$ и $g\colon Y \to X$ такие, что $g \circ f = \mathrm{Id}_X$, $f \circ g = \mathrm{Id}_Y$ являются взаимно-обратными биекциями, то есть f и g биективны и $g = f^{-1}$, $f = g^{-1}$ (см. Предложение 1.5). ∎

Из доказанного Предложения следует, что все понятия, относящиеся к симметричным билинейным функциям (матрица, ранг, невырожденность и т.д.) переносятся на квадратичные функции. В дальнейшем изложении из соображений удобства мы будем иногда говорить о симметричных билинейных, иногда — о квадратичных функциях.

Заметим, что так как матрицей квадратичной функции по определению является матрица соответствующей ей *симметричной* билинейной функции, то

$$q(v) = \sum_{i,j} a_{ij} v_i v_j = \sum_i a_{ii} v_i^2 + 2 \sum_{i<j} a_{ij} v_i v_j.$$

10.2 Приведение билинейных симметричных (квадратичных) функций к диагональному виду

Начиная с этого момента все рассматриваемые билинейные функции, если не оговорено противное, предполагаются симметричными или кососимметричными.

Для изучения билинейных функций полезно привлечь геометрическую интуицию, связанную с конкретным примером билинейной функции — скалярным произведением в евклидовом пространстве. Например, условие ортогональности двух векторов в евклидовом пространстве равносильно тому, что их скалярное произведение равно нулю. Это мотивирует следующее определение.

Определение 10.24. Векторы u, $v \in V$ называются *ортогональными относительно* α, если $\alpha(u, v) = 0$. Условие ортогональности векторов записывается $u \perp v$.

Заметим, что так как α по предположению симметрична или кососимметрична, то отношение ортогональности симметрично (то есть $u \perp v \;\Leftrightarrow\; v \perp u$).

Определение 10.25. *Ортогональным дополнением к подпространству $U \subset V$ относительно α* называется подпространство

$$U^\perp := \{v \in V \mid \alpha(u, v) = 0 \;\forall\, u \in U\} \subset V.$$

Очевидно, что

$$V^\perp = \operatorname{Ker} \alpha.$$

Предложение 10.26. *Если функция α невырождена, то*

$$\dim U^\perp = \dim V - \dim U \quad u \;\; (U^\perp)^\perp = U.$$

Доказательство. Если $\{e_1, \ldots, e_k\}$ — базис в U, то

$$U^\perp = \{v \in V \mid \alpha(e_i, v) = 0,\; i = 1, \ldots, k\}. \tag{93}$$

Продолжим $\{e_1, \ldots, e_k\}$ до базиса $\{e_1, \ldots, e_n\}$ во всем пространстве V, пусть A — матрица α в этом базисе. Равенство (93) теперь означает, что в выбранном базисе в V условие

$v \in U^\perp$ равносильно тому, что координаты v удовлетворяют СЛОУ, матрица которой образована первыми k строками матрицы A. Так как α невырождена, то и матрица A невырождена, в частности, ее строки линейно независимы. Отсюда $\dim U^\perp = n - k$, где $n = \dim V,\ k = \dim U$, тем самым доказано первое из соотношений.

Дважды применяя доказанное соотношение, имеем

$$\dim (U^\perp)^\perp = n - \dim U^\perp = n - (n - k) = k = \dim U.$$

С другой стороны, очевидно, что $U \subset (U^\perp)^\perp$ (действительно, любой вектор из U ортогонален любому вектору из ортогонального дополнения к U), поэтому $U = (U^\perp)^\perp$ (ср. Теорему 6.19). ■

Задача 10.27. *Докажите, что если функция α невырождена, то для подпространств U, W в V*

$$U \subset W \ \Leftrightarrow\ U^\perp \supset W^\perp.$$

Если α — билинейная функция на V и $U \subset V$ — произвольное подпространство, то очевидным образом определяется ограничение $\alpha|_U$, являющееся билинейной функцией на U.

Определение 10.28. Подпространство $U \subset V$ называется *невырожденным относительно α*, если ограничение $\alpha|_U$ невырождено.

Очевидно, что $\operatorname{Ker} \alpha|_U = U \cap U^\perp$, поэтому подпространство U невырождено тогда и только тогда, когда $U \cap U^\perp = 0$.

Очень важно понимать, что *из невырожденности α на всем пространстве не следует невырожденность ее ограничения на любое подпространство*. Причина в том, что для ограничения $\alpha|_U$ мы рассматриваем "скалярные произведения" векторов $u \in U$ только на векторы из U, но может так оказаться, что несмотря на то, что $\alpha|_U(u, u') = \alpha(u, u') = 0\ \forall u' \in U$, во всем пространстве V найдется такой вектор $v \in V$, что $\alpha(u, v) \neq 0$. Вот конкретный пример.

Пример 10.29. Рассмотрим билинейную симметричную функцию α на двумерном пространстве V с матрицей $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ в базисе $\{e_1, e_2\}$. В координатах она записывается как $\alpha(u, v) = u_1v_1 - u_2v_2$. Очевидно, что α невырождена, но тем не менее скалярный квадрат $\alpha(e_1 + e_2,\ e_1 + e_2)$ вектора $e_1 + e_2$ равен нулю. Поэтому ограничение $\alpha|_{\langle e_1+e_2\rangle}$ на одномерное подпространство $\langle e_1 + e_2\rangle \subset V$ нулевое. На самом деле $\langle e_1 + e_2\rangle^\perp = \langle e_1 + e_2\rangle$. То же верно и для вектора $e_1 - e_2$.

Выбирая новый базис $\{e'_1,\ e'_2\}$ в V, $e'_1 = e_1 + e_2,\ e'_2 = e_1 - e_2$, получаем для α матрицу $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$, из которой видно, что ограничения α на одномерные подпространства $\langle e'_1\rangle$ и $\langle e'_2\rangle$ нулевые (причем $V = \langle e'_1\rangle \oplus \langle e'_2\rangle$!), в то же время сама α невырождена.

Как показывает следующее Предложение, если бы ограничение невырожденной α на любое подпространство было бы невырожденным, это сильно облегчило бы жизнь. Но, как мы только что убедились, в общем случае это неверно. Важным частным случаем когда это все же верно, является случай *положительно определенных* билинейных функций, который будет подробнее изучен далее.

Предложение 10.30. *Подпространство $U \subset V$ невырождено относительно α тогда и только тогда, когда $V = U \oplus U^\perp$.*

Доказательство. Как следует из доказательства Предложения 10.26, в любом случае $\dim U^\perp \geq \dim V - \dim U$.

Если подпространство U невырождено, то $U \cap U^\perp = \operatorname{Ker} \alpha|_U = 0$, значит сумма $U + U^\perp$ прямая и, согласно предыдущему абзацу, $\dim (U \oplus U^\perp) \geq \dim V$, поэтому $V = U \oplus U^\perp$.

Обратно, если $V = U \oplus U^\perp$, то, в частности, $U \cap U^\perp = 0$, а так как $U \cap U^\perp = \operatorname{Ker} \alpha|_U$, то ограничение $\alpha|_U$ невырождено. ∎

Например, как мы видели в Примере 10.29 для $U = \langle e_1 + e_2 \rangle$ имеет место соотношение $U^\perp = U$ и, значит, сумма U и $U^\perp$ не может быть прямой.

Любопытно отметить, что (в обозначениях предыдущего Предложения) из $V = U \oplus U^\perp$ не следует, что подпространство $U^\perp$ невырождено (читателю предлагается привести пример).

Начиная с этого момента все рассматриваемые билинейные функции, если не оговорено противное, предполагаются симметричными.

Определение 10.31. Базис $\{e_1, \ldots, e_n\}$ в V называется *ортогональным относительно* α, если его векторы попарно ортогональны, то есть $\alpha(e_i, e_j) = 0$ при $i \neq j$.

Очевидно, что базис $\{e_1, \ldots, e_n\}$ ортогонален тогда и только тогда, когда матрица α в нем диагональна, то есть $A = \operatorname{diag}(a_1, \ldots, a_n)$. При этом билинейная и квадратичная функции имеют вид

$$\alpha(u, v) = a_1 u_1 v_1 + \ldots + a_n u_n v_n, \quad q(v) = a_1 v_1^2 + \ldots + a_n v_n^2$$

соответственно.

Теорема 10.32. *Для всякой симметричной билинейной функции существует ортогональный базис.*

Доказательство. Доказывать теорему будем индукцией по $n = \dim V$. При $n = 1$ теорема очевидна. Пусть $n > 1$, тогда если $\alpha \equiv 0$, то теорема очевидна. Пусть $\alpha \not\equiv 0$, тогда (в силу формулы (92)) $q_\alpha \not\equiv 0$ и значит существует вектор $e_1 \in V$ такой, что $\alpha(e_1, e_1) = q_\alpha(e_1) \neq 0$. Значит, одномерное подпространство $U := \langle e_1 \rangle$ невырождено относительно α и, согласно Предложению 10.30, $V = U \oplus U^\perp$. Поскольку $\dim U^\perp = n - 1$, к этому подпространству

применимо предположение индукции: в нем существует базис $\{e_2, \ldots, e_n\}$, ортогональный относительно $\alpha|_{U^\perp}$. Поскольку вектор e_1 ортогонален подпространству $U^\perp$, а значит каждому из векторов $e_2, \ldots, e_n$, то $\{e_1, \ldots, e_n\}$ — ортогональный базис в V относительно α, и шаг индукции доказан. ∎

Задача 10.33. *Докажите, что если билинейная функция α не симметрична, то она не приводится к диагональному виду ни в каком базисе.*

10.3 Билинейные симметричные (квадратичные) функции над полями $\mathbb{C}$ и $\mathbb{R}$

Заметим, что до сих пор никаких условий (кроме $2 \neq 0$) мы на поле $\mathbb{K}$ не накладывали, то есть предыдущие результаты верны для любого поля характеристики, не равной 2. Дальнейшее более тонкое исследование проведем для случаев $\mathbb{K} = \mathbb{C}$ или $\mathbb{R}$. Общий случай сложен: для поля $\mathbb{Q}$, например, классификация квадратичных функций связана с тонкими вопросами теории чисел.

Итак, к настоящему моменту мы нашли базис $\{e_1, \ldots, e_n\}$ в V, в котором квадратичная функция имеет вид

$$q(v) = a_1 v_1^2 + \ldots + a_n v_n^2,$$

где $a_i = q(e_i)$. Путем перестановки базисных векторов можно добиться того, чтобы нулевые коэффициенты a_i (если они есть) стояли бы в конце.

Если $a_i \neq 0$, то замена $e_i \mapsto e_i' = \lambda e_i$, $\lambda \neq 0$ приводит к замене $a_i' = \lambda^2 a_i$, то есть a_i и a_i' отличаются умножением на квадрат ненулевого числа. Для $\mathbb{K} = \mathbb{C}$ все ненулевые числа являются такими квадратами, поэтому, умножая базисные векторы на подходящие ненулевые скаляры, можно добиться, чтобы в новом базисе

$$q(v) = v_1'^2 + \ldots + v_r'^2, \tag{94}$$

где $r = \operatorname{rk} \alpha$ (количество ненулевых a_i).

Для $\mathbb{K} = \mathbb{R}$ квадраты ненулевых чисел — в точности положительные числа, поэтому умножением базисного вектора на подходящее ненулевое число мы можем модуль $|a_i|$, $a_i \neq 0$ сделать равным 1, но при этом знак a_i изменить не можем. Поэтому для $\mathbb{K} = \mathbb{R}$ мы можем добиться, чтобы

$$q(v) = \sum_{i=1}^{k} v_i'^2 - \sum_{j=k+1}^{k+l} v_j'^2 \tag{95}$$

где $k + l = r = \operatorname{rk} \alpha$.

Определение 10.34. *Нормальным видом* квадратичной функции над полем $\mathbb{C}$ (соответственно над $\mathbb{R}$) называется вид (94) (соответственно (95)).

Предложение 10.35. *Для произвольной квадратичной функции q на векторном пространстве V над полем $\mathbb{C}$ (соответственно $\mathbb{R}$) существует базис в V, в котором она записывается в нормальном виде (94) (соответственно (95)).*

Переформулируем полученный результат в терминах матриц.

Следствие 10.36. *Для произвольной симметричной матрицы A с элементами из поля $\mathbb{C}$ (соответственно $\mathbb{R}$) существует невырожденная матрица C с элементами из соответствующего поля такая, что $C^TAC = A' = \operatorname{diag}(a_1, \ldots, a_n)$, где $a_i = 1$ или 0 в случае поля $\mathbb{C}$ и ± 1 или 0 в случае поля $\mathbb{R}$.*

Доказательство следует непосредственно из предыдущего Предложения и формулы (88). ■

За исключением тривиальных случаев, имеется много базисов, в котором данная квадратичная функция имеет нормальный вид. Возникает вопрос: однозначно ли он определен для данной квадратичной функции? Ясно, что путем перестановки базисных векторов можно менять порядок расположения диагональных элементов в матрице квадратичной функции, поэтому инвариантный смысл может иметь только общее количество тех или иных элементов в диагональном виде (единиц и нулей для $\mathbb{C}$, единиц, минус единиц и нулей для $\mathbb{R}$).

Ясно, что количество единиц в нормальном виде квадратичной функции над $\mathbb{C}$ равно ее рангу и поэтому не зависит от выбора базиса (см. Следствие 10.15). То же относится к сумме $k+l$ количества плюс и минус единиц (см. (95)) для нормального вида квадратичной функции над $\mathbb{R}$. Мы собираемся доказать более тонкий результат: числа k и l в нормальном виде (95) и по отдельности не зависят от базиса.

Итак, пусть $\mathbb{K} = \mathbb{R}$.

Определение 10.37. Вещественная квадратичная функция $q\colon V \to \mathbb{R}$ называется *положительно определенной*, если $q(v) > 0$ для любого $v \in V$, $v \neq 0$. Вещественная билинейная симметричная функция α называется *положительно определенной*, если соответствующая ей квадратичная функция q_α положительно определена. Аналогично определяются отрицательно определенные вещественные квадратичные и симметричные билинейные функции.

Вещественная квадратичная функция $q\colon V \to \mathbb{R}$ (и соответствующая ей билинейная симметричная функция) называется *положительно полуопределенной*, если $q(v) \geq 0$ для любого $v \in V$. Аналогично определяются отрицательно полуопределенные функции.

Заметим, что из положительной определенности α на V следует ее невырожденность; более того, поскольку ограничение $\alpha|_U$ положительно определенной функции α на произвольное подпространство $U \subset V$ положительно определено, то любое подпространство $U \subset V$ невырождено относительно α.

Помимо положительно и отрицательно (полу)определенных квадратичных функций, есть *неопределенные* функции, которые могут принимать как положительные, так и отрицательные значения. Такая функция используется, например, в математической модели специальной теории относительности (метрика Лоренца).

Заметим, что если $\dim V = n$, то положительно определенная квадратичная функция на V имеет нормальный вид $q(v) = \sum_{i=1}^{n} v_i^2$ и ее матрица в соответствующем (ортонормированном) базисе есть $A = E$. Тогда в любом другом базисе $A' = C^T A C = C^T C$, в частности, $\det A' = (\det C)^2 > 0$. Отсюда следует важный вывод: *определитель матрицы положительно определенной функции в произвольном базисе положителен*. Более общо, *знак определителя невырожденной вещественной квадратичной функции не зависит от базиса.*

Теорема 10.38. *Число k в нормальном виде (95) произвольной вещественной квадратичной функции q есть максимальная размерность подпространства, на котором q положительно определена.*

Доказательство. Ясно, что q положительно определена на линейной оболочке $\langle e_1, \ldots, e_k \rangle$ первых k векторов того базиса, в котором она имеет вид (95). Пусть U — произвольное подпространство в V на котором q положительно определена и $W := \langle e_{k+1}, \ldots, e_n \rangle$. Так как $q(w) \leq 0$ для произвольного $w \in W$, а $q(u) > 0$ для $u \in U$, $u \neq 0$, то $U \cap W = 0$, откуда $\dim U \leq k$ (в самом деле, поскольку сумма $U + W$ — подпространство в V, то $\dim (U + W) = \dim U + n - k \leq \dim V = n$). ∎

Аналогично доказывается, что число l в нормальном виде (95) равно максимальной размерности подпространства, на котором q отрицательно определена. (Для доказательства последнего факта можно воспользоваться также следующим очевидным соображением: q положительно определена тогда и только тогда, когда $-q$ отрицательно определена).

Следствие 10.39. *("Закон инерции"). Числа k и l в нормальном виде (95) вещественной квадратичной функции q не зависят от выбора базиса, в котором функция q имеет нормальный вид.*

Числа $r_+ := k$ и $r_- := l$ называются соответственно *положительным* и *отрицательным* индексами инерции вещественной квадратичной функции q. Они связаны соотношением $r_+ + r_- = r = \operatorname{rk} q$. Набор (r_+, r_-) называют еще *сигнатурой* вещественной квадратичной функции q (или соответствующей билинейной симметричной функции α_q).

Ранг в случае комплексной, а также положительный и отрицательный индексы инерции в случае вещественной квадратичной функции на n-мерном пространстве V являются полными наборами инвариантов в следующем смысле: если даны две такие функции с одинаковыми наборами инвариантов, то существует замена базиса, переводящая первую функцию во вторую.

Пример 10.40. Найдем положительный и отрицательный индексы инерции для вещественной квадратичной функции $q(v) = v_1v_2$ на двумерном пространстве. Производя замену базиса $e_1' = e_1 + e_2,\ e_2' = e_1 - e_2$ (или соответствующую ей замену координат $v_1 = v_1' + v_2',\ v_2 = v_1' - v_2'$) приводим ее к нормальному виду $q(v) = v_1'^2 - v_2'^2$. Таким образом, $r_+ = 1 = r_-$.

Задача 10.41. *Пусть $A(t)$ — семейство вещественных симметричных матриц, непрерывно зависящих от параметра $t \in \mathbb{R}$. Известно, что при $t > t_0$ матрицы положительно определены. Докажите, что матрица $A(t_0)$ положительно полуопределена.*

Решение. Из условия следует, что при $t > t_0$ $x^TA(t)x > 0$ для любого $0 \neq x \in \mathbb{R}^n$. В силу того, что для любого $x \in \mathbb{R}^n$ функция

$$f_x\colon \mathbb{R} \to \mathbb{R}, \quad f_x(t) := x^TA(t)x$$

непрерывна, получаем, что $\lim_{t\to t_0+} f_x(t) = f_x(t_0) \geq 0$. ■

Задача 10.42. *Найдите положительный и отрицательный индексы инерции квадратичной функции $q(x) = \sum_{1\leq i<j\leq n} x_ix_j$ на n-мерном пространстве.*

Решение. Заметим, что

$$2q(x) = (x_1 + x_2 + \ldots + x_n)^2 - x_1^2 - x_2^2 - \ldots - x_n^2.$$

Легко видеть, что ограничение q на одномерное подпространство, заданное системой $x_1 = x_2 = \ldots = x_n$, положительно определено, поэтому положительный индекс инерции не меньше 1, а ограничение q на $n-1$-мерное подпространство, заданное уравнением $x_1 + \ldots + x_n = 0$, отрицательно определено. Значит, положительный индекс инерции равен 1, а отрицательный — $n-1$. ■

Не следует думать, что если вещественная квадратичная функция положительно определена на двух подпространствах, то она обязательно положительно определена и на их сумме. В частности, Теорема 10.38 не утверждает, что среди всех подпространств, на которых квадратичная функция положительно определена, существует максимальное в том смысле, что оно содержит все такие подпространства.

Задача 10.43. *Предположим, что вещественное векторное пространство V, на котором задана квадратичная форма $q\colon V \to \mathbb{R}$, разложено в прямую сумму $V = U \oplus W$ своих подпространств, причем ограничения $q|_U$ и $q|_W$ положительно определены. Следует ли отсюда, что сама q положительно определена?*

Решение. Ответ отрицательный, причем для построения контрпримера достаточно рассмотреть случай, когда двумерное пространство V разложено в прямую сумму одномерных подпространств. Рассуждать при построении контрпримера можно следующим образом. Выберем базис $\{e_1, e_2\}$ в V такой, что $U = \langle e_1\rangle$, $W = \langle e_2\rangle$. То, что ограничения q на

указанные подпространства положительно определены означает, что на главной диагонали в матрице q в базисе $\{e_1,\, e_2\}$ стоят положительные числа, скажем, равные 1. Требуется выбрать элементы вне главной диагонали так, чтобы полученная симметричная матрица не была положительно определенной, чего, конечно, легко добиться, положив эти элементы равными произвольному числу больше либо равному 1.

Другой вариант рассуждения использует аргумент "по непрерывности". А именно, пусть ограничение q на $\langle e_1\rangle$ положительно определено. Рассмотрим вектор $e_2' := e_1 + \varepsilon e_2$, где положительное число ε достаточно мало. Ясно, что линейная оболочка $\langle e_1,\, e_2'\rangle$ совпадает с $V = \langle e_1,\, e_2\rangle$, в то же время из непрерывности q и $q(e_1) > 0$ следует, что и $q(e_2') > 0$ при достаточно малых ε. Это показывает, для любой квадратичной функции, у которой положительный индекс инерции больше нуля, существует базис, на всех векторах которого она принимает только положительные значения. ■

Задача 10.44. *Известно, что квадратичная функция q на n-мерном вещественном пространстве на всех базисных векторах некоторого базиса принимает положительные значения. Что можно сказать про ее положительный индекс инерции?*

Решение. Очевидно, что положительный индекс инерции не меньше 1, оказывается, он может быть в точности равен 1. Приведем соответствующий пример. Пусть $\{e_1, \ldots, e_n\}$ — ортогональный базис для q такой, что $q(e_1) = 1$, $q(e_i) = -1$ при $i = 2, \ldots, n$. Перейдем к новому базису $\{e_1, \varepsilon e_2 + e_1, \ldots, \varepsilon e_n + e_1\}$. При этом $q(\varepsilon e_i + e_1) = 1 - \varepsilon^2 > 0$, если модуль ε достаточно мал. Отсюда легко получить, что r_+ может принимать значения от 1 до n. ■

Задача 10.45. *Известно, что квадратичная функция q на n-мерном вещественном пространстве V имеет матрицу, все диагональные элементы которой равны нулю. Определите наибольшую возможную размерность подпространства $U \subset V$ такого, что на нем данная квадратичная функция положительно определена.*

Решение. Размерность U — положительный индекс инерции q. Ясно, что $\dim U \leq n - 1$. Покажем, что существует q с положительным индексом инерции, равным $n - 1$, и при этом имеющая в некотором базисе матрицу с нулевыми элементами на главной диагонали. Пусть $q(v) := -v_1^2 + v_2^2 + \ldots + v_n^2$ в некотором базисе $\{e_1, \ldots, e_n\}$. Для доказательства достаточно заметить, что "изотропный конус"

$$\{v \in V \mid q(v) = 0\} \subset V$$

содержит некоторый базис пространства V, поскольку в таком базисе матрица q имеет требуемый вид. Действительно, векторы $e_1 + e_2$ и $e_1 - e_2$ принадлежат изотропному конусу и через них выражается e_1. Далее, поскольку векторы $e_1 + e_k,\ 2 \leq k \leq n$ принадлежат изотропному конусу, то через них и через e_1 выражаются оставшиеся векторы $e_k,\ 2 \leq k \leq n$. ■

Задача 10.46. *Пусть α — невырожденная симметричная билинейная функция на пространстве V, имеющая отрицательный индекс инерции, равный 1, и $\alpha(v,v) < 0$ для некоторого $v \in V$. Докажите, что ограничение α на любое подпространство, содержащее v, невырождено.*

Решение. Так как подпространство $\langle v\rangle \subset V$ невырождено относительно α, то $V = \langle v\rangle \oplus \langle v\rangle^{\perp}$. Из условия следует, что ограничение α на $\langle v\rangle^{\perp} \subset V$ положительно определено.

Пусть $v \in U \subset V$ — подпространство. Тогда ортогональное дополнение к $\langle v\rangle \subset U$ есть $\langle v\rangle_U^{\perp} = \langle v\rangle^{\perp} \cap U$ и $U = \langle v\rangle \oplus \langle v\rangle_U^{\perp}$. Из этого легко следует, что сумма положительного и отрицательного индексов инерции ограничения α на U равно $\dim U$, то есть подпространство U невырождено. ■

10.4 Алгоритмы приведения к нормальному виду

Приведем классические алгоритмы отыскания ортогональных базисов.

Во-первых, опишем **метод Лагранжа** — приведение квадратичной функции к сумме квадратов. Пусть

$$q(x_1,\dots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j, \quad a_{ij} = a_{ji}$$

— квадратичная функция над полем $\mathbb{K}$ характеристики $\neq 2$. Следующая процедура дает удобный практический способ отыскания линейной невырожденной замены переменных x_i (а значит и замены базиса), приводящей q к сумме квадратов (с коэффициентами).

Случай 1. *Существует ненулевой диагональный коэффициент.* Перенумеровав переменные, мы можем считать, что $a_{11} \neq 0$. Тогда

$$q(x_1,\dots x_n) = a_{11}x_1^2 + x_1(2a_{12}x_2 + \dots + 2a_{1n}x_n) + q'(x_2,\dots,x_n),$$

где q' — квадратичная функция от $\leq n-1$ переменных. Выделяя полный квадрат, находим

$$q(x_1,\dots,x_n) = a_{11}\left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n\right)^2 + q''(x_2,\dots,x_n),$$

где q'' — новая квадратичная функция от $\leq n-1$ переменных. Полагая

$$y_1 = x_1 + a_{11}^{-1}(a_{12}x_2 + \dots + a_{1n}x_n), \quad y_2 = x_2,\ \dots,\ y_n = x_n,$$

мы получаем в новых переменных функцию

$$a_{11}y_1^2 + q''(y_2,\dots,y_n),$$

и следующий шаг алгоритма состоит в применении его к q''.

Случай 2. *Все диагональные коэффициенты равны нулю.* Если вообще $q = 0$, то делать ничего не нужно: $q = \sum_{i=1}^{n} 0 \cdot x_i^2$. Иначе, перенумеровав переменные, можно считать, что $a_{12} \neq 0$. Тогда

$$q(x_1,\dots,x_n) = 2a_{12}x_1x_2 + x_1l_1(x_3,\dots,x_n) + x_2l_2(x_3,\dots,x_n) + q'(x_3,\dots,x_n),$$

где l_1, l_2 — линейные функции, а q' — квадратичная. Положим

$$x_1 = y_1 + y_2, \quad x_2 = y_1 - y_2, \quad x_i = y_i, \quad i \geq 3.$$

В новых переменных функция q приобретает вид

$$2a_{12}(y_1^2 - y_2^2) + q''(y_1, y_2, \ldots, y_n),$$

где q'' не содержит членов с y_1^2, y_2^2. Поэтому к q в новых переменных можно применить способ выделения полного квадрата (случай 1 выше) и снова свести задачу к меньшему числу переменных. Последовательное применение этих шагов приведет функцию к виду $\sum_{i=1}^{n} a_i z_i^2$. Окончательная линейная замена переменных будет невырожденной, так как таковы все промежуточные замены.

Последняя замена переменных $u_i = \sqrt{|a_i|}z_i$ при $a_i \neq 0$ в случае $\mathbb{K} = \mathbb{R}$ и $u_i = \sqrt{a_i}z_i$ при $a_i \neq 0$ в случае $\mathbb{K} = \mathbb{C}$ приведет функцию к сумме квадратов с коэффициентами 0, ± 1 или 0, 1.

Во-вторых, опишем **метод элементарных преобразований**. Пусть нам дана симметричная матрица A; нужно найти такую невырожденную матрицу C, что матрица $A' = C^T AC$ (см. формулу (88)) диагональна.

Как мы знаем, любую невырожденную матрицу можно представить в виде произведения элементарных. Посмотрим, что из себя представляет преобразование $A \mapsto S^T AS$, где S — элементарная матрица. Например, рассмотрим случай элементарных матриц $P_{ij}(\lambda) = E + \lambda E_{ij}$ (см. (10)), отвечающих преобразованиям типа I — прибавлению к i-й строке j-й строки, умноженной на λ. Легко видеть, что матрица $P_{ij}(\lambda)$ получается из единичной также прибавлением к j-му столбцу i-го столбца, умноженного на λ, поэтому умножение матрицы A на $P_{ij}(\lambda)$ справа отвечает соответствующему преобразованию столбцов матрицы A.

Заметим, что $P_{ij}(\lambda)^T = P_{ji}(\lambda)$. Таким образом, для $S = P_{ij}(\lambda)$ преобразование $A \mapsto S^T AS$ отвечает прибавлению к j-й строке i-й строки, умноженной на λ с последующим прибавлением к j-му столбцу i-го, умноженного на λ.

Аналогичное утверждение верно и для произвольной элементарной матрицы S: $A \mapsto S^T AS$ отвечает некоторому элементарному преобразованию строк матрицы A с последующим аналогичным преобразованием столбцов полученной матрицы[52]. Заметим, что при таких "сдвоенных" элементарных преобразованиях сохраняется симметричность матрицы A.

Опишем теперь шаг алгоритма. Пусть дана симметричная матрица A порядка n.

1. Основной случай. *Если* $a_{11} \neq 0$, то вычитая из строк, начиная со второй, нужную кратность первой строки и проделывая аналогичные преобразования со столбцами, полу-

[52] Данный результат также можно получить, используя равенство $(AS)^T = S^T A^T$.

чаем блочно-диагональную матрицу $\begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}$, где A' — симметричная матрица порядка $n-1$.

2. Особый случай. *Если* $a_{11} = 0$, *но* $a_{1k} \neq 0$ *для некоторого* $2 \leq k \leq n$, то при условии $a_{kk} \neq 0$ поменяем местами 1-ю и k-ю строки и 1-й и k-й столбцы (это соответствует перестановке 1-го и k-го базисных векторов), тогда придем к ситуации основного случая. Если же $a_{kk} = 0$, то к 1-й строке прибавим k-ю и к 1-му столбцу прибавим k-й, тогда получим $a'_{11} = 2a_{1k} \neq 0$ и снова окажемся в ситуации основного случая.

В результате мы получим диагональную матрицу $A' = \operatorname{diag}(b_1, \ldots, b_n)$. Далее при $b_i \neq 0$ нужно i-е строку и столбец поделить на $\sqrt{|b_i|}$ в вещественном или на $\sqrt{b_i}$ в комплексном случае.

Пример 10.47. Найти нормальный вид билинейной функции с матрицей

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Решим задачу с помощью метода элементарных преобразований. Имеет место особый случай, поэтому прибавим к первой строке вторую строку и к первому столбцу второй столбец, получим матрицу

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix},$$

далее вычитая из второй строки и второго столбца половину первой строки и первого столбца соответственно, получим матрицу

$$\begin{pmatrix} 2 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix},$$

далее деля первую строку и столбец на $\sqrt{2}$, а вторую строку и столбец — умножая на $\sqrt{2}$, получим

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

что дает нормальный вид для поля $\mathbb{R}$. В случае поля $\mathbb{C}$ нужно вторую строку и столбец умножить на i, при этом получится единичная матрица.

Чтобы получить матрицу перехода, нужно все преобразования столбцов применить к единичной матрице.

Третий алгоритм нахождения ортогональных базисов — **алгоритм Грама-Шмидта** — мы опишем в одном из следующих параграфов.

10.5 Критерий Сильвестра

Цель этого параграфа — доказательство критерия положительной определенности вещественной квадратичной (симметричной билинейной) функции.

Пусть V — n-мерное вещественное векторное пространство, α — билинейная симметричная функция, $\{e_1, \dots, e_n\}$ — базис в V и A — матрица α в этом базисе. Очевидно, что если α положительно определена, то ее ограничение $\alpha|_U$ на любое подпространство $U \subset V$ также положительно определено. Значит, для любого набора $i_1, \dots, i_k$, $1 \le i_1 < \dots < i_k \le n$ определитель подматрицы матрицы A, образованной пересечениями строк и столбцов с этими номерами, положителен, поскольку сама подматрица является матрицей ограничения $\alpha|_{\langle e_{i_1}, \dots, e_{i_k}\rangle}$ в базисе $\{e_{i_1}, \dots, e_{i_k}\}$ (см. абзац перед Теоремой 10.38).

Таким образом, все миноры матрицы положительно определенной квадратичной функции описанного выше вида положительны. Будет ли это условие достаточным для того, чтобы квадратичная функция с матрицей A была бы положительно определена? Оказывается, для положительной определенности A уже достаточно положительности ее так называемых *угловых миноров* — определителей подматриц порядков от 1 до n, стоящих в левом верхнем углу матрицы A (отвечающих ограничениям α на линейные оболочки $\langle e_1, \dots, e_k\rangle$, $1 \le k \le n$).

Теорема 10.48. *(Критерий Сильвестра). Вещественная симметричная билинейная функция $\alpha\colon V \times V \to \mathbb{R}$, имеющая матрицу A в некотором базисе, положительно определена тогда и только тогда, когда все угловые миноры матрицы A положительны.*

Доказательство. Необходимость условия положительности главных миноров уже доказана выше.

Достаточность этого условия докажем индукцией по $n = \dim V$. Случай $n = 1$ очевиден. Пусть результат верен для билинейных функций на пространствах размерности, не превосходящей $n-1$, докажем что он верен и для пространств размерности n. Пусть A — вещественная симметричная матрица порядка n, у которой все n штук угловых миноров положительны. Покажем, что соответствующая билинейная функция α положительно определена.

Применяя предположение индукции получаем, что ограничение $\alpha|_{\langle e_1, \dots, e_{n-1}\rangle}$ положительно определено. Значит, по Теореме 10.38 положительный индекс инерции $r_+ = r_+(\alpha)$ не меньше $n-1$. Так как из условия следует, что α невырождена, то $r_+ + r_- = \operatorname{rk}\alpha = n$, и для отрицательного индекса инерции возможны варианты $r_- = 0$ (в этом случае α положительно определена) или $r_- = 1$. В последнем случае нормальный вид α есть $\sum_{i=1}^{n-1} u_i v_i - u_n v_n$, и определитель матрицы A отрицателен (поскольку знак определителя матрицы билинейной функции не зависит от базиса), что противоречит условию. Значит, единственная возможность $r_+ = n$, $r_- = 0$, то есть α положительно определена и шаг индукции доказан. ∎

Задача 10.49. *Докажите, что вещественная симметричная матрица A отрицательно определена тогда и только тогда, когда знаки ее угловых миноров $\delta_1, \delta_2, \ldots, \delta_n$ чередуются, начиная со знака "$-$". (Указание: воспользуйтесь тем, что q отрицательно определена $\Leftrightarrow -q$ положительно определена).*

Задача 10.50. *Верно ли, что у матрицы положительно полуопределенной квадратичной функции все угловые миноры неотрицательны? А в обратную сторону?*

Решение. Приведем решение части задачи. Рассмотрим пример квадратичной функции с матрицей

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & a \end{pmatrix},$$

$a < 1$. У нее следующий набор угловых миноров $\delta_1 = 1$, $\delta_2 = 0$, $\delta_3 = 0$. Соответствующая ей квадратичная функция имеет вид

$$q(x) = (x_1 + x_2 + x_3)^2 + (a-1)x_3^2.$$

Легко видеть, что она не является знакоопределенной (например, она отрицательно полуопределена на подпространстве $U := \{x \mid x_1 + x_2 + x_3 = 0\}$. ■

Задача 10.51. *Предположим, что для матрицы A вещественной квадратичной функции q на трехмерном пространстве угловые миноры δ_1, δ_2, δ_3 имеют следующий набор знаков: $+$, 0, $-$ соответственно. Чему равны положительный r_+ и отрицательный r_- индексы инерции q?*

Решение. Заметим, что так как $\delta_3 \neq 0$, то $r := \operatorname{rk} q = 3$. Мы также знаем, что $r_+ + r_- = r$. Кроме того, знак определителя матрицы квадратичной функции не меняется при замене базиса, поэтому из $\delta_3 < 0$ следует, что отрицательный индекс инерции нечетен (количество минус единиц в нормальном виде нечетно). Если $r_- = 3$, то функция была бы отрицательно определенной, что противоречит критерию Сильвестра (Задаче 10.49). Значит, единственная возможность $r_- = 1$, $r_+ = 2$. Матрица

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

показывает, что данный набор значений главных миноров действительно реализуется. ■

Замечание 10.52. Пусть A — матрица квадратичной формы q в некотором базисе n-мерного вещественного пространства V. Мы знаем, что при произвольной замене базиса в V ранг A, а также знак $\delta_n = \det A$ (при условии, что он не равен нулю), не меняются. В то же время, если q не является положительно или отрицательно определенной, то

знаки угловых миноров $\delta_1, \ldots, \delta_{n-1}$ (и условие их равенства или неравенства нулю) могут измениться. Например,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

— матрицы одной и той же квадратичной функции в разных базисах. Мы можем гарантировать сохранение знаков всех δ_i только при треугольных заменах координат (как в алгоритме Грама-Шмидта из следующего параграфа).

Задача 10.53. *Даны матрицы* $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ *и* $B = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. *Существует ли такая вещественная матрица* C, *что* $B = C^T AC$?

Решение. Найдем индексы инерции данных матриц (интерпретируя их как матрицы вещественных квадратичных функций относительно некоторых базисов). Это можно сделать, используя сдвоенные элементарные преобразования строк и столбцов, но проще рассуждать следующим образом. Набор главных миноров матрицы A имеет знаки $+, +, -$, поэтому ее положительный индекс инерции $r_+(A)$ не меньше двух (левый верхний угол порядка 2 — положительно определенная матрица), а ранг A равен 3, откуда $r_+(A) + r_-(A) = 3$, но A не является положительно определенной, значит, единственная возможность $r_+(A) = 2$, $r_-(A) = 1$.

Аналогично, набор главных миноров матрицы B имеет знаки $+, -, -$, но переставляя второй и третий базисный векторы, получим матрицу $B' = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ той же функции в другом базисе с тем же набором знаков, что и A, поэтому положительный и отрицательный индексы инерции у B такие же как у A, и обе они приводятся заменами базисов к нормальному виду $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, откуда следует, что матрица C из условия существует. ■

Кстати, не все варианты наборов знаков главных миноров реализуются. Например, для матрицы квадратичной формы на двумерном пространстве запрещен набор $\delta_1 = 0,\ \delta_2 > 0$. Вот несколько более сложный пример.

Задача 10.54. *Может ли матрица* A *вещественной квадратичной функции* q *на трехмерном пространстве* V *иметь угловые миноры* $\delta_1 > 0$, $\delta_2 = 0$, $\delta_3 > 0$?

Решение. Из условия легко следует, что $r_+ + r_- = 3$, функция q не является знакоопределенной и r_- четно, что оставляет только возможность $r_+ = 1$, $r_- = 2$. Попробуем доказать, что последний вариант также невозможен.

Пусть матрица A дана в базисе $\{e_1, e_2, e_3\}$; рассмотрим ограничение q на линейную оболочку $U := \langle e_1, e_2 \rangle$. В базисе $\{e_1, e_2\}$ матрица $q|_U$ имеет главные миноры δ_1, δ_2, откуда легко видеть, что индексы

инерции $q|_U$ суть $r'_+ = 1, r'_- = 0$. Таким образом, при переходе от двумерного подпространства U к пространству V отрицательный индекс инерции увеличивается сразу на 2, что, очевидно, невозможно. ■

Задача 10.55. *При каком значении параметра $a \in \mathbb{R}$ матрицы*

$$\begin{pmatrix} 1 & 4-a-a^2 \\ 2 & -1 \end{pmatrix} \quad \begin{pmatrix} -a-1 & 3 \\ 3 & -5 \end{pmatrix}$$

являются матрицами одной и той же билинейной функции $b\colon V \times V \to \mathbb{R}$ в разных базисах?

Задача 10.56. *(Р.Н. Карасев) Докажите, что если сеть из резисторов подключена в некоторых точках к источникам напряжения, то токи в этой сети будут определены однозначно.*

Подсказка. Выпишите квадратичную форму рассеиваемой сетью мощности

$$P = \sum_{i \neq j} (u_i - u_j)^2 / R_{ij}$$

(при бесконечном сопротивлении R_{ij} слагаемое пропускается) и перепишите условия Кирхгофа на токи (сумма входящих в узел i токов равна сумме исходящих) как $\frac{\partial P}{\partial u_i} = 0$. Проверьте, что если сеть связная и хотя бы одно значение u_i зафиксированно (подключено к источнику напряжения), то квадратичная часть многочлена P является положительно определённой квадратичной формой, и заметьте, что поэтому P имеет единственный минимум и вообще единственную точку, где обращаются в нуль частные производные по нефиксированным переменным. Несвязную сеть разбейте на не связанные между собой связные сети. Не подключенные к источникам напряжения сети проанализируйте аналогично.

10.6 Алгоритм Грама-Шмидта и метод Якоби

В данном параграфе мы изложим очень полезный алгоритм ортогонализации Грама-Шмидта и применим его для доказательства теоремы Якоби, обобщающей критерий Сильвестра и Задачу 10.49.

Для изложения алгоритма нам потребуются понятия ортогональной проекции и ортогональной составляющей. Определим, что это такое.

Напомним (см. Предложение 10.30), что если подпространство $U \subset V$ невырождено относительно α, то $V = U \oplus U^\perp$. Значит, любой вектор $v \in V$ единственным образом представляется в виде суммы $u + w$, где $u \in U$, $w \in U^\perp$. Вектор u называется *ортогональной проекцией* v на U и обозначается $pr_U(v)$, а вектор w — *ортогональной составляющей* вектора v относительно подпространства U и обозначается $ort_U(v)$.

То есть, в нашей прежней терминологии, $pr_U(v)$ — проекция v на подпространство U параллельно его ортогональному дополнению $U^\perp$, а $ort_U(v)$ — проекция v на $U^\perp$ параллельно U.

Пусть в конечномерном пространстве V фиксирован базис $\{e_1, \dots, e_n\}$. Тогда мы имеем цепочку вложенных подпространств

$$0 = V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \dots \subsetneq V_{n-1} \subsetneq V_n = V,$$

где $V_k := \langle e_1, \dots, e_k \rangle$.

Теорема 10.57. *Пусть на V задана билинейная симметричная функция α, причем каждое из подпространств V_k предполагается невырожденным относительно α. Тогда в V существует единственный базис $\{f_1, \dots, f_n\}$ такой, что*

1) $\{f_1, \dots, f_n\}$ ортогонален относительно α и

2) *матрица перехода C от $\{e_1, \ldots, e_n\}$ к $\{f_1, \ldots, f_n\}$ верхняя треугольная с единицами на главной диагонали (в частности, $\langle f_1, \ldots, f_k\rangle = V_k$, $1 \le k \le n$).*

Такой базис $\{f_1, \ldots, f_n\}$ называется *ортогонализацией* базиса $\{e_1, \ldots, e_n\}$.

Доказательство. Ортогонализацию $\{f_1, \ldots, f_n\}$ будем строить пошагово — сначала построим ортогонализацию $\{f_1\}$ базиса $\{e_1\}$ в V_1, затем дополним ее вектором f_2 до ортогонализации $\{f_1, f_2\}$ базиса $\{e_1, e_2\}$ в V_2 и т.д. При этом для каждого k, $1 \le k \le n$ матрица перехода C_k от базиса $\{e_1, \ldots, e_k\}$ к базису $\{f_1, \ldots, f_k\}$ в V_k будет верхняя треугольная с единицами на главной диагонали. Очевидно, что каждая из матриц C_k тогда будет левым верхним углом в C_{k+1} (и в $C = C_n$). Читателю рекомендуется разобраться в геометрическом смысле проводимых построений (при необходимости рисовать картинки).

Пусть $k = 1$. Так как матрица перехода $C_1 = (1)$, то $f_1 = e_1$.

Пусть $k = 2$. Подпространство $V_1 \subset V$ по условию невырождено, поэтому $V = V_1 \oplus V_1^\perp$. Пусть $e_2 = v_1 + f_2$ — соответствующее представление вектора e_2, где $v_1 = pr_{V_1} e_2 \in V_1$, $f_2 = ort_{V_1} e_2$.

Мы утверждаем, что вектор f_2 — искомый. Действительно, поскольку $f_2 \in V_1^\perp$, то $f_2 \perp f_1$, кроме того, поскольку $f_2 = e_2 - v_1$, где v_1 лежит в $V_1 = \langle e_1\rangle$, то матрица перехода C_2 от $\{e_1, e_2\}$ к $\{f_1, f_2\}$ имеет вид $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, то есть является верхней треугольной с единицами на главной диагонали.

Легко видеть, что вектор f_2 с указанными свойствами единственный. В самом деле, пусть f_2' — еще один вектор с требуемыми свойствами. Тогда $f_2' = e_2 - v_1'$, где $v_1' \in V_1$. Имеем $f_2 - f_2' = v_1' - v_1 \in V_1 \cap V_1^\perp$, что равно нулю, поскольку подпространство V_1 по условию невырождено.

Заметим, что $\langle f_1, f_2\rangle = V_2$.

Предположим, что уже построены векторы $f_1, \ldots, f_k$, составляющие ортогональный базис в V_k, причем матрица перехода C_k от $\{e_1 \ldots, e_k\}$ к $\{f_1, \ldots, f_k\}$ верхняя треугольная с единицами на главной диагонали. Подпространство $V_k \subset V$ невырождено, поэтому $V = V_k \oplus V_k^\perp$. Пусть $e_{k+1} = v_k + f_{k+1}$ — соответствующее представление вектора e_{k+1}, где $v_k = pr_{V_k} e_{k+1} \in V_k$, $f_{k+1} = ort_{V_k} e_{k+1} \in V_k^\perp$.

Мы утверждаем, что вектор f_{k+1} — искомый. Действительно, так как $f_{k+1} \in V_k^\perp$, то f_{k+1} ортогонален векторам $f_1, \ldots, f_k$ и, кроме того, $f_{k+1} = e_{k+1} - v_k$, где v_k лежит в $V_k = \langle e_1, \ldots, e_k\rangle$, поэтому в $k+1$-м столбце матрицы C_{k+1} внизу стоит 1, то есть матрица перехода C_{k+1} от базиса $\{e_1 \ldots, e_{k+1}\}$ к $\{f_1, \ldots, f_{k+1}\}$ снова верхняя треугольная с единицами на главной диагонали.

Легко видеть, что вектор f_{k+1} с требуемыми свойствами единственный. Действительно, пусть f_{k+1}' — еще один вектор с нужными свойствами. Тогда $f_{k+1}' = e_{k+1} - v_k'$, где $v_k' \in V_k$, откуда $f_{k+1} - f_{k+1}' = v_k' - v_k \in V_k \cap V_k^\perp$, что равно нулю в силу невырожденности подпространства V_k.

Заметим, что $\langle f_1, \ldots, f_{k+1}\rangle = V_{k+1}$.

Продолжая указанный алгоритм, получаем ортогональный базис $\{f_1, \ldots, f_n\}$ в пространстве V с нужными свойствами. ■

Из доказанной Теоремы мы сейчас выведем важное следствие. Пусть при тех же условиях, что и в Теореме, A — матрица α в базисе $\{e_1, \ldots, e_n\}$. Пусть A_k, $1 \le k \le n$ — подматрица матрицы A порядка k, стоящая в левом верхнем углу. Очевидно, что A_k — матрица ограничения $\alpha|_{V_k}$ в базисе $\{e_1, \ldots, e_k\}$ пространства V_k. Пусть $\delta_k := \det A_k$ — угловые миноры матрицы A. По условию все они отличны от нуля. Введем еще $\delta_0 := 1$.

Следствие 10.58. *В введенных выше обозначениях*

$$q_\alpha(f_k) := \alpha(f_k, f_k) = \frac{\delta_k}{\delta_{k-1}},\ 1 \le k \le n.$$

Доказательство. Для $1 \le k \le n$ имеем

$$\operatorname{diag}(q_\alpha(f_1), \ldots, q_\alpha(f_k)) = C_k^T A_k C_k,$$

откуда, переходя к определителям и используя то, что матрицы C_k верхние треугольные с единицами на главной диагонали, получаем требуемое. ■

Пусть теперь A — матрица вещественной симметричной функции α в некотором базисе.

Следствие 10.59. *(Метод Якоби). При условии, что все главные миноры $\delta_1, \dots, \delta_n$ матрицы A отличны от нуля, отрицательный индекс инерции α равен числу перемен знака в последовательности $\delta_0, \delta_1, \dots, \delta_n$.*

Доказательство. Из предыдущего Следствия вытекает, что число перемен знака равно числу отрицательных коэффициентов в диагональном виде α. ■

Из доказанного Следствия легко выводится критерий Сильвестра а также его обобщение на случай отрицательно определенных функций (см. Задачу 10.49).

А что будет, если в последовательности главных миноров есть нули? Оказывается, результат теоремы Якоби сохраняется, если нули изолированные (то есть нет двух идущих подряд нулей). Например, рассмотрим ситуацию $\delta_k > 0$, $\delta_{k+1} = 0$, $\delta_{k+2} < 0$. Пусть (r_+^k, r_-^k) — сигнатура для ограничения на k-мерное координатное подпространство, причем так как $\delta_k \neq 0$, то $r_+^k + r_-^k = k$. При переходе к $k+1$-мерному координатному пространству индексы инерции уменьшиться не могут, в то же время $r_+^{k+1} + r_-^{k+1} < k+1$, так как $\delta_{k+1} = 0$, поэтому $r_+^{k+1} = r_+^k$, $r_-^{k+1} = r_-^k$. При переходе к $k+2$-мерному пространству и положительный, и отрицательный индексы инерции могут увеличиться максимум на 1; с другой стороны, так как $\delta_{k+2} \neq 0$, то $r_+^{k+2} + r_-^{k+2} = k+2$, поэтому $r_+^{k+2} = r_+^{k+1} + 1$, $r_-^{k+2} = r_-^{k+1} + 1$, то есть отрицательный индекс инерции увеличился на 1. (Возможна ли ситуация $\delta_k > 0$, $\delta_{k+1} = 0$, $\delta_{k+2} > 0$?)

10.7 Кососимметрические билинейные функции

Пусть f_1, $f_2 \colon V \to \mathbb{K}$ — линейные функции, $f_i \in V^*$. Легко проверить, что функция

$$\alpha = f_1 \otimes f_2, \quad (f_1 \otimes f_2)(u, v) := f_1(u) f_2(v) \ \forall\, u, v \in V$$

билинейна и имеет ранг 1, и любая билинейная функция ранга 1 имеет такой вид (см. Пример 10.17 и Задачу 10.18). Пусть $\beta = \alpha^-$ — проекция α на подпространство кососимметрических функций (см. формулу (89)), тогда

$$\beta(u, v) = \frac{1}{2}(\alpha(u, v) - \alpha(v, u)) = \frac{1}{2}(f_1(u) f_2(v) - f_1(v) f_2(u)) = \frac{1}{2}\begin{vmatrix} f_1(u) & f_1(v) \\ f_2(u) & f_2(v) \end{vmatrix}.$$

Для произвольной пары линейных функций $f_1, f_2 \in V^*$ определим билинейную кососимметрическую функцию $f_1 \wedge f_2$ формулой $(f_1 \wedge f_2)(u, v) := \begin{vmatrix} f_1(u) & f_1(v) \\ f_2(u) & f_2(v) \end{vmatrix} \ \forall\, u, v \in V$. В тензорных обозначениях $f_1 \wedge f_2 = f_1 \otimes f_2 - f_2 \otimes f_1$ (ср. (91)).

Напомним, что пространство всех билинейных функций на линейном пространстве V мы обозначили $\mathcal{B}(V)$, а подпространство в $\mathcal{B}(V)$, состоящее из кососимметрических билинейных функций — $\mathcal{B}^-(V)$. Если $\dim V = n$, то $\dim \mathcal{B}(V) = n^2$ и $\dim \mathcal{B}^-(V) = \frac{n(n-1)}{2}$.

Предложение 10.60. *Если $\{\varepsilon_1, \dots, \varepsilon_n\}$ образуют базис в V^*, то $\{\varepsilon_i \wedge \varepsilon_j \mid 1 \leq i < j \leq n\}$ — базис в $\mathcal{B}^-(V)$.*

Доказательство. Мы знаем (см. Задачу 7.105), что произвольный базис в V^* биортогонален некоторому базису в V. Пусть $\{\varepsilon_1, \dots, \varepsilon_n\}$ биортогонален базису $\{e_1, \dots, e_n\}$ в V. Тогда для $1 \leq i < j \leq n$ имеем

$$(\varepsilon_i \wedge \varepsilon_j)(e_k, e_l) = \begin{vmatrix} \varepsilon_i(e_k) & \varepsilon_i(e_l) \\ \varepsilon_j(e_k) & \varepsilon_j(e_l) \end{vmatrix} = \delta_{ik}\delta_{jl} - \delta_{il}\delta_{jk} = \begin{cases} 1, & \text{если } k = i,\ l = j; \\ -1, & \text{если } k = j,\ l = i; \\ 0 & \text{в остальных случаях.} \end{cases}$$

Пусть теперь

$$\sum_{1\le i<j\le n} \lambda_{ij}\varepsilon_i \wedge \varepsilon_j = 0$$

— произвольная линейная зависимость. Вычисляя значение стоящей слева билинейной функции на всевозможных парах (e_k, e_l), $1 \le k < l \le n$, получаем, что $\lambda_{ij} = 0$ для всех i, j. Поэтому указанные в условии билинейные кососимметрические функции действительно линейно независимы. Чтобы завершить доказательство, достаточно заметить, что $\dim \mathcal{B}^-(V) = \frac{n(n-1)}{2}$, хотя можно и явно записать разложение

$$\beta = \sum_{1\le i<j\le n} \beta(e_i, e_j)\varepsilon_i \wedge \varepsilon_j$$

произвольной билинейной кососимметрической функции β по указанной в условии системе (ср. равенство (84)). ■

К какому каноническому виду можно привести кососимметрическую функцию? Оказывается, ответ для кососимметрических функций не зависит от поля $\mathbb{K}$.

Пусть $\beta\colon V \times V \to \mathbb{K}$ — билинейная кососимметрическая функция на n-мерном пространстве V. Базис $\{e_1, \ldots, e_n\}$ пространства V называется *симплектическим* (относительно β), если

$$\beta(e_{2k-1}, e_{2k}) = -\beta(e_{2k}, e_{2k-1}) = 1 \quad \text{при} \quad k = 1, \ldots, m$$

$$\beta(e_i, e_j) = 0 \quad \text{во всех остальных случаях.}$$

Иначе говоря, матрица функции β имеет в этом базисе блочно-диагональный вид с m ненулевыми блоками вида $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Очевидно, что при этом $\operatorname{rk}\beta = 2m$. Эквивалентно,

$$\beta = \varepsilon_1 \wedge \varepsilon_2 + \varepsilon_3 \wedge \varepsilon_4 + \ldots + \varepsilon_{2m-1} \wedge \varepsilon_{2m},$$

где $\{\varepsilon_1, \ldots, \varepsilon_n\}$ — биортогональный базис к $\{e_1, \ldots, e_n\}$.

Теорема 10.61. *Для любой кососимметричной билинейной функции существует симплектический базис.*

Доказательство. Докажем это утверждение индукцией по n. При $n = 1$ доказываеть нечего (любая кососимметрическая функция на одномерном пространстве нулевая). Пусть $n > 1$. Если $\beta = 0$, то доказывать опять-таки нечего. Если $\beta \ne 0$, то существуют такие векторы e_1 и e_2, что $\beta(e_1, e_2) \ne 0$ (такие e_1, e_2, очевидно, линейно независимы). Умножив один из этих векторов на подходящий скаляр, можно добиться того, чтобы

$$\beta(e_1, e_2) = -\beta(e_2, e_1) = 1.$$

Матрица ограничения функции β на $\langle e_1, e_2\rangle$ в базисе $\{e_1, e_2\}$ имеет вид $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и, в частности, невырождена. Согласно Предложению 10.30,

$$V = \langle e_1, e_2\rangle \oplus \langle e_1, e_2\rangle^{\perp}.$$

По предположению индукции в пространстве $\langle e_1, e_2\rangle^{\perp}$ для $\beta|_{\langle e_1, e_2\rangle^{\perp}}$ существует симплектический базис $\{e_3, \ldots, e_n\}$. Добавляя к нему векторы e_1 и e_2, получаем симплектический базис $\{e_1, e_2, e_3, \ldots, e_n\}$ всего пространства V. ■

Следствие 10.62. *Ранг кососимметрической билинейной функции всегда является четным числом.*

Задача 10.63. *Докажите, что определитель целочисленной кососимметричной матрицы A является квадратом целого числа.*

Решение. Пусть кососимметрическая матрица $A \in \mathrm{Mat}_{2n}(\mathbb{Z})$ невырождена. Тогда ее можно рассматривать как матрицу с коэффициентами из поля $\mathbb{Q}$. В силу предыдущей теоремы существует невырожденная матрица $C \in \mathrm{Mat}_{2n}(\mathbb{Q})$ такая, что $A = C^T I C$, где I — блочно-диагональная матрица из блоков вида $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Тогда $\det A = (\det C)^2$, и целое число $\det A$ является квадратом рационального числа. Тогда $\det A$ является квадратом целого числа. ■

На самом деле верен более сильный результат: определитель кососимметрической матрицы как многочлен от ее элементов является полным квадратом многочлена с целыми коэффициентами, называемого *пфаффианом.* Например, для кососимметрических матриц порядка 4 пфаффиан равен $x_{12}x_{34} + x_{23}x_{14} + x_{31}x_{24}$. Точные определения и доказательства читатель может найти, например, в [17, 11].

11 Евклидовы пространства

Евклидовы пространства размерности 1, 2 и 3 — это те векторные[53] пространства, с которыми мы имели дело в курсе аналитической геометрии. В таких пространствах имеют смысл понятия длины вектора, угла между векторами, расстояния между подмножествами, объема параллелепипеда, построенного на системе векторов и т.д. Для определения этих понятий на вещественном векторном пространстве необходимо скалярное произведение — фиксированная билинейная симметричная положительно определенная функция.

Отметим отличие нашего подхода от принятого в курсе аналитической геометрии: там для скалярного произведения постулировалась формула $(u,\, v) = |u||v| \cos\alpha$, мы же придем к ней как к следствию из определения угла между векторами (см. конец параграфа 11.4).

11.1 Определение и примеры

Определение 11.1. *Евклидовым пространством* называется пара $(V,\, \alpha)$, состоящая из вещественного векторного пространства V и билинейной симметричной положительно определенной функции α на нем. Такая функция называется *скалярным произведением.*

Если не оговорено противное, все рассматриваемые евклидовы пространства предполагаются конечномерными.

В дальнейшем скалярное произведение $\alpha(u,\, v)$ векторов $u,\, v$ мы будем для простоты обозначать просто скобками (u, v). При этом соответствующая квадратичная функция принимает неотрицательные значения, и мы определяем *модуль* вектора v как $|v| := \sqrt{(v, v)}$. Заметим, что для любого $v \neq 0$ его модуль $|v| > 0$.

[53] В курсе аналитической геометрии также рассматривались пространства, состоящие из точек, а не векторов (первые, в отличие от вторых, нельзя складывать), такие пространства называются *аффинными* пространствами и изучаются в более полных курсах линейной алгебры.

За исключением нульмерного случая, скалярных произведений (то есть билинейных симметричных положительно определенных функциий) на V бесконечно много, в определении евклидова пространства предполагается, что фиксировано одно из них. Часто евклидовым пространством мы будем называть само вещественное векторное пространство V, предполагая фиксированным некоторое скалярное произведение на нем.

Из положительной определенности скалярного произведения следует, что оно — невырожденная билинейная функция. Кроме того, его ограничение на любое подпространство также положительно определено, и значит также невырождено.

Из общих результатов о квадратичных функциях мы можем вывести ряд следствий для евклидовых пространств.

Предложение 11.2. *В любом (конечномерном) евклидовом пространстве есть ортонормированный базис.*

Доказательство. Это следует либо непосредственно из Предложения 10.35, либо может быть выведено из Теоремы 10.57: для этого нужно взять произвольный базис в V (из Следствия 6.10 мы знаем, что он всегда существует), ортогонализировать его по Граму-Шмидту и затем нормировать. ■

Приведем примеры евклидовых пространств.

Пример 11.3. Пусть $V = \mathbb{R}^n$, и для произвольных столбцов $x, y \in V$ зададим их скалярное произведение как $(x, y) = x^T y$. (Читателю предлагается убедиться в выполнениии условий из определения евклидова пространства самостоятельно). Поскольку в любом конечномерном евклидовом пространстве (V, α) есть ортонормированный базис $\{e_1, \dots, e_n\}$, то, отождествляя V с пространством $\mathbb{R}^n$ координатных столбцов в этом базисе мы одновременно отождествим скалярное произведение $\alpha(u, v)$ произвольных векторов $u, v \in V$ с произведением $\overrightarrow{u}^T \overrightarrow{v}$ их координатных столбцов. То есть любое евклидово n-мерное пространство изоморфно данному (причем определенный таким образом изоморфизм линейных пространств сохраняет также скалярные произведения, то есть является изометрией, см. Определение 11.25). В обозначениях Предложения 6.53 полученный результат можно переписать так: выбор ортонормированного базиса e в V задает такой линейный изоморфизм $\varphi_e \colon V \to \mathbb{R}^n$ (заметим, что $\varphi_e(v)$ — то же что и $\overrightarrow{v}$ выше), что $\alpha(u, v) = \varphi_e(u)^T \varphi_e(v)$.

Еще раз отметим, что, выбирая ортонормированный базис в n-мерном евклидовом пространстве (V, α), мы отождествляем его с евклидовым пространством из Примера 11.3.

Пример 11.4. Пусть $V = \mathbb{R}^n$, и для произвольных столбцов $x, y \in V$ зададим их скалярное произведение как $(x, y) = x^T G y$, где G — произвольная симметричная положительно определенная матрица[54] порядка n. Тогда данная пара является евклидовым пространством.

[54] то есть матрица положительно определенной билинейной симметричной функции. Как мы помним, условие положительной определенности в силу критерия Сильвестра равносильно положительности всех угловых миноров.

На первый взгляд, это — более общий пример n-мерного евклидова пространства, чем предыдущий. Однако это не так. А именно, в $\mathbb{R}^n$ можно найти такой базис (то есть такой набор базисных столбцов), что относительно него заданное выше скалярное произведение будет задаваться формулой из Примера 11.3. Это просто следствие того факта, что в любом евклидовом пространстве существует ортонормированный базис. В нашем случае это означает, что можно найти такой набор столбцов $\{c_1, \ldots, c_n\}$, что $c_i^T G c_j = \delta_{ij}$, $1 \leq i, j \leq n$.

Пусть C — матрица, составленная из этих столбцов, то есть матрица перехода от стандартного базиса к базису $\{c_1, \ldots, c_n\}$. Тогда $C^T G C = E$, откуда $G = (C^{-1})^T E C^{-1}$. Мы видим, что матрица G является матрицей скалярного произведения в базисе, который получается из ортонормированного с помощью матрицы перехода C^{-1}. Поскольку любая невырожденная матрица порядка n является матрицей перехода от данного базиса в n-мерном пространстве, мы видим, что *любая симметричная положительно определенная матрица порядка n является матрицей скалярного произведения евклидова n-мерного пространства в некотором базисе.*

Пример 11.5. Пусть $V = \mathrm{Mat}_n(\mathbb{R})$, для матриц X, $Y \in V$ определим их скалярное произведение (X, Y) как $\mathrm{tr}\,(X^T Y)$. Читателю предлагается проверить, что это — действительно скалярное произведение. Заметим, что $\mathrm{tr}\,(X^T Y) = \sum_{i,j=1}^n x_{ij} y_{ij}$, это показывает, что базис в V, состоящий из матричных единиц (произвольным образом упорядоченных), является ортонормированным.

Наконец, приведем пример бесконечномерного евклидова пространства.

Пример 11.6. Пусть $V = C[0, 1]$ — пространство непрерывных вещественнозначных функций на отрезке $[0, 1]$. Определим скалярное произведение функций формулой $(f, g) = \int_0^1 f(x) g(x)\, dx$. Читатель легко убедится, что так определенная функция $V \times V \to \mathbb{R}$ является билинейной, симметричной и положительно определенной. Таким образом, данная пара — евклидово пространство. Легко видеть, что ограничение положительно определенной билинейной симметричной функции на любое подпространство также обладает данными свойствами, поэтому, скажем, подпространство многочленов $\mathbb{R}[x]_n \subset V$ с указанным скалярным произведением также является (на этот раз конечномерным) евклидовым пространством.

11.2 Ортогональное дополнение к подпространству

Продолжим выводить следствия из общих результатов о билинейных функциях.

Пусть $U \subset V$ — произвольное подпространство евклидова пространства V. Так как ввиду положительной определенности скалярное произведение невырождено, из Предложения 10.26 получаем, что $\dim U^\perp = \dim V - \dim U$ и $(U^\perp)^\perp = U$, а так как ограничение скалярного произведения на подпространство $U \subset V$ невырождено, из Предложения 10.30 — что $V = U \oplus U^\perp$. Значит, любой вектор $v \in V$ единственным образом представляется

в виде суммы $u + w$, где $u \in U$, $w \in U^\perp$. Вектор u называется *ортогональной проекцией* v на U и обозначается $pr_U(v)$, а вектор w — *ортогональной составляющей* вектора v относительно подпространства U и обозначается $ort_U(v)$. То есть, в нашей прежней терминологии, $pr_U(v)$ — проекция v на подпространство U параллельно его ортогональному дополнению $U^\perp$, а $ort_U(v)$ — проекция v на $U^\perp$ параллельно U.

В частности, линейный оператор $pr_U\colon V \to V$, сопоставляющий произвольному вектору $v \in V$ его ортогональную проекцию $pr_U(v)$ на подпространство $U \subset V$, называется *ортогональным проектором* на U. Это — частный случай проектора, когда проектирование происходит параллельно ортогональному дополнению.

Задача 11.7. *Пусть V — евклидово пространство из Примера 11.5. Докажите, что ортогональное дополнение к подпространству $\mathrm{Mat}_n^+(\mathbb{R}) \subset V$ симметрических матриц совпадает с подпространством $\mathrm{Mat}_n^-(\mathbb{R}) \subset V$ кососимметрических матриц, и наоборот, ортогональное дополнение к подпространству $\mathrm{Mat}_n^-(\mathbb{R}) \subset V$ кососимметрических матриц совпадает с подпространством $\mathrm{Mat}_n^+(\mathbb{R}) \subset V$ симметрических матриц.*

Решение. Покажем, что кососимметрическая матрица Y ортогональна любой симметрической матрице X. В самом деле,

$$(X, Y) = \mathrm{tr}\,(X^T Y) = \mathrm{tr}\,(XY) = \mathrm{tr}\,(YX) = -\mathrm{tr}(Y^T X) = -(Y, X),$$

откуда $(X, Y) = 0$. Значит, $\mathrm{Mat}_n^-(\mathbb{R}) \subset (\mathrm{Mat}_n^+(\mathbb{R}))^\perp$. С другой стороны, эти два подпространства имеют одинаковые размерности. Поэтому они совпадают. Второе утверждение проще всего вывести из доказанного с использованием $(U^\perp)^\perp = U$. ∎

Пусть V — евклидово n-мерное пространство, $U \subset V$ — его подпространство, которое является линейной оболочкой $\langle u_1, \ldots, u_k\rangle$ некоторой системы векторов u_i, $i = 1, \ldots, k$ из V. Тогда ортогональное дополнение $U^\perp$ задается системой уравнений

$$U^\perp = \{w \in V \mid (u_i, w) = 0,\ i = 1, \ldots, k\}.$$

Если $a_1, \ldots, a_k \in \mathbb{R}^n$ — координатные столбцы векторов $u_1, \ldots, u_k$ относительно некоторого ортонормированного базиса пространства V, то $U^\perp$ в этом базисе задается СЛОУ $A^T x = 0$. Если Φ — фундаментальная матрица этой СЛОУ, то ее столбцы образуют некоторый базис в $U^\perp$. Поэтому СЛОУ $\Phi^T y = 0$ задает подпространство $(U^\perp)^\perp = U$, то есть линейную оболочку столбцов матрицы A. Таким образом, мы получаем новое доказательство (и интерпретацию) Теоремы 6.49 (в случае поля $\mathbb{R}$). Отметим, что при этом связь между $\mathrm{rk}\,A$ и размерностью пространства решений системы $Ax = 0$ превращается в результат о связи между размерностями U и $U^\perp$.

Задача 11.8. *Докажите, что имеет место одна из двух возможностей: либо система линейных уравнений совместна при любом столбце свободных членов, либо ее сопряженная однородная система имеет ненулевое решение.*

Пусть в подпространстве $U \subset V$ евклидова пространства V задан ортонормированный базис $\{e_1, \ldots, e_k\}$. Тогда для любого $v \in V$ его ортогональная проекция $pr_U(v)$ задается формулой

$$pr_U(v) = \sum_{i=1}^{k} (v, e_i) e_i.$$

Действительно, $\sum_{i=1}^{k} (v, e_i) e_i$ — такой вектор из U, что $v - \sum_{i=1}^{k} (v, e_i) e_i \in U^\perp$ (а значит эта разность есть $ort_U(v)$). В самом деле,

$$\left(v - \sum_{i=1}^{k} (v, e_i) e_i, e_j \right) = (v, e_j) - (v, e_j) = 0 \ \text{ при } j = 1, \ldots, k.$$

В случае, когда дан только ортогональный базис $\{f_1, \ldots, f_k\}$ в U, ортогональная проекция $pr_U(v)$ находится по формуле

$$pr_U(v) = \sum_{i=1}^{k} \frac{(v, f_i)}{|f_i|^2} f_i, \tag{96}$$

в чем читатель легко убедится самостоятельно.

11.3 Описание линейных функций на евклидовом пространстве

Скалярное произведение является билинейной функцией, поэтому если зафиксировать один из его аргументов, получится линейная функция. Оказывается, так можно получить любую линейную функцию на конечномерном евклидовом пространстве.

Предложение 11.9. *Для любой линейной функции f на евклидовом пространстве V существует такой единственный вектор $w \in V$, что $f(v) = (v, w) \quad \forall\, v \in V$.*

Доказательство. Скалярное произведение (v, w) как функция от вектора $v \in V$ при фиксированном $w \in V$ является линейной функцией на V. Рассмотрим отображение

$$\alpha = \alpha_V \colon V \to V^*, \quad \alpha(w) = (\cdot, w).$$

Его линейность следует из линейности скалярного произведения по второму аргументу. Таким образом, α — линейное отображение между пространствами одинаковой размерности. Чтобы доказать, что α — изоморфизм, достаточно убедиться в его инъективности. Если $\alpha(w) = 0$ как линейная функция, то $\forall\, v \in V \ (v, w) = 0$, тогда, полагая $v = w$, получаем $|w| = 0$, то есть $w = 0$. В частности, α биективно, что равносильно утверждению доказываемого Предложения. ∎

Таким образом, в отличие от общих линейных пространств, для (конечномерного) евклидова пространства V существует канонический (не зависящий от базиса, а только от скалярного произведения) изоморфизм $\alpha_V \colon V \to V^*$.

Задача 11.10. *Докажите, что построенный изоморфизм $\alpha_V : V \to V^*$ имеет единичную матрицу в паре базисов, состоящей из ортонормированного базиса в V и биортогонального к нему базиса в V^*.*

Заметим, что для евклидовых пространств есть также канонический изоморфизм между пространствами линейных операторов и билинейных функций, который мы опишем в разделе 12.4.

11.4 Матрица Грама и неравенство Коши-Буняковского

Определение 11.11. *Матрицей Грама* $G(v_1, \ldots, v_k)$ системы векторов $\{v_1, \ldots, v_k\}$ евклидова пространства V называется матрица $G = (g_{ij})$, $g_{ij} = (v_i, v_j)$, составленная из их попарных скалярных произведений.

В частности, матрица скалярного произведения (как билинейной функции) в базисе $\{e_1, \ldots, e_n\}$ называется матрицей Грама этого базиса.

Предложение 11.12. *Для любой системы векторов $\{v_1, \ldots, v_k\}$ евклидова пространства V выполнено неравенство* $\det G(v_1, \ldots, v_k) \geq 0$, *причем равенство нулю имеет место тогда и только тогда, когда система $\{v_1, \ldots, v_k\}$ линейно зависима.*

Доказательство. Если система $\{v_1, \ldots, v_k\}$ линейно независима, то она является базисом в своей линейной оболочке $U := \langle v_1, \ldots, v_k \rangle$. Ограничение скалярного произведения на любое подпространство $U \subset V$ положительно определено, откуда (например, по критерию Сильвестра) $\det G(v_1, \ldots, v_k) > 0$.

Если система $\{v_1, \ldots, v_k\}$ линейно зависима, то пусть $\sum_{i=1}^k \lambda_i v_i = 0$ — нетривиальная линейная зависимость. Скалярно умножая левую и правую части этого равенства на векторы v_j, $1 \leq j \leq k$, получаем $\sum_{i=1}^k \lambda_i (v_i, v_j) = 0$, $1 \leq j \leq k$, что дает линейную зависимость между строками матрицы $G(v_1, \ldots, v_k)$ с теми же коэффициентами. ∎

Ключом к геометрии евклидова пространства является неравенство Коши-Буняковского.

Теорема 11.13. *Для любых двух векторов u, v евклидова пространства V имеет место неравенство $|(u, v)| \leq |u||v|$, причем оно превращается в равенство тогда и только тогда, когда векторы u и v линейно зависимы.*

Доказательство. 1-й способ. Согласно предыдущему Предложению,

$$\det \begin{pmatrix} (u,u) & (u,v) \\ (v,u) & (v,v) \end{pmatrix} = |u|^2|v|^2 - (u,v)^2 \geq 0,$$

причем равенство имеет место тогда и только тогда, когда u и v линейно зависимы.

2-й способ. Если $u = 0$, то, с одной стороны, для любого v векторы u и v линейно зависимы, с другой стороны, неравенство Коши-Буняковского, очевидно, превращается в равенство. Если $u \neq 0$, рассмотрим квадратный трехчлен

$$(tu + v, tu + v) = |u|^2 t^2 + 2(u, v)t + |v|^2,$$

который принимает неотрицательные значения для любого $t \in \mathbb{R}$. Значит, его дискриминант неположителен, то есть $(u, v)^2 - |u|^2|v|^2 \leq 0$, причем u и v линейно зависимы тогда и только тогда, когда трехчлен имеет вещественный корень, что эквивалентно тому, что дискриминант равен нулю. ■

Задача 11.14. *Докажите, что для любых непропорциональных функций f, $g \in C[0, 1]$ верно неравенство*

$$\left(\int_0^1 f(x)g(x)\,dx\right)^2 < \int_0^1 f^2(x)\,dx \int_0^1 g^2(x)\,dx.$$

В частности, для непрерывной функции $f \neq const$

$$\left(\int_0^1 f(x)\,dx\right)^2 < \int_0^1 f(x)^2\,dx.$$

Следствие 11.15. *(Неравенство треугольника). Для любых двух векторов u и v евклидова пространства*

$$|u + v| \leq |u| + |v|.$$

Доказательство.

$$(u + v, u + v) = |u|^2 + 2(u, v) + |v|^2 \leq |u|^2 + 2|u||v| + |v|^2 = (|u| + |v|)^2. \quad ■$$

Из неравенства треугольника следует, что для любых трех векторов u, v, w евклидова пространства V имеет место неравенство

$$|u - w| \leq |u - v| + |v - w|. \tag{97}$$

Наличие скалярного произведения позволяет измерять углы и расстояния в евклидовом пространстве.

Пусть u, $v \neq 0$ — векторы евклидова пространства V. Тогда из неравенства Коши-Буняковского

$$-1 \leq \frac{(u, v)}{|u||v|} \leq 1,$$

поэтому существует единственный угол α, $0 \leq \alpha \leq \pi$ такой, что $\cos\alpha = \frac{(u,v)}{|u||v|}$. По определению, он называется углом между ненулевыми векторами u и v. То есть мы возвращаемся к известной из аналитической геометрии формуле $(u, v) = |u||v| \cos\alpha$ (только теперь это не определение скалярного произведения, а следствие из определения угла).

11.5 Расстояния в евклидовом пространстве

Определим функцию $\rho\colon V \times V \to \mathbb{R}$ на евклидовом пространстве V равенством $\rho(u, v) := |u - v|$. Тогда она обладает следующими свойствами:

(i) $\rho(u, v) = \rho(v, u)$;

(ii) $\rho(u, u) = 0$; $\rho(u, v) > 0$ при $u \neq v$;

(iii) $\rho(u, w) \leq \rho(u, v) + \rho(v, w)$.

Заметим, что (iii) — просто неравенство треугольника (97) в других обозначениях. Таким образом, ρ является *метрикой* на V. Значит, в евклидовом пространстве определены все понятия, которые могут быть заданы с помощью метрики (расстояние между подмножествами, понятия открытого шара и открытого множества и т.п.).

Например, если A и B — произвольные подмножества в V, то определим расстояние между ними как

$$\rho(A, B) := \inf\{\rho(a, b) \mid a \in A,\, b \in B\}.$$

Получим формулу для расстояния от вектора $v \in V$ до подпространства $U \subset V$. Напомним, что $V = U \oplus U^{\perp}$ и $v = pr_U(v) + ort_U(v)$.

Предложение 11.16. $\rho(v, U) = |ort_U(v)|$.

Доказательство. $\forall\, u \in U$ имеем

$$|v - u|^2 = |pr_U(v) - u + ort_U(v)|^2 = |u - pr_U(v)|^2 + |ort_U(v)|^2,$$

откуда $|v - u|^2 \geq |ort_U(v)|^2$, причем $u = pr_U(v)$ — единственный вектор из U, для которого равенство достигается, то есть $pr_U(v)$ — единственный ближайший к v вектор из U. ∎

11.6 Замечание о топологии метрических пространств

Далее нам потребуются некоторые простейшие факты о топологии метрических пространств, поэтому напомним здесь соответствующие общие определения.

Пусть (X, ρ_X) — метрическое пространство. *Открытым шаром* с центром в точке $x \in X$ радиуса $\varepsilon > 0$ называется его подмножество $B_\varepsilon(x) := \{x' \in X \mid \rho(x, x') < \varepsilon\}$. Подмножество $U \subset X$ метрического пространства (X, ρ_X) называется *открытым*, если $\forall x \in U$ найдется такое $\varepsilon = \varepsilon(x) > 0$, что $B_\varepsilon(x) \subset U$. Множество всех открытых подмножеств в X (включающее также пустое множество $\varnothing$, всякая точка которого удовлетворяет приведенному условию) называется *топологией метрического пространства* (X, ρ_X) (оно в самом деле удовлетворяет аксиомам топологии и превращает множество X в топологическое пространство). Например, стандартная топология на $\mathbb{R}^n$, рассматриваемая в анализе

— это топология метрического пространства $(\mathbb{R}^n, \rho)$, где

$$\rho(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

— евклидова метрика.

Чтобы определить понятие непрерывного отображения между метрическими пространствами, достаточно рассматривать только открытые шары. Отображение $\varphi\colon (X, \rho_X) \to (Y, \rho_Y)$ между метрическими пространствами называется *непрерывным в точке* $x \in X$, если для всякого $\varepsilon > 0$ существует такое $\delta = \delta(\varepsilon) > 0$, что $\varphi(B_\delta(x)) \subset B_\varepsilon(\varphi(x))$. Отображение φ *непрерывно*, если оно непрерывно в каждой точке $x \in X$. Читатель легко убедится, что это определение в случае метрических пространств $(\mathbb{R}^n, \rho)$ (где ρ — евклидова метрика) и $(\mathbb{R}, \rho)$, где $\rho(a, b) = |a - b|$ (на самом деле это частный случай метрического пространства $(\mathbb{R}^n, \rho)$ при $n = 1$) приводит к обычному понятию непрерывной функции n переменных, используемому в анализе.

Отображение $\varphi\colon (X, \rho_X) \to (Y, \rho_Y)$ между метрическими пространствами называется *изометрией*, если оно биективно и $\forall x, x' \in X\ \rho_Y(\varphi(x), \varphi(x')) = \rho_X(x, x')$. Легко видеть, что обратное к изометрии отображение также является изометрией, и что для любого $\varepsilon > 0$ изометрия определяет биекцию между множествами открытых шаров радиуса ε в метрических пространствах (X, ρ_X) и (Y, ρ_Y). Из этого очевидно, что изометрия является непрерывным отображением (и даже гомеоморфизмом — напомним, что так называется изоморфизм топологических пространств). Более того, она устанавливает биекцию между множествами непрерывных функций (скажем, вещественнозначных) на X и на Y. Точнее, функция $f\colon Y \to \mathbb{R}$ непрерывна тогда и только тогда, когда $f \circ \varphi\colon X \to \mathbb{R}$ непрерывна.

Если V — n-мерное евклидово пространство с определенной выше метрикой $\rho_V(u, v) = |u - v|$, то выбор ортонормированного базиса e в V определяет линейный изоморфизм $\varphi_e\colon V \to \mathbb{R}^n$, который является изометрией $(V, \rho_V) \to (\mathbb{R}^n, \rho)$.

Любое подмножество $Z \subset X$ метрического пространства (X, ρ_X) само является метрическим пространством относительно метрики $\rho_Z = \rho_X|_{Z \times Z}$, являющейся ограничением метрики ρ_X на Z. Легко проверяется, что ограничение $f|_Z$ любой непрерывной функции $f\colon X \to \mathbb{R}$ на Z будет непрерывно как отображение $(Z, \rho_Z) \to \mathbb{R}$.

В параграфе 12.5 нам потребуется следующее утверждение: произвольная квадратичная функция $q\colon V \to \mathbb{R}$ на евклидовом пространстве V является непрерывной. Для доказательства этого факта можно рассуждать следующим образом. Выберем произвольный ортонормированный базис $\{e_1, \ldots, e_n\}$ в V, в соответствующих координатах квадратичная функция запишется как однородный многочлен 2-й степени $p_q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$. Из курса анализа мы знаем, что он — непрерывная функция на $(\mathbb{R}^n, \rho)$, где ρ — евклидова метрика. А так как выбор базиса задает изометрию, а значит, в силу сказанного выше, непрерывное отображение[55] $\varphi_e\colon V \to \mathbb{R}^n$, то $q = p_q \circ \varphi_e$ непрерывна на V (поскольку

[55] еще точнее, гомеоморфизм.

является композицией непрерывных отображений).

11.7 Алгоритм Грама-Шмидта

Теорема 11.17. *Пусть $\{e_1, \dots, e_n\}$ — произвольный базис в евклидовом пространстве V. Тогда существует единственный ортогональный базис $\{f_1, \dots, f_n\}$ в V, матрица перехода к которому от исходного базиса верхняя треугольная с единицами на главной диагонали.*

Базис $\{f_1, \dots, f_n\}$ называется *ортогонализацией* базиса $\{e_1, \dots, e_n\}$. Заметим, что из условия следует, что линейные оболочки $\langle e_1, \dots, e_k\rangle$ и $\langle f_1, \dots, f_k\rangle$ совпадают при $k = 1, \dots, n$.

Заметим еще, что вместо базиса в V можно ортогонализовать произвольную линейно независимую систему векторов в V (тогда она будет базисом в своей линейной оболочке, и рассуждение можно применить к последней).

Доказательство. Из вида матрицы перехода следует, что для f_1 единственная возможность — положить $f_1 = e_1$. Пусть система с требуемыми свойствами $\{f_1, \dots, f_{k-1}\}$ уже построена. Из вида матрицы перехода следует, что мы должны искать f_k в виде $f_k = e_k + \sum_{i=1}^{k-1} \mu_i e_i$, но так как $V_{k-1} := \langle e_1, \dots, e_{k-1}\rangle = \langle f_1, \dots, f_{k-1}\rangle$ (это снова следует из вида матрицы перехода и предположения индукции), то, эквивалентно, f_k можно также искать в виде $f_k = e_k + \sum_{i=1}^{k-1} \lambda_i f_i$. Условия $f_k \perp f_1, \dots, f_{k-1}$ (что равносильно $f_k \in V_{k-1}^{\perp}$) записываются в виде системы $(f_k, f_j) = 0,\ j = 1, \dots, k-1$, более подробно

$$\left(e_k + \sum_{i=1}^{k-1} \lambda_i f_i,\ f_j\right) = (e_k, f_j) + \lambda_j |f_j|^2 = 0, \tag{98}$$

откуда $\lambda_j = -\frac{(e_k, f_j)}{|f_j|^2},\ j = 1, \dots, k-1$. Теперь формула (96) показывает, что $f_k = ort_{V_{k-1}} e_k$. Так как $\{e_1, \dots, e_n\}$ — базис, то $e_k \notin V_{k-1}$ и поэтому $f_k \neq 0$. Тем самым шаг построения ортогонального базиса завершен. ∎

Пример 11.18. Рассмотрим подпространство $\mathbb{R}[x]_2$ в бесконечномерном евклидовом пространстве $C[0,1]$ из Примера 11.6. Найдем ортогонализацию $\{f_1, f_2, f_3\}$ "стандартного" базиса $\{1, x, x^2\}$ в нем. Имеем

$$f_1 = 1,\quad f_2 = x - \frac{(x,1)}{|1|^2}1 = x - \frac{1}{2},\quad f_3 = x^2 - \frac{(x^2,1)}{|1|^2}1 - \frac{(x^2, x-\frac{1}{2})}{|x-\frac{1}{2}|^2}\left(x - \frac{1}{2}\right) = x^2 - x + \frac{1}{6}.$$

Геометрический смысл описанного в Теореме алгоритма можно представить следующим образом. Натянем на исходный неортогональный базис $\{e_1, \dots, e_n\}$ n-мерный параллелепипед $\Pi[e_1, \dots, e_n]$. Тогда изложенный выше алгоритм сводится к следующему: вектор $f_1 = e_1$ мы оставляем тем же, а вектор e_2 заменяем на высоту f_2 параллелепипеда $\Pi[e_1, e_2]$ относительно основания $\Pi[e_1]$, далее вектор e_3 — на высоту f_3 параллелепипеда $\Pi[e_1, e_2, e_3]$

относительно основания $\Pi[e_1, e_2]$ и т.д. Ясно, что при этом получается прямоугольный параллелепипед $\Pi[f_1, \dots, f_n]$ того же n-мерного объема (если правильно определить это понятие).[56]. Кроме того, каждый из k-мерных параллелепипедов $\Pi[e_1, \dots, e_k]$ при этом заменяется прямоугольным k-мерным параллелепипедом $\Pi[f_1, \dots f_k]$ того же k-мерного объема.

Используя приведенные соображения, можно обосновать, что квадрат n-мерного объема $\mathrm{Vol}(e_1, \dots, e_n)$ параллелепипеда $\Pi[e_1, \dots, e_n]$, построенного на базисе $\{e_1, \dots, e_n\}$, равен $\det G$, где G — матрица Грама скалярного произведения в этом базисе. Действительно, по предшествующей Теореме у базиса $\{e_1, \dots, e_n\}$ есть ортогонализация $\{f_1, \dots, f_n\}$, то есть существует верхняя треугольная матрица C с единицами на главной диагонали такая, что $\mathrm{diag}\,(|f_1|^2, \dots, |f_n|^2) = C^T G C$. В частности, $\det G = |f_1|^2 \dots |f_n|^2$, причем правая часть совпадает с квадратом $\mathrm{Vol}\,(f_1, \dots, f_n)^2$ объема прямоугольного параллелепипеда, построенного на ортогональном базисе $\{f_1, \dots, f_n\}$ (поскольку есть произведение квадратов длин его сторон), а выше мы "обосновали", что объем параллелепипеда, построенного на базисе, не меняется при ортогонализации этого базиса.

Из доказанной Теоремы мы сейчас выведем важное следствие. Пусть G — матрица Грама базиса $\{e_1, \dots, e_n\}$. Пусть G_k, $1 \le k \le n$ — подматрица матрицы G порядка k, стоящая в левом верхнем углу. Очевидно, что G_k — матрица ограничения $(\cdot, \cdot)|_{V_k}$ скалярного произведения на подпространство V_k в базисе $\{e_1, \dots, e_k\}$ этого пространства. Пусть $\delta_k := \det G_k$ — угловые миноры матрицы G. Из положительной определенности скалярного произведения следует, что все они больше нуля. Введем еще $\delta_0 := 1$.

Следствие 11.19. *В введенных выше обозначениях*

$$|f_k|^2 = (f_k, f_k) = \frac{\delta_k}{\delta_{k-1}},\ 1 \le k \le n.$$

Доказательство. Для $1 \le k \le n$ имеем

$$\mathrm{diag}\,(|f_1|^2, \dots, |f_k|^2) = C_k^T G_k C_k,$$

откуда, переходя к определителям и используя то, что матрицы C_k верхние треугольные с единицами на главной диагонали, получаем требуемое. ■

Доказанное в Следствии тождество имеет следующий геометрический смысл: *квадрат длины высоты k-мерного параллелепипеда равен отношению квадрата его k-мерного объема к квадрату $k-1$-мерного объема соответствующего основания.* Действительно, выше мы "обосновали", что $\det G$ равен квадрату n-мерного объема параллелепипеда, построенного на базисе $\{e_1, \dots, e_n\}$. По тем же причинам δ_k есть квадрат k-мерного объема $\mathrm{Vol}\,(e_1, \dots, e_k)$. Тогда равенство $|f_k|^2 = \frac{\delta_k}{\delta_{k-1}}$ означает в точности то, что написано выше.

Полученный результат позволяет получить явную формулу для расстояния от вектора до подпространства. Пусть $U \subset V$ — подпространство евклидова пространства V и $v \in V$ — произвольный вектор. Пусть $\{e_1, \dots, e_k\}$ — произвольный базис в U. Тогда (ср. Предложение 11.16)

$$\rho(v, U)^2 = \frac{\det G(e_1, \dots, e_k, v)}{\det G(e_1, \dots, e_k)}.$$

Пусть $\varphi\colon V \to V$ — линейный оператор на евклидовом пространстве V, $\{e_1, \dots, e_n\}$ — произвольный ортонормированный базис в V.

[56] Строго определять что это такое в данном курсе мы не будем. Для n-мерного параллелепипеда при $n = 1, 2, 3$ n-мерный объем — это соответственно длина, (неориентированная) площадь и "обычный" (неориентированный) трехмерный объем.

Предложение 11.20. *Во введенных выше обозначениях* $\mathrm{Vol}(\varphi(e_1), \ldots, \varphi(e_n)) = |\det \varphi|$.

Доказательство. Пусть A — матрица оператора φ в базисе $\{e_1, \ldots, e_n\}$; тогда

$$(\varphi(e_1), \ldots, \varphi(e_n)) = (e_1, \ldots, e_n)A,$$

откуда $G(\varphi(e_1), \ldots, \varphi(e_n)) = A^T E A = A^T A$, и, значит, $\det G(\varphi(e_1), \ldots, \varphi(e_n)) = (\det A)^2$. ■

Доказанное равенство можно понимать как "геометрический смысл" числа $|\det \varphi|$ — оно показывает, во сколько раз меняется объем параллелепипеда при применении к нему оператора φ. Что касается знака числа $\det \varphi$ (который имеет смысл только при $\det \varphi \neq 0$), то он может быть истолкован как ориентация базиса $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ относительно базиса $\{e_1, \ldots, e_n\}$.

11.8 Описание ортонормированных базисов

Пусть V — евклидово n-мерное пространство, $e := \{e_1, \ldots, e_n\}$ — некоторый ортонормированный базис в нем (мы знаем, что он существует), $e' := \{e'_1, \ldots, e'_n\}$ — еще какой-то базис в V и C — матрица перехода от e к e'. Тогда матрица Грама базиса e' равна $G_{e'} = C^T C$. Таким образом, базис e' тоже ортонормированный тогда и только тогда, когда $C^T C = E$, или, что равносильно, $C^T = C^{-1}$.

Определение 11.21. Квадратная вещественная матрица C называется *ортогональной*, если $C^T C = E$.

Если рассмотреть матрицу C как совокупность столбцов $(c_1, \ldots, c_n)$, то условие ортогональности равносильно тому, что эти столбцы образуют ортонормированный базис в $\mathbb{R}^n$ относительно стандартного скалярного произведения: $c_i^T c_j = \delta_{ij}$. Очевидно, что условие ортогональности матрицы C можно также переписать в виде $CC^T = E$, что дает аналогичное условие для строк.

Заметим, что определитель любой ортогональной матрицы равен ± 1. Конечно, это условие не является достаточным условием ортогональности матрицы.

Задача 11.22. *Покажите, что ортогональные матрицы порядка* 2 *распадаются на два непересекающихся класса:* $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ *и* $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$, $0 \leq \alpha \leq 2\pi$. *Матрицы первого типа являются матрицами перехода между одинаково ориентированными, а второго — противоположно ориентированными ортонормированными базисами.*

Предложение 11.23. *Зафиксируем ортонормированный базис* $e := \{e_1, \ldots, e_n\}$ *в евклидовом пространстве* V. *Тогда сопоставление* $e' \mapsto C_{e'}$ *базису* e' *матрицы перехода* $C_{e'}$ *к нему от фиксированного базиса* e *определяет биекцию между ортонормированными базисами в* V *и ортогональными матрицами порядка* n.

Доказательство. Так как матрица перехода однозначно задается указанием упорядоченной пары базисов, описанное в условии Предложения отображение корректно определено.

Оно инъективно, так как базис e' однозначно определяется указанием базиса e и матрицы перехода $C_{e'}$. Оно сюръективно, так как произвольная ортогональная матрица является матрицей перехода от фиксированного ортонормированного базиса e к некоторому ортонормированному. ■

Задача 11.24. *Покажите, что ортогональные матрицы данного порядка n образуют группу (она стандартно обозначается $\mathrm{O}(n)$). Как этот результат связан с интерпретацией ортогональных матриц как матриц перехода между ортонормированными базисами?*

11.9 Изоморфизмы евклидовых пространств

Пусть V и U — евклидовы пространства со скалярными произведениями $(\cdot,\cdot)_V$ и $(\cdot,\cdot)_U$.

Определение 11.25. Линейное отображение $\varphi\colon V \to U$ называется *изометрией*, если $(\varphi(v_1),\varphi(v_2))_U = (v_1,v_2)_V \ \ \forall v_1, v_2, \in V$.

То есть изометрия сохраняет скалярные произведения, в частности, длины векторов и углы между ними. Также ясно, что она ортонормированный базис в V переводит в ортонормированную систему векторов в U. Уже отсюда понятно, что любая изометрия инъективна. Покажем это по-другому: пусть $v \in \operatorname{Ker}\varphi$. Тогда $0 = (\varphi(v),\varphi(v))_U = (v,v)_V = |v|^2$, откуда $v = 0$.

Геометрически более-менее понятно, что преобразование, сохраняющее длины (и углы) между всеми векторами, сохраняет и линейные соотношения между ними, поскольку отображает евклидово пространство "как твердое тело" (вспомните доказательство линейности поворота плоскости). Поэтому требование линейности в определении изометрии лишнее.

Задача 11.26. *Отображение между евклидовыми пространствами $\varphi\colon V \to U$ такое, что $(\varphi(v_1),\varphi(v_2))_U = (v_1,v_2)_V \ \ \forall v_1, v_2 \in V$, является линейным.*

Решение. Положим $w := v_1 + v_2$.

$$0 = |w - v_1 - v_2|^2 = |w|^2 + |v_1|^2 + |v_2|^2 + 2(v_1,v_2) - 2(v_1,w) - 2(v_2,w) =$$

$$= |\varphi(w)|^2 + |\varphi(v_1)|^2 + |\varphi(v_2)|^2 + 2(\varphi(v_1),\varphi(v_2)) - 2(\varphi(v_1),\varphi(w)) - 2(\varphi(v_2),\varphi(w)) =$$

$$= |\varphi(w) - \varphi(v_1) - \varphi(v_2)|^2,$$

откуда $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$. Аналогично проверяется, что $\varphi(\lambda v) = \lambda\varphi(v)$. ■

Определение 11.27. Биективная изометрия между евклидовыми пространствами называется *изоморфизмом евклидовых пространств*.

Два евклидовых пространства называются *изоморфными*, если между ними есть изоморфизм. Заметим, что любой изоморфизм евклидовых пространств является линейным изоморфизмом, который вдобавок является изометрией. В частности, если два евклидовых пространства изоморфны, то у них обязательно одинаковые размерности.

Предложение 11.28. *Два евклидовых пространства изоморфны тогда и только тогда, когда они имеют одинаковую размерность.*

Доказательство. В силу сделанного выше замечания достаточно доказать, что евклидовы пространства V и U одинаковой размерности изоморфны. Построим изометрию между ними следующим образом: выберем ортонормированный базис $\{e_1, \ldots, e_n\}$ в V и такой же базис $\{f_1, \ldots, f_n\}$ в U и определим линейное отображение $\varphi\colon V \to U$ условием $\varphi(e_i) = f_i,\ i = 1, \ldots, n$. Это — линейный изоморфизм, который, как легко убедится читатель, используя билинейность скалярного произведения, является также изометрией. ■

Доказанное Предложение свидетельствует о том, что геометрические свойства евклидовых пространств одинаковой размерности одни и те же, поэтому в качестве "модельного" n-мерного евклидова пространства можно взять пространство столбцов $\mathbb{R}^n$ со стандартным скалярным произведением.

Изоморфизмы евклидова пространства на себя называются ортогональными преобразованиями, их мы изучим позже.

11.10 QR-разложение

Предложение 11.29. *Для любой невырожденной вещественной матрицы A существуют единственные ортогональная матрица Q и верхняя треугольная матрица R с положительными элементами на главной диагонали такие, что $A = QR$.*

Доказательство. Пусть $\mathbb{R}^n$ — пространство столбцов со стандартным скалярным произведением. Рассмотрим A как совокупность столбцов $(a_1 \ldots a_n)$, $a_i \in \mathbb{R}^n$. Пусть $E = (e_1 \ldots e_n)$ — единичная матрица (ее столбцы образуют стандартный ортонормированный базис в $\mathbb{R}^n$). Тогда A является матрицей перехода от $\{e_1, \ldots, e_n\}$ к $\{a_1, \ldots, a_n\}$, то есть

$$(a_1 \ldots a_n) = (e_1 \ldots e_n)A.$$

Пусть $\{q_1, \ldots, q_n\}$ — ортонормированный базис из столбцов, полученный из $\{a_1, \ldots, a_n\}$ ортогонализацией по Граму-Шмидту с последующим нормированием. Тогда матрица перехода T от $\{a_1, \ldots, a_n\}$ к $\{q_1, \ldots, q_n\}$ является верхней треугольной с положительными элементами на главной диагонали. Обратная R к такой матрице тоже является верхней треугольной с положительными элементами на главной диагонали (чтобы это доказать, примените последовательность элементарных преобразований строк к $(T \mid E)$). Итак,

$$(a_1 \ldots a_n) = (q_1 \ldots q_n)R,$$

где R — верхняя треугольная матрица с положительными элементами на главной диагонали. Так как базис $\{q_1, \ldots, q_n\}$ ортонормирован, то матрица Q перехода к нему от $\{e_1, \ldots, e_n\}$ ортогональна (это есть матрица из столбцов $(q_1 \ldots q_n)$). Таким образом, получаем

$$(a_1 \ldots a_n) = (e_1 \ldots e_n)QR,$$

или в матричном виде $A = QR$.

Докажем теперь единственность. Пусть $A = QR = Q'R'$, тогда $Q'^{-1}Q = R'R^{-1}$. Нетрудно видеть, что справа стоит верхняя треугольная матрица с положительными элементами на главной диагонали, а

слева — ортогональная матрица. Очевидно, что пересечение указанных множеств матриц состоит только из E. ■

Заметим, что помимо QR-разложения для произвольной невырожденной матрицы A есть также аналогичное RQ-разложение. Чтобы это доказать, достаточно найти QR-разложение для A^{-1}.

Интересный вопрос: как описать множество всех скалярных произведений на вещественном векторном пространстве V? С одной стороны, поскольку скалярное произведение в фиксированном базисе однозначно определяется своей матрицей Грама, а такой матрицей может быть произвольная симметричная положительно определенная матрица (порядка, равного размерности V), то множество всех скалярных произведений на V биективно множеству таких матриц (причем биекция, конечно, зависит от базиса). Значит, это непустое (поскольку, например, оно содержит единичную матрицу), открытое (поскольку по критерию Сильвестра условие положительной определенности равносильно выполнению конечной системы строгих неравенств) подмножество в $\frac{n(n+1)}{2}$-мерном пространстве симметричных матриц порядка n, где $n = \dim V$.

Иначе можно рассуждать так. Задать скалярное произведение α можно, выбрав произвольный базис e в V и объявив его ортонормированным относительно α. Еще один базис e' в V задает то же самое скалярное произведение α тогда и только тогда, когда матрица перехода C от e к e' ортогональна. Действительно, это равносильно тому, что из $G_e = E$ следует $G_{e'} = C^T C = E$.

Более общо, зафиксируем некоторый базис e. Пусть C и D — матрицы перехода от e к базисам e' и e'' соответственно. При каком условии скалярные произведения, определенные базисами e' и e'' совпадают? Очевидно, тогда и только тогда, когда матрица перехода от e' к e'' ортогональна. То есть тогда и только тогда, когда $D = CQ$, где $Q \in \mathrm{O}(n)$, эквивалентно, тогда и только тогда, когда в RQ-разложениях матриц D и C верхние треугольные матрицы совпадают. Таким образом, мы получаем также конкретную биекцию между множеством скалярных произведений в вещественном векторном пространстве V размерности n и множеством верхних треугольных матриц порядка n с положительными элементами на главной диагонали.

12 Операторы и билинейные функции в евклидовых пространствах

На евклидовом пространстве можно выделить интересные классы линейных операторов. Во-первых те операторы, которые диагонализируются в ортонормированном базисе — они называются самосопряженными. Во-вторых, операторы, которые являются изометриями евклидова пространства — ортогональные операторы. Кроме того, на евклидовом пространстве линейные операторы можно превращать в билинейные формы и наоборот, что делает соответствующую теорию еще более богатой (например, возникает понятие положительных операторов, которые отвечают положительно определенным симметричным билинейным формам). Данный раздел и посвящен изучению этих тем.

12.1 Сопряженное отображение

Пусть U и V — евклидовы пространства со скалярными произведениями $(\ ,\ )_U$ и $(\ ,\ )_V$ соответственно, $\varphi\colon U \to V$ — линейное отображение.

Определение 12.1. Отображение $\varphi^*\colon V \to U$ называется *сопряженным* к φ, если

$$(\varphi(u),\, v)_V = (u,\, \varphi^*(v))_U \quad \forall\, u \in U,\, v \in V. \tag{99}$$

В частном случае $U = V$ мы приходим к понятию *сопряженного преобразования*.

Предложение 12.2. *Для любого линейного отображения $\varphi\colon U \to V$ между евклидовыми пространствами существует единственное сопряженное отображение φ^*. Кроме того, сопряженное отображение линейно.*

Доказательство. Рассмотрим выражение $f_{\varphi,\,v}(u) := (\varphi(u),\, v)_V$ как функцию от $u \in U$ при фиксированных $v \in V$ и φ. Из линейности φ и скалярного произведения по первому аргументу следует, что $f_{\varphi,\,v}$ линейна, то есть $f_{\varphi,\,v} \in U^*$.

Согласно Предложению 11.9, для данных $v \in V$ и φ существует единственный $w \in U$ такой, что

$$f_{\varphi,\,v}(u) = (u,\, w)_U \quad \forall\, u \in U.$$

Этот вектор w мы обозначим $\varphi^*(v)$ (что, в частности, подчеркивает его зависимость от $v \in V$ и φ). То есть для фиксированного φ и данного $v \in V$ существует единственный $\varphi^*(v) \in U$ такой, что

$$(\varphi(u),\, v)_V = (u,\, \varphi^*(v))_U \quad \forall\, u \in U.$$

Это означает, что сопряженное к φ отображение φ^* существует и единственно.

Проверим теперь линейность сопряженного отображения. Имеем

$$(u,\, \varphi^*(v_1 + v_2))_U = (\varphi(u),\, v_1 + v_2)_V = (\varphi(u),\, v_1)_V + (\varphi(u),\, v_2)_V =$$

$$= (u,\, \varphi^*(v_1))_U + (u,\, \varphi^*(v_2))_U = (u,\, \varphi^*(v_1) + \varphi^*(v_2))_U \quad \forall\, u \in U,$$

откуда получаем $\varphi^*(v_1 + v_2) = \varphi^*(v_1) + \varphi^*(v_2)$.

Аналогично,

$$(u,\, \varphi^*(\lambda v))_U = (\varphi(u),\, \lambda v)_V = \lambda(\varphi(u),\, v)_V =$$

$$= \lambda(u,\, \varphi^*(v))_U = (u,\, \lambda\varphi^*(v))_U,$$

откуда $\varphi^*(\lambda v) = \lambda\varphi^*(v)$. ∎

Замечание 12.3. Опишем связь введенной операции сопряжения линейных отображений между евклидовыми пространствами с операцией "линейного сопряжения" $\varphi \mapsto \varphi^\star$, введенной в конце параграфа 7.6. Для произвольного линейного отображения $\varphi\colon U \to V$ рассмотрим диаграмму

$$\begin{array}{ccc} V^* & \xrightarrow{\varphi^\star} & U^* \\ {\scriptstyle\alpha_V}\uparrow & & \uparrow{\scriptstyle\alpha_U} \\ V & \xrightarrow[\varphi^*]{} & U, \end{array}$$

где α_U, α_V — изоморфизмы, определенные в параграфе 11.3. Проверим, что она коммутативна. В самом деле, путь из левого нижнего угла вверх и вправо отвечает композиции

$$v \mapsto (\cdot, v)_V \mapsto (\varphi(\cdot),\, v)_V$$

(где мы использовали определение $\varphi^\star$), в то время как путь вправо и вверх — композиции

$$v \mapsto \varphi^*(v) \mapsto (\cdot, \varphi^*(v))_U.$$

Условие равенства линейных функций $(\varphi(\cdot),\, v)_V$ и $(\cdot, \varphi^*(v))_U$ на U эквивалентно определению сопряженного отображения. Таким образом, $\varphi^* = \alpha_U^{-1} \circ \varphi^\star \circ \alpha_V$.

Пусть $\mathcal{L}(U,\, V)$ обозначает линейное пространство всех линейных отображений $\varphi\colon U \to V$.

Предложение 12.4. *Операция*

$$*\colon \mathcal{L}(U,\, V) \to \mathcal{L}(V,\, U) \tag{100}$$

обладает следующими свойствами:

1) $(\varphi_1 + \varphi_2)^* = \varphi_1^* + \varphi_2^*$, $(\lambda\varphi)^* = \lambda\varphi^*$ *(то есть отображение (100) линейно);*

2) $\varphi^{**} = \varphi$ *(то есть* $*^2 = \mathrm{Id}_{\mathcal{L}(U,V)}$*);*

3) $\mathrm{Id}_U^* = \mathrm{Id}_U$, *где* $\mathrm{Id}_U\colon U \to U$ *— тождественное преобразование;*

4) *если* $\psi\colon V \to W$ *— еще одно линейное отображение между евклидовыми пространствами, то* $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$;

5) *если* φ *— изоморфизм, то* $(\varphi^{-1})^* = (\varphi^*)^{-1}$.

Доказательство. 1)

$$(u,\, (\varphi_1 + \varphi_2)^*(v))_U = ((\varphi_1 + \varphi_2)(u),\, v)_V = (\varphi_1(u) + \varphi_2(u),\, v)_V =$$

$$= (\varphi_1(u),\, v)_V + (\varphi_2(u),\, v)_V = (u,\, \varphi_1^*(v))_U + (u,\, \varphi_2^*(v))_U = (u,\, (\varphi_1^* + \varphi_2^*)(v))_U,$$

$$(u,\, (\lambda\varphi)^*(v))_U = ((\lambda\varphi)(u),\, v)_V = \lambda(\varphi(u),\, v)_V = \lambda(u,\, \varphi^*(v))_U = (u,\, \lambda\varphi^*(v))_U.$$

2)

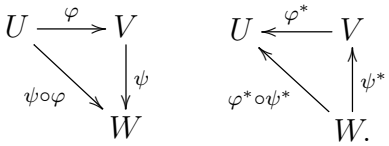
$$(\varphi(u),\, v)_V = (u,\, \varphi^*(v))_U = (\varphi^*(v),\, u)_U = (v,\, \varphi^{**}(u))_V = (\varphi^{**}(u),\, v)_V.$$

Заметим, что доказанное свойство в частности означает, что всякое отображение φ является сопряженным к некоторому (а именно к φ^*).

3)

$$(\mathrm{Id}_U(u_1),\, u_2) = (u_1,\, u_2) = (u_1,\, \mathrm{Id}_U^*(u_2)).$$

4) Чтобы лучше понять направления, в которых действуют отображения, полезно посмотреть на диаграммы



$$(u,\,(\psi\circ\varphi)^*(w))_U = ((\psi\circ\varphi)(u),\,w)_W = (\varphi(u),\,\psi^*(w))_V =$$
$$= (u,\,\varphi^*(\psi^*(w)))_U = (u,\,(\varphi^*\circ\psi^*)(w))_U.$$

5)
$$\mathrm{Id}_U = \mathrm{Id}_U^* = (\varphi^{-1}\circ\varphi)^* = \varphi^*\circ(\varphi^{-1})^*,$$
$$\mathrm{Id}_V = \mathrm{Id}_V^* = (\varphi\circ\varphi^{-1})^* = (\varphi^{-1})^*\circ\varphi^*,$$

откуда $(\varphi^{-1})^* = (\varphi^*)^{-1}$. ∎

Свойства операции "звездочка", доказанные в предыдущем Предложении, напоминают свойства операции транспонирования матриц (см. Предложение 2.19). Это неслучайно. Чтобы это увидеть, посмотрим, как связаны матрицы отображения и его сопряженного относительно выбранных базисов в U и V.

Пусть $\{e_1,\dots,e_n\}$ — некоторый базис в U, $\{f_1,\dots,f_m\}$ — базис в V, $\overrightarrow{u}$, $\overrightarrow{v}$ — координатные столбцы векторов u и v, G_U, G_V — матрицы Грама выбранных базисов в U и V, $A = A_\varphi$ — матрица линейного отображения $\varphi\colon U\to V$, а B — матрица сопряженного отображения $\varphi^*\colon V\to U$. Тогда в базисах соотношение (99) переписывается в следующем виде:

$$(A\overrightarrow{u})^T G_V\overrightarrow{v} = \overrightarrow{u}^T G_U B\overrightarrow{v},\quad \text{то есть}\quad \overrightarrow{u}^T A^T G_V\overrightarrow{v} = \overrightarrow{u}^T G_U B\overrightarrow{v};$$

поскольку это должно быть выполнено для любых столбцов $\overrightarrow{u}$ и $\overrightarrow{v}$, то отсюда следует, что

$$A^T G_V = G_U B. \tag{101}$$

То есть матрица B сопряженного отображения φ^* равна $G_U^{-1}A^T G_V$. В частности, если выбранные базисы являются ортонормированными (что, напомним, равносильно $G_U = E$, $G_V = E$), то $B = A^T$. Легко видеть, что выполнено и обратное: если относительно некоторых базисов евклидовых пространств U и V матрицы A и B отображений $\varphi\colon U\to V$ и $\psi\colon V\to U$ связаны соотношением (101), то эти отображения сопряжены, $\psi = \varphi^*$ (или, что равносильно, $\varphi = \psi^*$).

Задача 12.5. *Докажите, что преобразование $\varphi\colon V\to V$ и его сопряженное φ^* имеют одинаковые характеристический и минимальный многочлены.*

Задача 12.6. *Докажите, что преобразование $\varphi\colon V\to V$ евклидова пространства V диагонализируемо тогда и только тогда, когда φ^* диагонализируемо. (Указание: как связаны минимальные многочлены φ и φ^*?).*

Для любого базиса $e := \{e_1, e_2, \ldots, e_n\}$ в евклидовом пространстве V существует единственный *взаимный* базис $e^* := \{e_1^*, e_2^*, \ldots, e_n^*\}$ такой, что $(e_i, e_j^*) = \delta_{ij}$, $1 \leq i, j \leq n$. В самом деле, если A — матрица, составленная из координатных столбцов векторов базиса e в некотором ортонормированном базисе пространства V, то для аналогичной матрицы B для e^* в том же базисе имеем $A^T B = E$, откуда $B = A^{-T}$.

Задача 12.7. *Пусть $\varphi\colon V \to V$ — диагонализируемое преобразование евклидова пространства V и $\{e_1, e_2, \ldots, e_n\}$ — базис из его собственных векторов. Докажите, что взаимный базис $\{e_1^*, e_2^*, \ldots, e_n^*\}$ состоит из собственных векторов сопряженного оператора φ^*.*

12.2 Теорема Фредгольма

Пусть $\varphi\colon U \to V$ — линейное отображение между евклидовыми пространствами.

Теорема 12.8. $\operatorname{Im}\varphi = (\operatorname{Ker}\varphi^*)^\perp$ *(равенство подпространств в V).*

Доказательство. Заметим, что равенство подпространств из условия задачи равносильно равенству $(\operatorname{Im}\varphi)^\perp = \operatorname{Ker}\varphi^*$ их ортогональных дополнений в V, которое мы и будем доказывать.

Пусть $v \in \operatorname{Ker}\varphi^*$, тогда для любого $u \in U$

$$0 = (u,\, \varphi^*(v))_U = (\varphi(u),\, v)_V \quad \Rightarrow \quad v \in (\operatorname{Im}\varphi)^\perp,$$

то есть $\operatorname{Ker}\varphi^* \subset (\operatorname{Im}\varphi)^\perp$.

Пусть $v \in (\operatorname{Im}\varphi)^\perp$, тогда для любого $u \in U$

$$0 = (\varphi(u),\, v)_V = (u,\, \varphi^*(v))_U \quad \Rightarrow \quad v \in \operatorname{Ker}\varphi^*,$$

то есть $(\operatorname{Im}\varphi)^\perp \subset \operatorname{Ker}\varphi^*$. ∎

Дадим теперь геометрическое доказательство теоремы Фредгольма 6.51 (для случая поля $\mathbb{R}$).

А именно, рассмотрим теперь систему линейных уравнений над полем $\mathbb{R}$

$$A\overrightarrow{x} = \overrightarrow{b}, \tag{102}$$

где A — матрица размера $m \times n$, $\overrightarrow{x}$ — столбец высоты n, $\overrightarrow{b}$ — столбец высоты m. Для нее можно определить *сопряженную* однородную систему $A^T\overrightarrow{y} = \overrightarrow{0}$, матрицей коэффициентов которой является A^T.

Следствие 12.9. *Система (102) при данном столбце правых частей $\overrightarrow{b}$ разрешима $\Leftrightarrow$ $\overrightarrow{b}$ ортогонален любому решению $\overrightarrow{y}$ сопряженной однородной системы (здесь ортогональность понимается в смысле "стандартного скалярного произведения", $\sum_{i=1}^m y_i b_i = 0$).*

Доказательство. Рассмотрим A как матрицу линейного отображения φ между евклидовыми пространствами относительно выбранных ортонормированных базисов, тогда матрицей сопряженного отображения φ^* (относительно тех же базисов) будет A^T. В базисах

$\operatorname{Im}\varphi$ описывается как подпространство таких столбцов в $\overrightarrow{b} \in \mathbb{R}^m$, для которых система (102) разрешима, а $\operatorname{Ker}\varphi^*$ — как подпространство таких столбцов $\overrightarrow{y} \in \mathbb{R}^m$, что $A^T\overrightarrow{y} = \overrightarrow{0}$. Тогда имеем серию эквивалентностей:
система (102) разрешима $\Leftrightarrow$ $\overrightarrow{b} \in \operatorname{Im}\varphi$ $\Leftrightarrow$ $\overrightarrow{b} \in (\operatorname{Ker}\varphi^*)^\perp$ $\Leftrightarrow$ $\overrightarrow{b}$ ортогонально любому $\overrightarrow{y}$ такому, что $A^T\overrightarrow{y} = \overrightarrow{0}$. ■

12.3 Самосопряженные преобразования

Пусть V — евклидово пространство, а $\varphi\colon V \to V$ — его линейное преобразование.

Определение 12.10. Преобразование φ называется *самосопряженным*, если оно совпадает со своим сопряженным, $\varphi = \varphi^*$.

То есть преобразование φ самосопряжено, если для любых u, $v \in V$ имеет место тождество

$$(\varphi(u),\, v) = (u,\, \varphi(v)).$$

Из пункта 1) Предложения 12.4 легко следует, что самосопряженные преобразования образуют линейное подпространство в пространстве $\mathcal{L}(V)$ всех линейных преобразований пространства V. Тождественное преобразование самосопряжено, также самосопряжены преобразования вида $\lambda\operatorname{Id}_V$, $\lambda \in \mathbb{R}$ (при любом выборе скалярного произведения в V).

Самосопряженность φ равносильна тому, что в произвольном базисе $\{e_1, \ldots, e_n\}$ пространства V с матрицей Грама G его матрица A удовлетворяет тождеству $A^TG = GA$. В частности, если базис ортонормирован, то самосопряженность преобразования φ равносильна симметричности его матрицы. Таким образом, *оператор самосопряжен тогда и только тогда, когда в некотором (а значит любом) ортонормированном базисе он имеет симметричную матрицу.*

Заметим, что если для преобразования евклидова пространства существует ортонормированный базис из собственных векторов, то это преобразование — самосопряженное. Действительно, в этом базисе матрица данного преобразования является диагональной, в частности, симметричной.

Оказывается, верно и обратное утверждение: если оператор самосопряжен, то для него существует ортонормированный базис из его собственных векторов. Доказательство этого утверждения потребует некоторой подготовки.

Предложение 12.11. *Пусть $\varphi\colon V \to V$ — линейное преобразование евклидова пространства V. Тогда $U \subset V$ φ-инвариантно $\Leftrightarrow$ $U^\perp \subset V$ φ^*-инвариантно.*

Доказательство. Пусть $U \subset V$ φ-инвариантно. Тогда

$$\forall\, u \in U,\ v \in U^\perp \quad 0 = (\varphi(u),\, v) = (u,\, \varphi^*(v)) \quad \Rightarrow \quad \varphi^*(v) \in U^\perp.$$

Тем самым мы доказали импликацию $\varphi(U) \subseteq U \quad \Rightarrow \quad \varphi^*(U^\perp) \subseteq (U^\perp)$. Применяя ее к последнему включению, получаем $\varphi^{**}((U^\perp)^\perp) \subseteq (U^\perp)^\perp$, то есть (поскольку $(U^\perp)^\perp = U$, $\varphi^{**} = \varphi$) $\varphi(U) \subseteq U$. ■

Замечание 12.12. В действительности это Предложение — следствие Предложения 8.23 с учетом Замечания 12.3 и того очевидного факта, что при изоморфизмах $\alpha_V : V \to V^*$ (см. параграф 11.3) ортогональное дополнение $U^\perp$ подпространства $U \subset V$ отождествляется с его аннулятором U^0.

Следствие 12.13. *Пусть $\varphi\colon V \to V$ — самосопряженное преобразование и $U \subset V$ является φ-инвариантым. Тогда $U^\perp \subset V$ также φ-инвариантно.*

Другими словами, ортогональное дополнение к инвариантому подпространству самосопряженного преобразования также является инвариантным подпространством.

Напомним, что преобразование $\varphi\colon V \to V$ называется *нильпотентным*, если $\varphi^k = 0$ для некоторого натурального k.

При решении следующей задачи нам понадобится также следующий тривиальный результат: если $\varphi\colon V \to V$ — самосопряженное преобразование евклидова пространства V и $U \subset V$ — φ-инвариантное подпространство, то ограничение $\varphi|_U : U \to U$ является самосопряженным преобразованием пространства U.

Задача 12.14. *Докажите, что нильпотентное самосопряженное преобразование евклидова пространства нулевое.*

Решение. Пусть $\varphi\colon V \to V$ — такое преобразование. Воспользуемся индукцией по $n = \dim V$. Если $n = 1$, то $\varphi = 0$. Пусть $n > 1$, и по предположению индукции результат верен для пространств размерности меньше n. Предположим, что $\varphi \neq 0$, тогда $0 \neq \operatorname{Ker}\varphi \subsetneq V$. Согласно предыдущему следствию, подпространство $(\operatorname{Ker}\varphi)^\perp \subset V$ является φ-инвариантным. По предположению индукции ограничение φ на него нулевое. Тогда $V = \operatorname{Ker}\varphi \oplus (\operatorname{Ker}\varphi)^\perp$ — прямая сумма инвариантных подпространств, ограничения на которые оператора φ равны нулю, откуда следует, что $\varphi = 0$.

Приведем еще одно доказательство. Пусть k — наименьшее натуральное, такое что $\varphi^k = 0$. Если $k \geq 2$, то $\forall\, v \in V\ (\varphi^{k-1}(v), \varphi^{k-1}(v)) = (\varphi^{k-2}(v), \varphi^k(v)) = 0$, откуда и $\varphi^{k-1} = 0$. ■

12.4 Связь между линейными операторами и билинейными функциями на евклидовом пространстве

Пусть V — евклидово пространство со скалярным произведением $(\cdot,\cdot)$, $\varphi\colon V \to V$ — линейный оператор. Определим по нему билинейную функцию $h = h_\varphi\colon V \times V \to \mathbb{R}$ по формуле

$$h(\mathbf{u}, \mathbf{v}) := (\mathbf{u}, \varphi(\mathbf{v})) \quad \forall\, \mathbf{u}, \mathbf{v} \in V. \tag{103}$$

Заметим, что и множество линейных операторов $V \to V$, и множество билинейных функций $V \times V \to \mathbb{R}$ являются линейными пространствами над $\mathbb{R}$ одной и той же размерности n^2, где $n = \dim V$ (например, в базисе оператор и билинейная функция однозначно задаются своими матрицами, причем любая матрица может быть как матрицей линейного оператора, так и матрицей билинейной функции). Пространство билинейных функций на V обозначим $\mathcal{B}(V)$, пространство линейных операторов на V — $\mathcal{L}(V)$.

Предложение 12.15. *1) Сопоставление $\varphi \mapsto h_\varphi$ (см. (103)) определяет изоморфизм линейных пространств $\alpha\colon \mathcal{L}(V) \to \mathcal{B}(V)$.*

2) При изоморфизме α симметричные билинейные функции отвечают самосопряженным операторам.

Доказательство. 1) Линейность отображения α очевидна. Так как пространства операторов и билинейных функций на V, как указывалось, имеют одинаковые размерности, то для доказательства того, что α — изоморфизм линейных пространств, достаточно доказать его инъективность.

Пусть $\varphi \neq 0$, тогда существует такой вектор $\mathbf{v} \in V$, что $\varphi(\mathbf{v}) \neq \mathbf{0}$. Кроме того, в силу невырожденности скалярного произведения существует вектор $\mathbf{u} \in V$ такой, что

$$(\mathbf{u},\, \varphi(\mathbf{v})) = h_\varphi(\mathbf{u},\, \mathbf{v}) \neq 0 \quad \Rightarrow \quad \alpha(\varphi) = h_\varphi \neq 0.$$

Таким образом, линейное отображение α — изоморфизм.

2) Проверим теперь второе утверждение. Действительно, для всех $\mathbf{u}$, $\mathbf{v} \in V$

$$h(\mathbf{u},\, \mathbf{v}) = h(\mathbf{v},\, \mathbf{u}) \quad \Leftrightarrow \quad (\mathbf{u},\, \varphi(\mathbf{v})) = (\mathbf{v},\, \varphi(\mathbf{u})) = (\varphi(\mathbf{u}),\, \mathbf{v}),$$

что равносильно самосопряженности оператора φ. ∎

Пусть $\mathcal{L}^{sa}(V)$ обозначает подпространство самосопряженных операторов в $\mathcal{L}(V)$. Тогда результат предыдущего Предложения можно представить как существование коммутативной диаграммы

$$\begin{array}{ccc} \mathcal{L}(V) & \xrightarrow{\ \alpha\ } & \mathcal{B}(V) \\ \cup\uparrow & & \uparrow\cup \\ \mathcal{L}^{sa}(V) & \xrightarrow{\ \alpha|_{\mathcal{L}^{sa}(V)}\ } & \mathcal{B}^{+}(V), \end{array}$$

в которой горизонтальные стрелки — определенные выше изоморфизмы, а вертикальные — включения подпространств.

Отметим, что построенный изоморфизм между пространствами $\mathcal{L}(V)$ и $\mathcal{B}(V)$ является каноническим (он не зависит ни от каких базисов, а только от скалярного произведения).

Таким образом, для любой билинейной симметричной функции h на евклидовом пространстве V существует единственный самосопряженный оператор $\varphi = \varphi_h$ на V, для которого выполнено (103). Такой оператор назовем *присоединенным* к соответствующей билинейной функции.

Пусть $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ — некоторый базис в V, в котором евклидово скалярное произведение $(\cdot, \cdot)$ имеет матрицу Грама G, билинейная форма h — матрицу H, а оператор φ_h — матрицу $A = A_\varphi$. Кроме того, пусть $\overrightarrow{u}$, $\overrightarrow{v}$ — координатные столбцы векторов $\mathbf{u}$, $\mathbf{v}$. Тогда (103) переписывается в виде

$$\overrightarrow{u}^T H \overrightarrow{v} = \overrightarrow{u}^T G A \overrightarrow{v} \quad \forall\, \overrightarrow{u},\, \overrightarrow{v} \quad \Leftrightarrow \quad H = GA \quad \Leftrightarrow \quad A = G^{-1}H. \tag{104}$$

В частности, если базис ортонормированный, то $G = E$, а значит, $A = H$.

12.5 Существование ортонормированного базиса из собственных векторов самосопряженного оператора

Данный раздел посвящен доказательству основной теоремы о самосопряженных операторах — существованию для них ортонормированного базиса из собственных векторов. Ключевым моментом доказательства является следующее Предложение.

Предложение 12.16. *Пусть $\varphi\colon V \to V$ — самосопряженное преобразование евклидова пространства V, $\dim V > 0$. Тогда у φ существует собственный вектор.*

В этом разделе мы приведем доказательство этого результата с использованием теоремы анализа о том, что непрерывная функция на компакте достигает нижней грани своих значений (то есть имеет минимум). Читатель, предпочитающий алгебраической доказательство (с помощью существования одномерного или двумерного инвариантных подпространств) может найти его в Добавлении в конце главы, а затем перейти к Теореме 12.18. Третье доказательство основной теоремы будет приведено в главе про унитарные пространства.

Для доказательства нам понадобится следующая лемма.

Лемма 12.17. Пусть $\psi\colon V \to V$ — самосопряженное преобразование такое, что $(v,\, \psi(v)) \geq 0\ \forall\, v \in V$. Тогда любой $e \in V$ такой, что $(e,\, \psi(e)) = 0$, лежит в ядре ψ.

Доказательство Леммы. Рассмотрим векторы вида $v = e + tu$, где $t \in \mathbb{R}$, а u — произвольный вектор из V. Имеем

$$(e + tu,\, \psi(e + tu)) = (e,\, \psi(e)) + t((u,\, \psi(e)) + (e,\, \psi(u))) + t^2(u,\, \psi(u)) =$$

$$= (u,\, \psi(u))t^2 + 2(u,\, \psi(e))t \geq 0 \quad \forall\, t \in \mathbb{R}$$

(выше мы воспользовались билинейностью и симметричностью скалярного произведения, условием $(e,\, \psi(e)) = 0$ и самосопряженностью оператора ψ). То есть мы получили выражение вида

$$at^2 + bt, \quad a,\, b \in \mathbb{R},$$

которое при любом $t \in \mathbb{R}$ неотрицательно. Если при этом $b \neq 0$, то выражение $at^2 + bt = (at + b)t$ меняет знак при $t = 0$, противоречие. Следовательно, $(u, \psi(e)) = 0 \quad \forall\, u \in V$, откуда из невырожденности скалярного произведения $\psi(e) = 0$. ∎

Доказательство Предложения. Ассоциируем с самосопряженным оператором $\varphi\colon V \to V$ билинейную функцию $h = h_\varphi$ на V по формуле (103)

$$h(u, v) = (u, \varphi(v)) \quad \forall\, u, v \in V.$$

Согласно Предложению 12.15, из самосопряженности φ следует, что h симметрична. Пусть $q\colon V \to \mathbb{R}$ — соответствующая h квадратичная форма, $q(v) = h(v, v) = (v, \varphi(v)) \quad \forall\, v \in V$. Легко видеть, что q — непрерывная функция на V относительно стандартной топологии на V (то есть топологии V как метрического пространства, см. раздел 11.6). Например, при выбранном базисе в V форма q — однородный многочлен второй степени от соответствующих координат.

Пусть

$$S(V) := \{v \in V \mid |v| = 1\}$$

— единичная сфера пространства V. Это — замкнутое (как множество нулей непрерывной функции $\sum_{i=1}^n x_i^2 - 1$, где x_i, $i = 1, \ldots, n$ — координаты относительно ортонормированного базиса) и ограниченное, а значит компактное подмножество в $\mathbb{R}^n \cong V$. Согласно известной теореме из анализа, ограничение функции q на $S(V)$ достигает нижней грани своих значений. Пусть

$$\lambda_0 := \min_{v \in S(V)} q(v) \quad \text{и} \quad q(e) = \lambda_0, \quad e \in S(V).$$

Тогда для любого $v \in S(V)$ верно неравенство $q(v) \geq \lambda_0(v, v)$, а значит последнее неравенство выполнено и для любого $v \in V$. (Действительно, для $v = 0$ оно очевидно, а для $v \neq 0$ $\exists$ единственный $u \in S(V)$ такой, что $v = tu, \quad t > 0$ и $q(v) = t^2 q(u), \quad (v, v) = t^2(u, u)$).

Имеем

$$q(v) - \lambda_0(v, v) = (v, \varphi(v)) - (v, \lambda_0 v) = (v, \varphi(v) - \lambda_0 v) =$$

$$= (v, (\varphi - \lambda_0 \mathrm{Id}_V)(v)) \geq 0 \quad \forall\, v \in V.$$

Пусть $\psi := \varphi - \lambda_0 \mathrm{Id}_V$, тогда последнее неравенство перепишется в виде $(v, \psi(v)) \geq 0 \quad \forall\, v \in V$. Кроме того, легко видеть, что для $e \in S(V)$ равенство $q(e) = \lambda_0$ равносильно $(e, \psi(e)) = 0$. Применяя теперь Лемму к самосопряженному преобразованию ψ и вектору e, получаем $\psi(e) = 0$, то есть $\varphi(e) = \lambda_0 e$, значит e — собственный вектор преобразования φ с собственным значением λ_0 (он ненулевой, поскольку принадлежит единичной сфере). ∎

Теперь мы в состоянии доказать основную теорему о самосопряженных преобразованиях.

Теорема 12.18. *Для любого самосопряженного преобразования $\varphi\colon V \to V$ существует ортонормированный базис в V, состоящий из его собственных векторов.*

Доказательство. Индукция по $n = \dim V$. Случай $n = 1$ очевиден. Пусть $n > 1$. Согласно предыдущему предложению, у φ в V есть собственный вектор v; без ограничения общности можно считать, что $|v| = 1$. Подпространство $U := \langle v \rangle \subset V$ является φ-инвариантным, по Следствию 12.13 $n-1$-мерное подпространство $U^\perp \subset V$ также φ-инвариантно. Легко проверить, что ограничение $\varphi|_{U^\perp}$ является самосопряженным преобразованием $U^\perp$. По предположению индукции для $\varphi|_{U^\perp}$ в $U^\perp$ существует ортонормированный базис из собственных векторов; добавляя к нему вектор v, получаем ортонормированнный базис в V, состоящий из собственных векторов оператора φ. ∎

Таким образом, самосопряженные преобразования евклидова пространства суть в точности такие преобразования, которые диагонализируются в некотором ортонормированном базисе.

Доказанная теорема вместе с доказательством Предложения дают алгоритм поиска собственных векторов и собственных значений самосопряженного оператора. А именно, ассоциируем с таким оператором квадратичную форму, как было сделано в доказательстве Предложения. Тогда наименьшее собственное значение равно минимуму этой квадратичной формы на единичной сфере, и точка сферы, в которой этот минимум достигается, является соответствующим собственным вектором. Далее берем ортогональное дополнение к одномерному подпространству, порожденному данным вектором и ищем минимум квадратичной формы на нем и т.д.

Пример 12.19. Рассмотрим квадратичную форму $q(\overrightarrow{x}) = x_1^2 + x_1x_2 + x_2^2$, заданную в ортонормированном базисе двумерного евклидова пространства. Ее минимум (соотв. максимум) на единичной сфере $x_1^2 + x_2^2 = 1$ достигается в точке, в которой x_1x_2 принимает минимальное (соотв. максимальное) значение при условии $x_1^2 + x_2^2 = 1$. Легко видеть, что эта точка имеет координаты $\pm(1/\sqrt{2},\ -1\sqrt{2})^T$ и минимальное значение q равно $1/2$ (соотв. $\pm(1/\sqrt{2},\ 1\sqrt{2})^T$ и максимальное значение q равно $3/2$). Тот же результат мы получим, решая задачу на собственные значения и собственные векторы для оператора, заданного матрицей $\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}$ (матрицы квадратичной формы и присоединенного к ней самосопряженного оператора совпадают, поскольку базис ортонормированный).

Заметим также, что если для положительно определенной квадратичной формы q ее минимум на единичной сфере равен λ_0 и достигается на векторе $v_0 \in S(V)$, то v_0 — направляющий вектор большой полуоси эллипсоида $q(v) = 1$, которая равна $1/\sqrt{\lambda_0}$. То же для максимума и малой полуоси. Таким образом, в нашем примере большая полуось эллипса $x_1^2 + x_1x_2 + x_2^2 = 1$ равна $\sqrt{2}$ и направлена по вектору $(1,\ -1)^T$, а малая равна $\sqrt{\frac{2}{3}}$ и ее направление задается вектором $(1,\ 1)^T$.

Ниже мы еще вернемся к применению самосопряженных операторов к теории квадратичных форм в евклидовом пространстве.

Следствие 12.20. *Для любой симметричной матрицы $A \in \mathrm{Mat}_n(\mathbb{R})$ существует ор-*

тогональная матрица $C \in \mathrm{Mat}_n(\mathbb{R})$ *такая, что* $C^T AC = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. *В частности, все корни характеристического многочлена вещественной симметричной матрицы вещественны.*

Доказательство. Рассмотрим n-мерное евклидово пространство V, фиксируем в нем ортонормированный базис и определим линейное преобразование $\varphi\colon V \to V$ как такое преобразование, которое имеет матрицу A в выбранном базисе. Из симметричности A следует, что φ самосопряжено. По доказанной теореме для φ существует ортонормированный базис из собственных векторов, в этом базисе матрица φ диагональна (на главной диагонали стоят его собственные значения). Если C — матрица перехода от исходного ортонормированного базиса к базису из собственных векторов, то она ортогональна и $C^{-1}AC = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Для завершения доказательства осталось лишь вспомнить определение ортогональной матрицы $C^{-1} = C^T$. ∎

Предложение 12.21. *Собственные подпространства* V_λ, V_μ *самосопряженного преобразования* $\varphi\colon V \to V$, *отвечающие разным собственным значениям* $\lambda \neq \mu$, *ортогональны:* $V_\lambda \perp V_\mu$.

Доказательство. Пусть $u \in V_\lambda$, $v \in V_\mu$. Тогда

$$\lambda(u, v) = (\varphi(u), v) = (u, \varphi(v)) = \mu(u, v),$$

то есть $(\lambda - \mu)(u, v) = 0$. Поскольку $\lambda - \mu \neq 0$, то $(u, v) = 0$. ∎

Таким образом, для самосопряженного преобразования $\varphi\colon V \to V$ существует разложение $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_s}$ пространства V в *ортогональную прямую сумму* собственных подпространств (единственное при условии $\lambda_1 < \lambda_2 < \ldots < \lambda_s$), причем ограничение φ на V_{λ_i} действует как скалярный оператор умножения на λ_i: для $v = v_1 + v_2 + \ldots + v_s$ с $v_i \in V_{\lambda_i}$

$$\varphi(v) = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_s v_s.$$

Задача 12.22. *a) Выясните, может ли матрица* A *являться матрицей самосопряженного оператора в евклидовом пространстве в некотором, не обязательно ортонормированном, базисе, если*

$$1)\ A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad 2)\ A = \begin{pmatrix} 2 & 1 \\ -1 & 4 \end{pmatrix} \quad 3)\ A = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}.$$

b) В случае положительного ответа предъявите (хотя бы одно) скалярное произведение, относительно которого оператор самосопряжен.

Решение. a) Если бы в условии речь шла про ортонормированный базис, то никакая из указанных матриц не могла бы быть матрицей самосопряженного оператора, поскольку

в этом случае она должна быть симметричной. Однако в условии речь идет про произвольный базис. Согласно доказанной выше теореме, оператор $f\colon V \to V$ на евклидовом пространстве V самосопряжен $\Leftrightarrow$ он диагонализируется в ортонормированном базисе (состоящем из собственных векторов) и имеет вещественный спектр. То есть если оператор самосопряжен, то его матрица имеет вещественный спектр и диагонализируема (существует базис пространства из ее собственных векторов).

В случае 1) характеристический многочлен

$$\chi_A(t) = t^2 - (\operatorname{tr} A)\, t + \det A = t^2 - 2t + 2$$

имеет отрицательный дискриминант, поэтому собственные значения оператора с этой матрицей не являются вещественными.

В случае 2) характеристический многочлен

$$\chi_A(t) = t^2 - (\operatorname{tr} A)\, t + \det A = t^2 - 6t + 9 = (t-3)^2$$

имеет кратный корень; поэтому не выполнено достаточное условие диагонализируемости (что спектр оператора прост), и простое вычисление показывает, что размерность собственного подпространства равна 1, значит, не существует базиса двумерного пространства V, состоящего из собственных векторов, следовательно оператор не диагонализируем.

В случае 3) характеристический многочлен

$$\chi_A(t) = t^2 - (\operatorname{tr} A)\, t + \det A = t^2 - t - 2 = (t+1)(t-2)$$

имеет два различных вещественных корня, следовательно, он диагонализируем и имеет вещественный спектр. Таким образом, матрица п. 3) может быть матрицей самосопряженного оператора.

b) Чтобы найти скалярное произведение, относительно которого матрица A из п. 3) является матрицей самосопряженного оператора, найдем некоторый базис из собственных векторов и объявим его ортонормированным (ясно, что этим скалярное произведение будет однозначно определено). Например, в качестве такого базиса можно взять $\{\mathbf{v}\} := \{\mathbf{v}_1, \mathbf{v}_2\}$, где $\mathbf{v}_1 = (1, -1)^T$, $\mathbf{v}_2 = (1, 2)^T$.

Для лучшего понимания полезно провести независимую проверку ответа пункта b). По определению, матрица Грама полученного скалярного произведения в базисе $\{\mathbf{v}_1, \mathbf{v}_2\}$ есть единичная матрица E. Матрица перехода $C := C_{\{\mathbf{e}\}\to\{\mathbf{v}\}}$ от стандартного базиса $\{\mathbf{e}\} := \{\mathbf{e}_1, \mathbf{e}_2\}$, $\mathbf{e}_1 = (1, 0)^T$, $\mathbf{e}_2 = (0, 1)^T$ (относительно которого задана исходная матрица A) к базису $\{\mathbf{v}\}$ есть $C = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$. Таким образом, матрица Грама G относительно стандартного базиса $\{\mathbf{e}\}$ есть

$$G = (C^{-1})^T C^{-1} = \frac{1}{9} \begin{pmatrix} 5 & -1 \\ -1 & 2 \end{pmatrix}.$$

Простое вычисление теперь показывает, что матричное равенство $A^T G = GA$ действительно выполняется, а оно как раз и говорит о том, что матрица A является матрицей самосопряженного оператора относительно скалярного произведения с матрицей Грама G. ■

Напомним (см. Пример 8.5), что проекторами называются операторы φ, удовлетворяющие тождеству $\varphi^2 = \varphi$.

Задача 12.23. *Опишите проекторы на евклидовом пространстве, которые являются самосопряженными преобразованиями.*

Решение. В Примере 8.5 было показано, что всякий проектор, то есть оператор $\varphi\colon V \to V$, удовлетворяющий соотношению $\varphi^2 = \varphi$, является оператором проектирования на подпространство $U := \operatorname{Im}\varphi$ параллельно подпространству $W := \operatorname{Ker}\varphi$. Одновременно подпространства U и W (в случае, если они ненулевые) являются собственными подпространствами оператора φ с собственными значениями соответственно 1 и 0. Так как собственные подпространства самосопряженного оператора, отвечающие разным собственным значениям, ортогональны, то необходимым условием самосопряженности проектора является ортогональность U и W, откуда (ввиду $V = U \oplus W$) $W = U^\perp$. В этом случае проектор есть оператор ортогонального проектирования на подпространство $U \subset V$. Это условие является также достаточным: действительно, если v, $v' \in V$ и φ — ортогональный проектор, то $(\varphi(v),\, v') = (\varphi(v),\, \varphi(v')) = (v,\, \varphi(v'))$. ■

Задача 12.24. *Матрица*

$$\frac{1}{6}\begin{pmatrix} 5 & -2 & ? \\ -2 & 2 & ? \\ -1 & -2 & ? \end{pmatrix}$$

с неизвестным третьим столбцом является матрицей ортогонального проектора на двумерное подпространство в ортонормированном базисе. Восстановите неизвестный столбец.

Пусть $V = V_1 \oplus \ldots \oplus V_s$ — разложение евклидова пространства V в ортогональную прямую сумму своих подпространств. По нему строится система ортогональных (=самосопряженных в силу Задачи 12.23) проекторов $P_1, \ldots, P_s\colon V \to V$, $\operatorname{Im} P_i = V_i$, $1 \le i \le s$. Читатель легко убедится, что такая система проекторов обладает следующими свойствами:

$$P_i^2 = P_i,\quad P_i^* = P_i,\quad P_i P_j = 0 \ \text{ при } \ i \ne j \ \text{ и } \ \sum_{i=1}^{s} P_i = \mathrm{Id}_V. \tag{105}$$

Обратно, если дана система проекторов $P_1, \ldots, P_s$ на пространстве V, обладающая свойствами (105), то по ней строится разложение пространства V в ортогональную прямую сумму подпространств $V_i := \operatorname{Im} P_i$. В самом деле, применяя последнее из условий (105) к произвольному вектору из V, получаем $V = V_1 + \ldots + V_s$. Проверим, что последняя сумма прямая. Последовательно применяя к $P_1(v_1) + \ldots + P_s(v_s) = 0$ операторы P_j, $1 \le j \le s$ и используя первое и третье равенство из (105), получаем $P_j(v_j) = 0$, $1 \le j \le s$,

то есть подпространства $V_1, \ldots, V_s$ линейно независимы. Наконец, с учетом ортогональности проекторов третье условие из (105) обеспечивает взаимную ортогональность подпространств $V_1, \ldots, V_s$.

Систему $P_1, \ldots, P_s$ проекторов на V, обладающую свойствами (105), назовем *полной системой ортогональных проекторов* на V.

Пусть теперь $\varphi\colon V \to V$ — самосопряженный оператор, $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_s}$ — разложение пространства V в ортогональную прямую сумму его собственных подпространств и $P_1, \ldots, P_s$ — отвечающая этому разложению полная система проекторов на V. Как легко проверит читатель, имеет место равенство операторов

$$\varphi = \sum_{i=1}^{s} \lambda_i P_i, \tag{106}$$

называемое *спектральным разложением* самосопряженного оператора (ср. Замечание 8.49).

Предложение 12.25. *Для самосопряженного оператора φ спектральное разложение единственно.*

Доказательство. Пусть $\psi := \sum_{i=1}^{s} \lambda_i P_i$ ($\lambda_i \neq \lambda_j$ при $i \neq j$) — оператор, отвечающий некоторой полной системе ортогональных проекторов $P_1, \ldots, P_s$ на V. Он самосопряженный, так как является линейной комбинацией самосопряженных проекторов (а самосопряженные операторы, как мы знаем, образуют вещественное линейное подпространство в пространстве всех операторов). Тогда для $1 \leq j \leq s$ $\operatorname{Im} P_j \subseteq V_{\lambda_j}$, где V_{λ_j} — собственное подпространство оператора ψ, отвечающее собственному значению λ_j. В самом деле, $\forall\, v \in V$ $(\sum_{i=1}^{s} \lambda_i P_i)(P_j(v)) = \lambda_j P_j^2(v) = \lambda_j P_j(v)$. С другой стороны, так как $P_1, \ldots, P_s$ — полная система проекторов, то $V = \operatorname{Im} P_1 \oplus \ldots \oplus \operatorname{Im} P_s$. Значит на самом деле $\operatorname{Im} P_i = V_{\lambda_i}$, $1 \leq i \leq s$. То есть любое спектральное разложение самосопряженного оператора является линейной комбинацией ортогональных проекторов на его собственные подпространства с коэффициентами, равными соответствующим собственным значениям, и значит однозначно строится по самосопряженному оператору. ■

Заметим, что, более общо, спектральное разложение единственно для произвольного диагонализируемого оператора (читатель может доказать это самостоятельно).

Задача 12.26. *Пусть V — евклидово пространство из Примера 11.5. Пусть $\tau\colon V \to V$, $\tau(X) = X^T$ — линейный оператор на V, сопоставляющий произвольной матрице ее транспонированную. Покажите, что τ самосопряжен. Выведите из этого результат Задачи 11.7.*

Решение. Самосопряженность τ следует из выкладки:

$$(\tau(X), Y) = \operatorname{tr}(\tau(X)^T Y) = \operatorname{tr}(XY) = \operatorname{tr}(YX) = \operatorname{tr}(X^T Y^T) = (X, \tau(Y)).$$

Заметим (см. Пример 8.27), что подпространства симметричных (кососимметричных) матриц — в точности собственные подпространства оператора τ, отвечающие собственному значению 1 (соответственно -1). Теперь требуемый результат вытекает из предыдущего Предложения. ■

Задача 12.27. *Докажите, что два самосопряженных преобразования $\varphi, \psi\colon V \to V$ коммутируют (то есть $\varphi\psi = \psi\varphi$) тогда и только тогда, когда в V есть ортонормированный базис, состоящий из их общих собственных векторов (ср. Задачу 8.63).*

Решение. Пусть $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_s}$ — разложение пространства V в ортогональную прямую сумму собственных подпространств оператора φ. Из условия следует, что операторы ψ и $\varphi - \lambda_i \mathrm{Id}_V$ коммутируют, поэтому подпространства $V_{\lambda_i} = \mathrm{Ker}\,(\varphi - \lambda_i \mathrm{Id}_V)$ являются ψ-инвариантными. Для каждого i, $i = 1, \ldots, s$ ограничение $\psi|_{V_{\lambda_i}} : V_{\lambda_i} \to V_{\lambda_i}$ является самосопряженным оператором на V_{λ_i}, поэтому для него в V_{λ_i} существует ортонормированный базис из собственных векторов. Заметим, что эти базисные векторы также будут собственными векторами (с собственным значением λ_i) оператора φ. Поскольку подпространства V_{λ_i} при разных i попарно ортогональны, объединение таких базисов даст ортонормированный базис пространства V, состоящий из одновременных собственных векторов операторов φ и ψ.

В другую сторону утверждение очевидно, поскольку в общем базисе из собственных векторов операторы записываются диагональными матрицами, которые коммутируют. ■

Замечание 12.28. Пусть V — евклидово пространство. Выше мы определили линейный оператор $*\colon \mathcal{L}(V) \to \mathcal{L}(V)$, $\varphi \mapsto \varphi^*$ "взятия сопряженного". Из $** = \mathrm{Id}_{\mathcal{L}(V)}$ следует, что его собственными значениями могут быть только ± 1. Его собственными векторами с собственным значением 1 являются ненулевые самосопряженные операторы $\varphi^* = \varphi$, а собственными векторами с собственным значением -1 — ненулевые *кососимметрические операторы* $\varphi^* = -\varphi$. Их название оправдывается тем, что это — в точности те операторы, которые имеют кососимметрические матрицы в ортонормированных базисах[57]. Примером такого оператора в ориентированном трехмерном евклидовом пространстве V является оператор взятия векторного произведения с фиксированным вектором: $\varphi_w\colon V \to V$, $\varphi_w(v) = [w, v]$. В самом деле, для любых $u, v \in V$ имеем $(\varphi_w(u), v) + (u, \varphi_w(v)) = 0$. Заметим, что любой оператор на евклидовом пространстве V единственным образом представляется в виде суммы самосопряженного и кососимметрического:

$$\varphi = \frac{\varphi + \varphi^*}{2} + \frac{\varphi - \varphi^*}{2}$$

(это аналог представления любой квадратной матрицы в виде суммы симметричной и кососимметричной). Свойства кососимметрических операторов описаны в Задаче 12.68.

12.6 Билинейные и квадратичные формы в евклидовом пространстве

Выведем теперь ряд результатов о квадратичных (симметричных билинейных) функциях на евклидовом пространстве, используя их связь с самосопряженными операторами, описанную в Предложении 12.15.

Предложение 12.29. *Для любой симметричной билинейной (или квадратичной) формы на евклидовом пространстве существует ортонормированный базис, в котором ее матрица диагональна (для квадратичной формы последнее означает, что в соответствующих координатах она имеет вид $q(\overrightarrow{x}) = \sum_k \lambda_k x_k^2$).*

Доказательство. Пусть h — симметричная билинейная форма. Пусть φ_h — ее присоединенный самосопряженный оператор. Так как для φ_h существует ортонормированный базис

[57] Заметим, что самосопряженные операторы часто также называются симметрическими.

из собственных векторов, а в таком базисе, как мы знаем, его матрица A диагональна, то и матрица H билинейной формы h в этом базисе тоже диагональна (точнее, она просто равна A, поскольку базис ортонормированный). ■

Полезно сопоставить доказанное Предложение с Предложением 10.35. Новое Предложение сильнее старого в том отношении, что в нем утверждается существование не произвольного, а ортонормированного базиса, в котором квадратичная функция имеет диагональный вид, в то же время слабее старого в том отношении, что ненулевые λ_i не обязательно равны ± 1. Смысл нового Предложения состоит в том, что в евклидовых пространствах существует более тонкое отношение эквивалентности на квадратичных формах, которое сохраняет не только аффинную, но и метрическую информацию (такую как длины полуосей эллипсоида $\{v \in V \mid q(v) = 1\}$ в случае положительно определенной квадратичной функции q), которую как раз и несут числа λ_i.

Доказанный результат можно использовать для приведения уравнения кривой 2-го порядка к каноническому виду. А именно, пусть

$$a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + a_0 = 0 \tag{107}$$

— уравнение кривой второго порядка, заданное в прямоугольной системе координат Ox_1x_2 на плоскости. Напомним, что первый шаг алгоритма приведения к каноническому виду заключается в нахождении новой прямоугольной системы координат $Ox'_1x'_2$, в которой коэффициент перед $x'_1x'_2$ равен 0. Для этого рассмотрим квадратичную форму q, определенную равенством

$$q(\overrightarrow{x}) := a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$$

в ортонормированном базисе евклидовой плоскости. Согласно доказанному выше, для q существует ортонормированный базис, в котором она имеет диагональный вид $q(\overrightarrow{x}') = \lambda_1 x_1'^2 + \lambda_2 x_2'^2$. Эквивалентно, если C является матрицей перехода к такому базису, то она ортогональна и для $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$ справедливо равенство $C^TAC = \operatorname{diag}(\lambda_1, \lambda_2)$. Матрица C определяет в плоскости замену системы координат $\overrightarrow{x} = C\overrightarrow{x}'$ такую, что в новой системе уравнение (107) принимает вид

$$\lambda_1 x_1'^2 + \lambda_2 x_2'^2 + 2a'_1x'_1 + 2a'_2x'_2 + a'_0 = 0.$$

Далее, выделяя полные квадраты, находим параллельный перенос, приводящий уравнение кривой к (почти) каноническому виду. Этот же алгоритм работает и в случае уравнений поверхностей 2-го порядка.

Предложение 12.30. *Пусть V — векторное пространство над $\mathbb{R}$, g, h — две билинейные симметричные формы на V, причем g положительно определена. Тогда в V существует базис, в котором матрица Грама первой формы $G = E$, а матрица H второй формы h диагональна.*

Доказательство. Так как g положительно определена, то $(V,\, g)$ — евклидово пространство. Пусть φ_h — самосопряженный оператор в этом евклидовом пространстве, присоединенный к h (обратим внимание читателя, что сопоставление $h \mapsto \varphi_h$ зависит и от g). Тогда для построенного нами самосопряженного оператора φ_h существует ортонормированный базис из собственных векторов. В этом базисе мы имеем $G = E$, $A = H$ и A диагональна (с собственными значениями φ_h на главной диагонали). ■

Заметим, что случай, когда в условии предыдущего Предложения g отрицательно определена, сводится к рассмотренному заменой $g' = -g$.

Переформулируем полученный результат в матричном виде.

Следствие 12.31. *Для любых двух вещественных симметричных матриц G и H одинакового порядка n, где G положительно определена, существует невырожденная матрица C того же порядка такая, что $C^T G C = E$, $C^T H C = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.*

Изложим теперь алгоритм приведения пары форм к диагональному виду. Пусть в некотором базисе пространства V форма g имеет матрицу G, а форма h — матрицу H, тогда матрица оператора $\varphi = \varphi_h$ есть $A = A_\varphi = G^{-1}H$. Имеем

$$\det(A - \lambda E) = \det(G^{-1}H - \lambda E) = \det(G^{-1}H - \lambda G^{-1}G) =$$

$$= \det(G^{-1}(H - \lambda G)) = \det(G^{-1}) \det(H - \lambda G).$$

Таким образом, собственные значения φ совпадают с корнями "обобщенного характеристического уравнения" $\det(H - \lambda G) = 0$ (так как A — матрица самосопряженного оператора, то все они вещественны). Пусть λ_k — некоторый корень. Тогда соответствующие собственные векторы находятся как (ненулевые) решения системы линейных однородных уравнений $(A - \lambda_k E)\overrightarrow{v} = \overrightarrow{0}$ (здесь $\overrightarrow{v}$ — неизвестный столбец координат собственного вектора $\mathbf{v}$). Данная система эквивалентна системе $(H - \lambda_k G)\overrightarrow{v} = \overrightarrow{0}$. Заметим, что собственные векторы, отвечающие разным собственным значениям, автоматически будут ортогональны относительно g. В случае кратного собственного значения λ_k (например, для положительно определенной формы этот случай отвечает эллипсоиду вращения) базисные векторы из соответствующего собственного подпространства нужно ортогонализовать отдельно (например, с помощью алгоритма Грама–Шмидта) относительно матрицы Грама G. Далее полученный ортогональный базис, опять же используя матрицу G, нужно нормировать. В полученном ортонормированном относительно формы g базисе матрица Грама формы g будет единичной E, а матрица h — диагональной $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.

Замечание 12.32. Приведем пример пары квадратичных форм, которые не приводятся одновременно к диагональному виду. Ясно, что такой пример нужно искать среди форм, ни одна из которых не является знакоопределенной.

Рассмотрим квадратичные формы в двумерном пространстве, имеющие в некотором базисе матрицы

$$K = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{и} \quad H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Пусть $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — матрица перехода к новому базису. Тогда в нем квадратичные формы будут иметь матрицы

$$S^T K S = \begin{pmatrix} a^2 - c^2 & ab - cd \\ ab - cd & b^2 - d^2 \end{pmatrix} \quad \text{и} \quad S^T H S = \begin{pmatrix} 2ac & ad + bc \\ ad + bc & 2bd \end{pmatrix}.$$

Если они обе диагональны, то элементы матрицы перехода удовлетворяют системе

$$\begin{cases} ab - cd = 0 & (1) \\ ad + bc = 0. & (2) \end{cases}$$

Тогда $b(1) + d(2) = a(b^2 + d^2) = 0$, а также $d(1) - b(2) = c(b^2 + d^2) = 0$. В то же время из обратимости S следует, что $b^2 + d^2 \neq 0$, значит, $a = c = 0$ — противоречие.

Замечание 12.33. Отметим два применения результатов данного параграфа: во-первых, к теории малых колебаний [4, 5]; во-вторых, при изучении дифференциальной геометрии поверхностей в $\mathbb{R}^3$ (определение главных кривизн и главных направлений), см. например [18].

12.7 Ортогональные преобразования

Пусть V — евклидово пространство, а $\varphi\colon V \to V$ — его линейное преобразование.

Определение 12.34. Преобразование φ называется *ортогональным*, если оно сохраняет скалярное произведение, то есть

$$\forall\, u,\, v \in V \quad (\varphi(u),\, \varphi(v)) = (u,\, v). \tag{108}$$

Вспоминая определение изометрии евклидовых пространств мы видим, что ортогональное преобразование — то же что изометрия евклидова пространства с самим собой.

Так как длины векторов и углы между векторами выражаются через скалярные произведения, то ортогональные преобразования их тоже сохраняют.

Замечание 12.35. Так как изометрия автоматически линейна (см. Задачу 11.26), условие линейности в определении ортогонального преобразования можно опустить.

Перепишем соотношение (108) в матричном виде. Выберем произвольный базис в V, пусть G — его матрица Грама, и пусть φ имеет в нем матрицу A. Тогда легко видеть, что (108) равносильно матричному соотношению

$$A^T G A = G. \tag{109}$$

В частности, если базис ортонормированный, то ортогональность преобразования равносильна соотношению $A^TA = E$, то есть ортогональности его матрицы. Таким образом, *оператор ортогональный тогда и только тогда, когда в некотором (а значит любом) ортонормированном базисе он имеет ортогональную матрицу.* В частности, любой такой оператор обратим и его определитель равен ± 1.

Из (108) легко следует, что ортогональность φ равносильна соотношению $\varphi^*\varphi = \mathrm{Id}_V$, то есть $\varphi^* = \varphi^{-1}$. Это еще раз показывает, что любое ортогональное преобразование обратимо.

Предложение 12.36. *Ортогональные преобразования евклидова пространства V образуют группу относительно операции композиции.*

Эта группа обозначается $\mathrm{O}(V)$ и называется *ортогональной группой* пространства V. Она является подгруппой группы $\mathrm{GL}(V)$ всех обратимых (=невырожденных) преобразований пространства V.

Доказательство. Достаточно проверить непустоту множества ортогональных преобразований и его замкнутость относительно композиции и взятия обратного. Легко видеть, что тождественное преобразование Id_V ортогонально. Если φ, $\psi \in \mathrm{O}(V)$, то

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^* = \varphi^{-1} \circ \psi^{-1} = (\psi \circ \varphi)^{-1},$$

то есть $\psi \circ \varphi \in \mathrm{O}(V)$.

Пусть теперь $\varphi \in \mathrm{O}(V)$, проверим что и $\varphi^{-1} \in \mathrm{O}(V)$. Для этого докажем что для любого обратимого преобразования φ справедливо $(\varphi^{-1})^* = (\varphi^*)^{-1}$. Действительно,

$$\mathrm{Id}_V = (\mathrm{Id}_V)^* = (\varphi\varphi^{-1})^* = (\varphi^{-1})^*\varphi^*,$$

откуда и следует требуемое. Тогда если φ ортогонален, то для $\psi := \varphi^{-1}$ имеем

$$\psi^* = (\varphi^{-1})^* = (\varphi^*)^{-1} = (\varphi^{-1})^{-1} = \psi^{-1}. \quad \blacksquare$$

Ортогональные преобразования пространства V с определителем 1 образуют подгруппу группы $\mathrm{O}(V)$, обозначаемую $\mathrm{SO}(V)$ и называемую *специальной ортогональной группой* пространства V. Она состоит из поворотов.

Выбор ортонормированного базиса в V определяет изоморфизм группы $\mathrm{O}(V)$ с группой $\mathrm{O}(n)$ ортогональных матриц порядка n (соответственно группы $\mathrm{SO}(V)$ с группой $\mathrm{SO}(n)$ ортогональных матриц порядка n с определителем 1).

В отличие от самосопряженных преобразований, ортогональные не обязательно диагонализируемы. Это связано с тем, что корни их характеристического многочлена не обязательно вещественны (посмотрите, например, на поворот на угол $\pi/2$ в евклидовой плоскости). Однако если они вещественны, то равны ± 1.

Предложение 12.37. *Собственные значения ортогонального преобразования равны* ± 1.

Доказательство. Пусть ортогональное преобразование φ имеет собственное значение $\lambda \in \mathbb{R}$ и $v \in V$ — соответствующий собственный вектор. Имеем

$$\lambda^2(v,\, v) = (\varphi(v),\, \varphi(v)) = (v,\, v).$$

Так как $(v,\, v) \neq 0$, то $\lambda^2 = 1$. ∎

Например, направляющий вектор оси поворота φ в трехмерном пространстве — собственный вектор φ с собственным значением 1.

Можно доказать (см. параграф 12.9 ниже) что корни характеристического многочлена ортогонального преобразования лежат на единичной окружности в комплексной плоскости (причем из вещественности коэффициентов характеристического многочлена следует что вместе с каждым комплексным корнем λ комплексно сопряженное к нему число $\overline{\lambda}$ также будет корнем). Поэтому если они вещественны, то обязаны быть равными ± 1.

Предложение 12.38. *Если* $U \subset V$ *— инвариантное подпространство для ортогонального преобразования* $\varphi\colon V \to V$*, то его ортогональное дополнение* $U^\perp \subset V$ *также* φ*-инвариантно.*

Доказательство. Заметим, что из ортогональности φ следует ортогональность ограничения $\varphi|_U$, которое поэтому биективно (как преобразование U). То есть для любого $u \in U$ существует единственный $u' \in U$ такой что $\varphi(u') = u$.

Возьмем теперь произвольный $v \in U^\perp$, тогда

$$\forall\, u \in U \quad (u,\, \varphi(v)) = (\varphi(u'),\, \varphi(v)) = (u',\, v) = 0,$$

откуда $\varphi(v) \in U^\perp$. ∎

Например, для поворота вокруг некоторой оси в трехмерном пространстве ортогональное дополнение к этой оси инвариантно.

Теорема 12.39. *Пусть* V *— евклидово пространство,* $\dim V = 3$*. Пусть* $\varphi\colon V \to V$ *— ортогональное преобразование. Тогда в* V *найдется такой ортонормированный базис, в котором матрица* φ *имеет вид*

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \tag{110}$$

причем элемент, стоящий в правом нижнем углу матрицы A*, равен* $\det\varphi$*.*

Доказательство. Во-первых докажем, что у φ есть собственный вектор w с собственным значением $\det\varphi$. Это равносильно тому, что $\det\varphi$ является корнем характеристического

многочлена φ. Данный многочлен $\chi_\varphi(t) \in \mathbb{R}[t]$ имеет степень 3, и поэтому у него есть вещественный корень, причем равный ± 1 (поскольку это — собственное значение ортогонального оператора). Пусть λ_1, λ_2, λ_3 — все (в том числе комплексные) корни многочлена $\chi_\varphi(t)$, причем $\lambda_1 \in \mathbb{R}$. Тогда $\det\varphi = \lambda_1\lambda_2\lambda_3$. Возможно два варианта. 1) Не все корни $\chi_\varphi(t)$ вещественны, и тогда $\lambda_3 = \overline{\lambda}_2$, поэтому $\det\varphi = \lambda_1|\lambda_2|^2$, а так как $|\lambda_2|^2 > 0$, то, сравнивая модули левой и правой частей в предыдущем равенстве, получаем $|\lambda_2|^2 = 1$, и тогда $\det\varphi = \lambda_1$. 2) Все корни $\chi_\varphi(t)$ вещественны, и значит являются собственными значениями φ, которые как мы знаем равны ± 1. Из этого легко следует требуемое.

Таким образом, пусть w — нормированный собственный вектор φ с собственным значением $\det\varphi$. Тогда согласно предыдущему Предложению 2-мерное подпространство $U := \langle w\rangle^\perp \subset V$ является φ-инвариантным, и ограничение $\varphi|_U$ на него является ортогональным преобразованием U с определителем 1. Мы знаем, что такое преобразование является поворотом в U на некоторый угол α и в произвольном ортонормированном базисе $\{u, v\}$ в U имеет матрицу

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Таким образом, в ортонормированном базисе $\{u, v, w\}$ пространства V оператор φ имеет матрицу требуемого вида. ∎

Следствие 12.40. *Всякое сохраняющее ориентацию ортогональное преобразование трехмерного евклидова пространства является поворотом вокруг некоторой оси.*

Приведем алгоритм решения задачи о нахождении канонического вида (110) и базиса ортогональной матрицы A порядка 3. Читатель должен обосновать каждый его шаг с использованием изложенной теории. Мы считаем, что матрица A является матрицей ортогонального оператора φ в некотором ортонормированном базисе трехмерного евклидова пространства V.

Во-первых, посчитаем $\varepsilon := \det A$. Это дает нам элемент в правом нижнем углу в (110). Из инвариантности следа матрицы оператора получаем $\operatorname{tr} A = \varepsilon + 2\cos\alpha$, откуда $\cos\alpha = \frac{1}{2}(\operatorname{tr} A - \varepsilon)$. В качестве $\sin\alpha$ можно выбрать любое значение, удовлетворяющее основному тригонометрическому тождеству $\cos^2\alpha + \sin^2\alpha = 1$. Далее находим собственное подпространство V_ε с собственным значением ε.

Заметим, что если $\dim V_\varepsilon > 1$, то наш оператор диагонализируем в ортонормированном базисе, поэтому соответствующий оператор φ не только ортогонален, но и самосопряжен (и значит исходная матрица A не только ортогональна, но и симметрична). Это отвечает случаю, когда $\alpha = 0$ или π.

Пусть w — нормированный собственный вектор с собственным значением ε. Тогда ортогональное дополнение $\langle w\rangle^\perp$ двумерно и φ-инвариантно, причем ограничение φ на него является собственным (сохраняющим ориентацию) ортогональным оператором, значит имеет в ортонормированном базисе в $\langle w\rangle^\perp$ матрицу поворота на угол α или $-\alpha$, в зависимости

от выбранного порядка базисных векторов. Пусть $\{u, v\}$ — некоторый ортонормированный базис в $\langle w\rangle^\perp$, тогда $\{u, v, w\}$ — ортонормированный базис в V, в котором φ имеет матрицу вида (110), но, возможно, с противоположными знаками у синусов (ведь когда мы выбирали одно из двух (в общем случае) значений $\sin\alpha$, отвечающих $\cos\alpha$, у нас был произвол в выборе знака), и теперь выбор знака у $\sin\alpha$ нужно согласовать с выбором ориентации базиса в плоскости $\langle w\rangle^\perp$ ($\{u, v\}$ или $\{v, u\}$). Для этого нужно проверить, будет ли Au (здесь и далее векторы u, v, w отождествляются с соответствующими столбцами) равно $\cos\alpha\, u + \sin\alpha\, v$, или же $\cos\alpha\, u - \sin\alpha\, v$, во втором случае нужно вместо $\{u, v, w\}$ взять базис $\{v, u, w\}$ (или изменить знак у синуса).

Задача 12.41. *Опишите преобразования евклидова пространства, которые являются одновременно самосопряженными и ортогональными.*

Решение. Пусть $\varphi\colon V \to V$ — такое преобразование. Так как φ является самосопряженным, то V является ортогональной прямой суммой его собственных подпространств. Так как φ является ортогональным, то возможны только собственные значения ±1. Таким образом, (за исключением тривиальных случаев $\varphi = \pm\mathrm{Id}_V$) $V = V_1 \oplus V_{-1}$, причем $V_{-1} = (V_1)^\perp$. Если $v = v^+ + v^-$ — соответствующее разложение вектора $v \in V$, то $\varphi(v) = v^+ - v^-$, откуда следует, что φ является ортогональным отражением относительно подпространства V_1.

Другой способ решения данной задачи можно получить с помощью Примеров 8.6 и 8.27. Во-первых, заметим, что любые два из условий 1) $\varphi^* = \varphi$, 2) $\varphi^*\varphi = \mathrm{Id}_V$, 3) $\varphi^2 = \mathrm{Id}_V$ влекут третье. Таким образом, оператор, являющийся одновременно самосопряженным и ортогональным, удовлетворяет тождеству $\varphi^2 = \mathrm{Id}_V$, а значит, согласно Примеру 8.6, является отражением относительно подпространства V^+ параллельно V^-. Но так как φ самосопряжен, то $V^+ = (V^-)^\perp$, то есть φ — ортогональное отражение.

Пример такого оператора был приведен, например, в Задаче 12.26. ■

Задача 12.42. *Пусть V — евклидова плоскость, и оператор $\varphi\colon V \to V$ имеет матрицу* $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$ *в некотором ортонормированном базисе V. Без вычислений на бумаге укажите его диагональный вид и геометрический смысл.*

Задача 12.43. [58] *Выше мы видели определения самосопряженных $\varphi^* = \varphi$ и кососимметричных $\varphi^* = -\varphi$ операторов, а также ортогональных операторов $\varphi^* = \varphi^{-1}$. Естественно спросить, что можно сказать про "кососортогональные" операторы, задаваемые равенством $\varphi^* = -\varphi^{-1}$?*

Замечание 12.44. В современной физике большую роль играют так называемые псевдоевклидовы пространства, которые состоят из (конечномерного) вещественного векторного пространства и заданной на нем невырожденной квадратичной формы (которая, в отличие

[58] Сообщена автору И.И. Богдановым.

от евклидового случая, не предполагается, вообще говоря, положительно определенной). Примером такого пространства является пространство Минковского, которое является четырехмерным вещественным пространством с квадратичной формой сигнатуры $(3,1)$. Для такой формы существует базис, в котором она имеет вид $q(x) = x_1^2 + x_2^2 + x_3^2 - x_4^2$. Группа, сохраняющая данную форму, называется группой Лоренца. В ортонормированном базисе она состоит из матриц A, удовлетворяющих соотношению (109), где $G = \operatorname{diag}(1,1,1,-1)$.

12.8 Полярное и сингулярное разложения

Связь между самосопряженными операторами и билинейными симметрическими (квадратичными) функциями, описанная в Предложении 12.15, позволяет перенести на самосопряженные операторы такие понятия, как положительная (полу)определенность и т.д.

Определение 12.45. Самосопряженный оператор $\varphi\colon V \to V$ на евклидовом пространстве V называется *положительным* (соответственно *неотрицательным*), если соответствующая ему квадратичная функция q_φ положительно (соответственно неотрицательно) определена.

Предложение 12.46. *Пусть $\varphi\colon V \to V$ — произвольный (не обязательно самосопряженный) линейный оператор на евклидовом пространстве V. Тогда оператор $\varphi^*\varphi$ неотрицателен, причем он положителен тогда и только тогда, когда φ невырожден.*

Доказательство. Во-первых проверим, что $\varphi^*\varphi$ самосопряжен. Действительно, $(\varphi^*\varphi)^* = \varphi^*\varphi^{**} = \varphi^*\varphi$. Далее, для любого $v \in V$

$$q_\varphi(v) = (v, \varphi^*\varphi(v)) = (\varphi(v), \varphi(v)) = |\varphi(v)|^2 \geq 0,$$

что по определению означает, что $\varphi^*\varphi$ неотрицателен. Заметим, что невырожденность φ равносильна условию $|\varphi(v)|^2 > 0\ \forall v \neq 0$, что в свою очередь равносильно положительности $\varphi^*\varphi$. ■

Предложение 12.47. *Самосопряженный оператор $\varphi\colon V \to V$ неотрицателен (соответственно положителен) тогда и только тогда, когда все его собственные значения неотрицательны (положительны).*

Доказательство. Для самосопряженного φ существует ортонормированный базис, в котором его матрица $A_\varphi = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Тогда матрица H соответствующей квадратичной функции q_φ равна A_φ, а сама квадратичная функция в соответствующих координатах имеет вид $q_\varphi(v) = \sum_{i=1}^n \lambda_i v_i^2$. Ясно, что она положительно (неотрицательно) определена тогда и только тогда, когда все $\lambda_i > 0$ (соответственно $\lambda_i \geq 0$). ■

Задача 12.48. *Докажите, что самосопряженный оператор φ на евклидовом пространстве положителен тогда и только тогда, когда его матрица A в некотором (а значит и любом) ортонормированном базисе положительно определена.*

Определение 12.49. Пусть φ — линейный оператор на евклидовом пространстве V. Его *полярным разложением* называется представление вида $\varphi = \psi \circ \vartheta$, где ψ — неотрицательный самосопряженный, а ϑ — ортогональный операторы на V.

Полярное разложение можно рассматривать как обобщение представления комплексного числа z в показательной форме $re^{i\alpha}$, где r, $\alpha \in \mathbb{R}$ и $r \geq 0$ (особенно эта аналогия очевидна в случае операторов в унитарных пространствах).

Заметим, что имея *левое* полярное разложение $\varphi = \psi \circ \vartheta$, можно получить *правое* полярное разложение вида $\varphi = \vartheta \circ \psi'$, где $\psi' = \vartheta^{-1}\psi\vartheta$. В самом деле, последний оператор самосопряжен, поскольку

$$(\vartheta^{-1}\psi\vartheta)^* = \vartheta^*\psi^*(\vartheta^{-1})^* = \vartheta^{-1}\psi\vartheta,$$

где мы, в частности, использовали свойство 5) операции $*$ из Предложения 12.4. Оператор ψ' также является неотрицательным, что доказывает следующая выкладка:

$$(v,\, \vartheta^{-1}\psi\vartheta(v)) = \ [\text{полагаем } v =: \vartheta^{-1}(v')] \ = (\vartheta^{-1}(v'), \vartheta^{-1}\psi\vartheta\vartheta^{-1}(v')) =$$

$$= (\vartheta^{-1}(v'),\, \vartheta^{-1}\psi(v')) = (v',\, \psi(v')) \geq 0.$$

Из курса аналитической геометрии читатель, возможно, помнит теорему о том, что для любого аффинного преобразования плоскости существуют главные направления — такая пара взаимно перпендикулярных направлений, которые при аффинном преобразовании снова переходят во взаимно перпендикулярные направления (хотя общее аффинное преобразование не сохраняет углы между произвольными векторами).

Лемма 12.50. Для любого линейного оператора $\varphi\colon V \to V$ на евклидовом пространстве V существует такой ортонормированный базис $\{e_1, \ldots, e_n\}$, который под действием φ переходит в ортогональную систему векторов $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ (то есть такую, что $(\varphi(e_i), \varphi(e_j)) = 0$ при $i \neq j$).

Доказательство. В самом деле, возьмем в качестве $\{e_1, \ldots, e_n\}$ произвольный ортонормированный базис из собственных векторов самосопряженного оператора $\varphi^*\varphi$. Если λ_i, $1 \leq i \leq n$ — соответствующие собственные значения, то $(\varphi(e_i),\, \varphi(e_j)) = (e_i,\, \varphi^*\varphi(e_j)) = \lambda_j(e_i,\, e_j) = 0$ при $i \neq j$. ∎

Направления векторов базиса $\{e_1, \ldots, e_n\}$ называются *главными направлениями* оператора φ.

Теорема 12.51. *Для любого линейного оператора φ на евклидовом пространстве V существует полярное разложение.*

Доказательство. Докажем существование левого полярного разложения. Из доказательства Леммы следует, что $|\varphi(e_i)|^2 = \lambda_i$ при $1 \leq i \leq n$. Переупорядочивая элементы базиса

$\{e_1, \ldots, e_n\}$ можно добиться того, чтобы $\lambda_i > 0$ при $1 \leq i \leq r$ и $\lambda_{r+1} = \ldots = \lambda_n = 0$ (конечно, если φ невырожден, то $r = n$). Произвольным образом дополним ортонормированную систему векторов $f_1 = \frac{\varphi(e_1)}{\sqrt{\lambda_1}}, \ldots, f_r = \frac{\varphi(e_r)}{\sqrt{\lambda_r}}$ до ортонормированного базиса $\{f_1, \ldots, f_n\}$ в V. Пусть $\vartheta\colon V \to V$ — линейный оператор, переводящий базис $\{e_1, \ldots, e_n\}$ в базис $\{f_1, \ldots, f_n\}$. Поскольку оба базиса ортонормированы, оператор ϑ является ортогональным. Теперь рассмотрим оператор $\psi\colon V \to V$, переводящий базис $\{f_1, \ldots, f_n\}$ в систему векторов $\{\sqrt{\lambda_1} f_1, \ldots, \sqrt{\lambda_r} f_r, 0, \ldots, 0\}$. Поскольку ψ имеет в ортонормированном базисе диагональную матрицу с неотрицательными элементами на диагонали, он неотрицательный самосопряженный. Посмотрим теперь на композицию $\psi \circ \vartheta$. Это — линейный оператор, действующий на векторы базиса $\{e_1, \ldots, e_n\}$ следующим образом:

$$e_i \mapsto \frac{\varphi(e_i)}{\sqrt{\lambda_i}} = f_i \mapsto \sqrt{\lambda_i} f_i = \varphi(e_i) \quad \text{при } 1 \leq i \leq r,$$

$$e_i \mapsto f_i \mapsto \sqrt{\lambda_i} f_i = 0 = \varphi(e_i) \quad \text{при } r+1 \leq i \leq n.$$

Поскольку операторы φ и $\psi \circ \vartheta$ действуют одинаково на элементы некоторого базиса, они равны. ■

Кстати, из доказательства Теоремы сразу видно, что в случае вырожденного φ ортогональный оператор ϑ определен неоднозначно. В то же время можно доказать (см. мелкий шрифт ниже), что неотрицательный самосопряженный оператор однозначно определяется по φ (но, вообще говоря, свой для левого и правого полярных разложений), а в случае невырожденного φ ортогональный ϑ тоже определен однозначно (и поэтому совпадает для обоих полярных разложений).

Неотрицательные операторы похожи на неотрицательные действительные числа, в частности, из любого такого оператора можно извлечь единственный арифметический (то есть неотрицательный) квадратный корень.

Предложение 12.52. *Для любого неотрицательного оператора $\varphi\colon V \to V$ существует единственный неотрицательный оператор $\psi\colon V \to V$ такой, что $\psi^2 = \varphi$.*

Доказательство. Пусть $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_s}$ — разложение пространства V в ортогональную прямую сумму собственных подпространств самосопряженного оператора φ. Будем считать, что $0 \leq \lambda_1 < \lambda_2 < \ldots < \lambda_s$, в этом случае указанная запись единственна. На каждом собственном подпространстве $V_{\lambda_i} \subset V$ оператор φ действует как скалярный оператор умножения на соответствующее собственное значение λ_i. Мы имеем спектральное разложение

$$\varphi = \sum_{i=1}^{s} \lambda_i P_i, \tag{111}$$

где P_i — ортогональный проектор на V_{λ_i} (см. формулу (106)). Так как все $\lambda_i \geq 0$, для каждого собственного значения λ_i существует единственный арифметический квадратный корень $\sqrt{\lambda_i}$ и оператор $\psi := \sum_{i=1}^{s} \sqrt{\lambda_i} P_i$ является неотрицательным самосопряженным, причем $\psi^2 = \varphi$, поскольку $P_i P_j = 0$ при $i \neq j$ и $P_i^2 = P_i$.

Пусть ψ' — еще один неотрицательный самосопряженный оператор такой, что $\psi'^2 = \varphi$, и пусть $\psi' = \sum_{i=1}^{r} \mu_i P'_i$ — его спектральное разложение. Можно считать, что $0 \leq \mu_1 < \ldots < \mu_r$. Тогда $\psi'^2 = \sum_{i=1}^{r} \mu_i^2 P'_i$

— еще одно спектральное разложение для φ, причем $0 \leq \mu_1^2 < \ldots < \mu_r^2$. Согласно Предложению 12.25 спектральное разложение данного оператора единственно, поэтому $\sum_{i=1}^{r} \mu_i^2 P_i'$ совпадает с (111), откуда $P_i = P_i'$ (и следовательно $V_{\mu_i} = V_{\lambda_i}$), $\mu_i = \sqrt{\lambda_i}$ и $r = s$, и значит $\psi' = \psi$. ■

Следствие 12.53. *Неотрицательный самосопряженный оператор ψ в полярном разложении $\varphi = \psi \circ \vartheta$ определен однозначно.*

Доказательство. Имеем

$$\varphi\varphi^* = \psi\vartheta\vartheta^*\psi^* = \psi^2,$$

поэтому ψ является арифметическим квадратным корнем из неотрицательного самосопряженного оператора $\varphi\varphi^*$. ■

Корень из самосопряженного оператора без условия неотрицательности не единственен. Рассмотрим, например, в качестве положительного самосопряженного φ тождественный оператор на евклидовой плоскости V. Мы знаем, что помимо $\pm\mathrm{Id}_V$ самосопряженными операторами ψ, удовлетворяющими условию $\psi^2 = \mathrm{Id}_V$, являются всевозможные ортогональные отражения относительно одномерных подпространств. То есть уравнение $X^2 = \mathrm{Id}_V$ имеет континуальное множество решений в пространстве самосопряженных операторов, но только одно из них (а именно сам тождественный оператор) является положительным. То есть неединственность корня в общем случае связана с неединственностью квадратного корня из положительного действительного числа a также с тем, что собственное подпространство размерности больше 1 с положительным собственным собственным значением λ можно расщепить в ортогональную прямую сумму собственных подпространств корня с собственными значениями $\pm\sqrt{\lambda}$.

Задача 12.54. *Пусть φ и ω — самосопряженные операторы, причем φ положительный. Докажите, что оператор $\varphi\omega$ диагонализируем.*

Решение. Пусть ψ — положительный квадратный корень из φ. Очевидно, что операторы $\varphi\omega$ и $\psi^{-1}\varphi\omega\psi$ диагонализируемы или не диагонализируемы одновременно. В то же время $\psi^{-1}\varphi\omega\psi = \psi\omega\psi$, а последний оператор, очевидно, самосопряжен. ■

В случае невырожденного оператора φ ортогональный оператор ϑ в его полярном разложении также определен однозначно. Докажем это, например, для правого полярного разложения.

Предложение 12.55. *Для любого невырожденного оператора $\varphi\colon V \to V$ на евклидовом пространстве V существуют и единственны такие положительный ψ и ортогональный ϑ операторы на V, что $\varphi = \vartheta \circ \psi$.*

Доказательство. Из Предложения 12.46 мы знаем, что для невырожденного оператора φ оператор $\varphi^*\varphi$ положительный самосопряженный. Пусть ψ — положительный корень из $\varphi^*\varphi$, который согласно Предложению 12.52 существует и единственен.

Проверим, что оператор $\varphi\psi^{-1}$ ортогонален. Действительно,

$$(\varphi\psi^{-1})^*\varphi\psi^{-1} = (\psi^*)^{-1}\varphi^*\varphi\psi^{-1} = \psi^{-1}\psi^2\psi^{-1} = \mathrm{Id}_V.$$

Поэтому мы полагаем $\vartheta := \varphi\psi^{-1}$ и получаем требуемое разложение $\varphi = \vartheta\psi$.

Проверим единственность. Если $\varphi = \vartheta\psi$, то $\varphi^*\varphi = \psi\vartheta^*\vartheta\psi = \psi^2$, откуда однозначно восстанавливается положительный самосопряженный ψ. А тогда ортогональный ϑ однозначно задается равенством $\vartheta = \varphi\psi^{-1}$. ■

Следствие 12.56. *Любую невырожденную вещественную матрицу A можно единственным образом представить в виде произведения UB, где B — положительно определенная симметричная, а U — ортогональная матрицы.*

Приведем алгоритм нахождения матриц B и U, входящих в правое полярное разложение $A = UB$ данной невырожденной вещественной матрицы A. Матрицу A можно рассматривать как матрицу невырожденного оператора φ в некотором ортонормированном базисе.

Если уже получено требуемое разложение $A = UB$, то $A^TA = B^TU^TUB = B^2$. Заметим, что матрица A^TA симметричная положительная (это матрица положительного самосопряженного оператора $\varphi^*\varphi$ в ортонормированном базисе), поэтому существует такая ортогональная матрица C, что $\Lambda = C^TA^TAC$ — диагональная матрица $\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, причем все $\lambda_i > 0$ (как собственные значения положительного самосопряженного оператора $\varphi^*\varphi$). Поэтому $A^TA = C\Lambda C^T$ и оператор с матрицей $B = C\sqrt{\Lambda}C^T$, где $\sqrt{\Lambda} := \operatorname{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$, является положительным самосопряженным (поскольку данная матрица симметрична и все ее собственные значения положительны). Кроме того, $B^2 = A^TA$, поскольку $B^2 = C\sqrt{\Lambda}C^TC\sqrt{\Lambda}C^T = C\Lambda C^T = A^TA$. Значит, оператор с матрицей B является искомым арифметическим квадратным корнем из A^TA. Теперь ортогональная матрица U однозначно находится из соотношения $U = AB^{-1}$.

Заметим, что для левого полярного разложения $A = B'U'$ симметричная матрица B' ищется как арифметический квадратный корень из AA^T.

Посмотрим, какую геометрическую картину дает полярное разложение $\varphi = \vartheta\psi$ для невырожденного линейного оператора φ на евклидовом пространстве. Пусть $\{e_1, \ldots, e_n\}$ — ортонормированный базис из собственных векторов положительного самосопряженного оператора ψ, и $\mu_i = \sqrt{\lambda_i}$ — соответствующие собственные значения. Пусть $S(V) = \{v \in V \mid |v| = 1\}$ — единичная сфера пространства V. Тогда в координатах относительно базиса $\{e_1, \ldots, e_n\}$ она задается уравнением $\sum_{i=1}^n v_i^2 = 1$. Посмотрим, куда она переходит под действием ψ. Для $v = \sum_{i=1}^n v_ie_i \in S(V)$ получаем $w := \psi(v) = \sum_{i=1}^n \mu_iv_ie_i = \sum_{i=1}^n w_ie_i$, откуда $v_i = \frac{w_i}{\mu_i}$, поэтому $1 = \sum_{i=1}^n v_i^2 = \sum_{i=1}^n \frac{w_i^2}{\mu_i^2}$ — уравнение n-мерного эллипсоида с полуосями μ_i. То есть ψ единичную сферу отображает в указанный эллипсоид. Дальнейшее применение ϑ к указанному эллипсоиду как-то его поворачивает и (возможно) отражает, но не меняет его геометрию (длины полуосей).

Вернемся снова к матричной форме полярного разложения $A = UB$. Через D обозначим введенную выше матрицу $\sqrt{\Lambda}$, тогда $B = CDC^T$, где C — ортогональная матрица. Подставляя это выражение в полярное разложение получим, что для невырожденной вещественной матрицы A существуют такие ортогональные матрицы U_1, U_2, что $A = U_1DU_2$ где D — диагональная матрица, на диагонали которой стоят арифметические квадратные корни из собственных значений матрицы A^TA. Это так называемое *сингулярное разложение* матрицы A.

Задача 12.57. *Выясните, насколько однозначно сингулярное разложение? (Ответ: матрица D определена однозначно с точностью до перестановки диагональных элементов. При заданной матрице D матрицы U_1 и U_2 определены с точностью до преобра-*

зования $U_1 \mapsto U_1U$, $U_2 \mapsto U^{-1}U_2$, где U — ортогональная матрица, коммутирующая с D).

12.9 Инвариантные подпространства малых размерностей над $\mathbb{R}$

В данном разделе мы докажем важное утверждение о том, что у любого линейного оператора на векторном пространстве конечной положительной размерности над полем $\mathbb{R}$ существует одномерное или двумерное инвариантное подпространство. Затем, используя этот результат, мы дадим еще одно доказательство существования собственного вектора у самосопряженного оператора, а также доказательство существования канонического вида ортогонального оператора.

Мы знаем, что любой оператор на пространстве положительной размерности над полем $\mathbb{C}$ имеет собственный вектор. Это выводится из алгебраической замкнутости $\mathbb{C}$: любой многочлен $f(t) \in \mathbb{C}[t]$ положительной степени n имеет корень в $\mathbb{C}$ (а значит раскладывается на линейные множители $f(t) = a_0(t - \lambda_1) \dots (t - \lambda_n)$).

Для многочленов с вещественными коэффициентами нам известно, что всякий такой многочлен нечетной степени имеет вещественный корень, что приводит к существованию собственного вектора у любого оператора на вещественном пространстве нечетной размерности. Однако многочлен четной степени над $\mathbb{R}$ может не иметь вещественных корней, и у оператора на четномерном вещественном пространстве не обязательно есть собственный вектор. Во всяком случае мы знаем, что вещественный многочлен положительной степени раскладывается на линейные и квадратичные вещественные множители. Это связано с тем, что неприводимые многочлены над $\mathbb{R}$ — не только многочлены первой степени, но также второй степени с отрицательным дискриминантом.

Пусть $f(t) \in \mathbb{R}[t]$ — многочлен второй степени с отрицательным дискриминантом, пусть его старший коэффициент равен 1. Тогда над полем $\mathbb{C}$ он раскладывается на линейные множители: $f(t) = (t - \lambda)(t - \overline{\lambda}) = t^2 - (\lambda + \overline{\lambda})t + |\lambda|^2$. Здесь мы использовали тот факт, что если многочлен $f(t) \in \mathbb{R}[t]$ имеет корень $\lambda \in \mathbb{C}\backslash\mathbb{R}$, то также его корнем будет и $\overline{\lambda}$ (это легко выводится из свойств комплексного сопряжения).

Когда мы изучали инвариантные подпространства линейных операторов, мы доказали такой результат: характеристический многочлен ограничения оператора на инвариантное подпространство делит характеристический многочлен самого оператора. Нельзя ли это утверждение обратить в том смысле, что делителю характеристического многочлена отвечает инвариантное подпространство? Если бы это можно было сделать, то, поскольку вещественный многочлен положительной степени, не имеющий вещественных корней, обязан делиться над $\mathbb{R}$ на многочлен второй степени, то мы бы доказали существование двумерного инвариантного подпространства. По-существу, мы именно это сейчас и сделаем.

Итак, пусть $\varphi\colon V \to V$ — линейный оператор, где V — векторное пространство над

полем $\mathbb{R}$, причем $\dim V \geq 2$. Пусть $\chi_\varphi(t) \in \mathbb{R}[t]$ — характеристический многочлен оператора φ и $\lambda \in \mathbb{C}\backslash\mathbb{R}$ — его невещественный корень, $\chi_\varphi(\lambda) = 0$. Тогда $f(t) = (t-\lambda)(t-\overline{\lambda}) = t^2 + pt + q \in \mathbb{R}[t]$ делит $\chi_\varphi(t)$ в кольце $\mathbb{R}[t]$ (то есть $\chi_\varphi(t) = f(t)g(t)$, где $g(t) \in \mathbb{R}[t]$).

Напомним, что для любого многочлена $p(t) \in \mathbb{R}[t]$ и оператора φ как выше мы имеем линейный оператор $p(\varphi)\colon V \to V$.

Докажем теперь серию небольших лемм.

Лемма 12.58. Пусть $U := \operatorname{Ker} f(\varphi) \subset V$. Тогда U является φ-инвариантным.

Доказательство. Если два оператора $\varphi, \psi\colon V \to V$ коммутируют, то ядро одного из них инваринатно относительно другого. Легко проверяется, что для любого многочлена p операторы φ и $p(\varphi)$ коммутируют. ■

Лемма 12.59. Определенное в предыдущей лемме подпространство U ненулевое.

Доказательство. Пусть $A \in \operatorname{Mat}_n(\mathbb{R})$ — матрица оператора φ в некотором базисе пространства V. Тогда матрицей оператора $f(\varphi)$ в том же базисе будет $f(A)$. Заметим, что $f(A)$ является произведением двух комплексных матриц $A - \lambda E$ и $A - \overline{\lambda}E$. В самом деле,

$$(A - \lambda E)(A - \overline{\lambda}E) = A^2 - (\lambda + \overline{\lambda})A + \lambda\overline{\lambda}E = f(A).$$

Поэтому $\det f(A) = (\det(A - \lambda E))(\det(A - \overline{\lambda}E))$. Но так как λ — (комплексный) корень $\chi_\varphi(t)$, то матрица $(A - \lambda E)$ вырождена (то же, конечно, верно и для $(A - \overline{\lambda}E)$). Значит, и матрица $f(A)$ тоже вырождена, поэтому у оператора $f(\varphi)$ ядро U ненулевое. ■

Лемма 12.60. Подпространство U не содержит собственных векторов оператора φ.

Доказательство. Пусть, напротив, $u \in U$ — собственный вектор φ. Тогда $u \neq 0$ и $\varphi(u) = \mu u$ для некоторого $\mu \in \mathbb{R}$. Тогда

$$0 = f(\varphi)(u) = (\varphi^2 + p\varphi + q\mathrm{Id}_V)u = (\mu^2 + p\mu + q)u$$

и μ — вещественный корень многочлена $f(t)$ в противоречии с нашим выбором многочлена f. ■

Лемма 12.61. Пусть $0 \neq u \in U$. Тогда $W := \langle u, \varphi(u)\rangle \subseteq U$ — двумерное φ-инвариантное подпространство.

Доказательство. Заметим, что W содержится в U, так как $\varphi(u) \in U$ в силу φ-инвариантности U (см. лемму 12.58). Если $\varphi(u)$ пропорционально (с вещественным коэффициентом) u, то u — собственный вектор φ, чего в силу предыдущей леммы быть не может. Поэтому $\dim W = 2$. Осталось показать, что само W φ-инвариантно. Для этого, очевидно, достаточно показать, что его базис $\{u, \varphi(u)\}$ при применении φ остается в W.

Для u это очевидно, для $\varphi(u)$ это следует из равенства $\varphi^2(u) = -p\varphi(u) - qu$, которое выполнено для любого $u \in U$ в силу определения U. ■

Заметим, что матрицей $\varphi|_W$ в базисе $\{u, \varphi(u)\}$ пространства W будет $B = \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$. Интересно заметить, что $\chi_B(t) = f(t)$. Как это связано с теоремой Гамильтона-Кэли?

Соберем вместе доказанные в леммах результаты.

Предложение 12.62. *Пусть V — конечномерное линейное пространство над полем $\mathbb{R}$, $\varphi\colon V \to V$ — линейный оператор, λ — комплексный (невещественный) корень $\chi_\varphi(t)$. Пусть $f(t) = (t-\lambda)(t-\overline{\lambda}) \in \mathbb{R}[t]$ и $U = \operatorname{Ker} f(\varphi)$. Тогда U — ненулевое φ-инвариантное подпространство в V, и произвольный ненулевой вектор $u \in U$ содержится в единственном двумерном φ-инвариантном подпространстве $W \subseteq U$.*

Следствие 12.63. *Пусть V — конечномерное линейное пространство положительной размерности над полем $\mathbb{R}$, $\varphi\colon V \to V$ — линейный оператор. Тогда в V существует одно- или двумерное φ-инвариантное подпространство.*

Заметим, что над полем $\mathbb{Q}$ оператор, действующий в пространстве сколь угодно большой размерности, может не иметь нетривиальных инвариантных подпространств (см. Задачу 8.66).

Дадим теперь новое доказательство Предложения 12.16, утверждающего существование собственного вектора самосопряженного преобразования.

Итак, пусть $\varphi\colon V \to V$ — самосопряженное преобразование евклидова пространства V, $\dim V \geq 1$. Если у φ есть одномерное инвариантное подпространство, то его порождает собственный вектор. Если одномерного инвариантного подпространства нет, то обязательно найдется двумерное φ-инвариантное подпространство $U \subset V$. Ограничение $\psi := \varphi|_U$ является самосопряженным преобразованием двумерного евклидова пространства U. Пусть $\{e_1, e_2\}$ — ортонормированный базис в U и $B = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ — матрица ψ в нем. Легко посчитать, что дискриминант характеристического многочлена $\chi_B(t)$ равен $(a-c)^2 + 4b^2$, поэтому он всегда неотрицателен, и значит корни $\chi_B(t)$ вещественные, поэтому ψ имеет собственный вектор, а значит и φ имеет собственный вектор, лежащий в подпространстве U. Это противоречит предположению о том, что у φ нет одномерного инвариантного подпространства и завершает доказательство. ■

Выведем теперь из Следствия 12.63 существование канонического вида ортогонального оператора.

Предложение 12.64. *Пусть $\varphi\colon V \to V$ — ортогональное преобразование конечномерного евклидова пространства V. Тогда в V существует ортонормированный базис, в котором матрица имеет блочно-диагональный вид с диагональными блоками порядков 1 и 2. Блоки порядка 1 равны ± 1, блоки порядка 2 являются матрицами поворота на углы $\alpha \neq \pi k$ (вообще говоря, углы разные для разных блоков).*

Доказательство. Требуемый базис можно строить так. Напомним, что собственными значениями ортогонального оператора могут быть только ± 1. Если у φ есть собственные подпространства V_1 и V_{-1}, то легко проверяется, что они ортогональны. Выберем ортонормированный базис в каждом из них и объединим их, так мы получим часть искомого базиса, которая отвечает диагональным блокам порядка 1. Если $V_1 \oplus V_{-1} \neq V$, заметим, что так как $V_1 \oplus V_{-1}$ φ-инвариантно, то в силу Предложения 12.38 и $(V_1 \oplus V_{-1})^\perp$ φ-инвариантно. Подпространство $(V_1 \oplus V_{-1})^\perp$ уже не содержит собственных векторов φ, но согласно Следствию 12.63, в нем найдется 2-мерное φ-инвариантное подпространство U. Ограничение $\varphi|_U$ будет ортогональным преобразованием плоскости, не имеющим собственных векторов, и значит поворотом на угол $\alpha \neq \pi k$, и его матрицей в соответствующем ортонормированном базисе будет $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$. Далее переходим к $(V_1 \oplus V_{-1} \oplus U)^\perp$ и т.д., так как V по условию конечномерно, так мы придем к искомому базису за конечное число шагов. ■

Следствие 12.65. *Комплексное число является корнем характеристического многочлена некоторого ортогонального преобразования тогда и только тогда, когда оно по модулю равно единице.*

Доказательство. Легко следует из предыдущего Предложения с учетом того, что характеристические числа матрицы поворота плоскости на угол α равны $e^{i\alpha}$ и $e^{-i\alpha}$. ■

Задача 12.66. *Выясните, может ли какая-нибудь из приведенных ниже матриц являться матрицей ортогонального оператора в евклидовом пространстве в некотором, не обязательно ортонормированном, базисе, если*

$$A = \begin{pmatrix} 1/2 & -1/2 \\ 1/2 & 3/2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 3/2 & 1/2 \end{pmatrix}.$$

Решение. Заметим, что у всех трех матриц определитель равен 1, поэтому нужны более тонкие необходимые условия того, что матрица может быть матрицей ортогонального оператора.

$\chi_A(t) = t^2 - 2t + 1 = (t-1)^2$, поэтому данная матрица не диагонализируема (даже над $\mathbb{C}$), а значит не может быть матрицей ортогонального оператора ни в каком базисе.

$\chi_C(t) = t^2 - 3/2t - 1 = (t-2)(t+1/2)$; в этом случае собственные значения отличны от ± 1, а значит оператор с такой матрицей не может быть ортогональным.

$\chi_B(t) = t^2 + t + 1$; в данном случае собственные значения равны $e^{\frac{2\pi i}{3}}$ и $e^{-\frac{2\pi i}{3}}$ и можно предположить, что оператор в подходящем ортонормированном базисе имеет матрицу $\begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$. В любом случае эта матрица сопряжена с матрицей B над полем $\mathbb{C}$, поскольку обе они приводятся к диагональной форме $\operatorname{diag}(e^{\frac{2\pi i}{3}}, e^{-\frac{2\pi i}{3}})$. То есть для того, чтобы доказать, что матрица B в самом деле является матрицей ортогонального оператора в некотором базисе, достаточно доказать следующую Лемму.

Лемма 12.67. Если две вещественные матрицы подобны над полем $\mathbb{C}$, то они подобны и над $\mathbb{R}$.

Доказательство. Две матрицы $A, B \in \operatorname{Mat}_n(\mathbb{R})$ подобны над полем $\mathbb{R}$, если система линейных однородных уравнений $XA = BX$ имеет решение, являющееся невырожденной матрицей из $\operatorname{Mat}_n(\mathbb{R})$. Пусть $\{C_1, \ldots, C_m\}$ — фундаментальная система решений указанной системы ($C_1, \ldots, C_m \in \operatorname{Mat}_n(\mathbb{R})$). Если матрицы A и B не подобны над $\mathbb{R}$, то $\det(\lambda_1 C_1 + \ldots + \lambda_m C_m) = 0$ при любых $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ и следовательно $\det(t_1 C_1 + \ldots + t_m C_m)$ — нулевой многочлен от $t_1, \ldots, t_m$. Но тогда $\det(\lambda_1 C_1 + \ldots + \lambda_m C_m) = 0$ и при любых $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$, а значит A и B не подобны и над полем $\mathbb{C}$. ■

Задача 12.68. *Оператор φ на евклидовом пространстве V называется кососимметрическим, если $\varphi^* = -\varphi$.*

a) Докажите, что если подпространство $U \subset V$ φ-инвариантно, то и $U^\perp$ φ-инвариантно.

b) Найдите канонический вид матрицы кососимметрического оператора (в некотором ортонормированном базисе).

c) Что можно сказать про корни (в $\mathbb{C}$) характеристического многочлена кососимметрического оператора?

Задача 12.69. [59] *Пусть $\varphi\colon V \to V$ — линейный оператор на евклидовом пространстве V такой, что $\varphi(v) \perp v\ \forall v \in V$. Докажите, что $\operatorname{rk}\varphi$ — четное число.*

13 Унитарные (эрмитовы) пространства

Вещественными векторными пространствами с наиболее богатой геометрией являются евклидовы пространства. В них, в частности, можно измерять длины векторов и углы между векторами. Все это возможно благодаря наличию билинейной симметричной положительно определенной формы — евклидовой структуры.

Если рассмотреть комплексное векторное пространство с билинейной симметричной формой на нем, то сразу выясняется, что понятие положительной определенности для нее теряет смысл — любое комплексное число является квадратом комплексного числа. Получить положительное действительное число из ненулевого комплексного числа z можно, взяв вместо квадрата z^2 произведение $z\overline{z}$ на комплексно сопряженное. Возникает мысль рассмотреть аналог билинейных форм, для которых квадратичной формой является сумма квадратов модулей координат (в некотором базисе). Простейшие такие формы в координатах имеют вид

$$x_1\overline{y}_1 + x_2\overline{y}_2 + \ldots + x_n\overline{y}_n.$$

Так мы приходим к понятию полуторалинейной формы.

Такие полуторалинейные формы приводят к комплексным аналогам евклидовых пространств со столь же богатой геометрией, называемым *унитарными* пространствами. Унитарное пространство — это пара, состоящая из (конечномерного, если не оговорено противное) векторного пространства над $\mathbb{C}$ и полуторалинейной эрмитово симметричной положительно определенной формы на нем, которая определяет соответствующее скалярное произведение. Практически все понятия, имеющие смысл для евклидова пространства, имеют его и для унитарного (длина вектора, угол между векторами, ортонормированный базис, ортогональное дополнение к подпространству, самосопряженные преобразования и т.д.). Причем для них верны аналоги теорем для евклидова пространства (неравенства Коши-Буняковского и треугольника, теоремы об ортогональном дополнении, ортогонализация Грама-Шмидта, свойства самосопряженных преобразований и т.п.).

Для удобства читателя мы приведем таблицу, связывающую аналогичные понятия в вещественном (евклидовом) и комплексном (унитарном) случаях.

[59] Сообщена автору И.И. Богдановым.

в вещественном случае	в комплексном случае
билинейная форма	полуторалинейная форма
симметричная билинейная форма	эрмитово симметричная полуторалинейная форма
квадратичная форма	эрмитова квадратичная форма
евклидово пространство	унитарное (=эрмитово) пространство
сопряженное преобразование	эрмитово сопряженное преобразование
самосопряженное (=симметричное) преобразование	эрмитово (симметричное) преобразование
ортогональное преобразование	унитарное преобразование

13.1 Полуторалинейные формы

Пусть V — векторное пространство над полем $\mathbb{C}$.

Определение 13.1. Функция $f\colon V \to \mathbb{C}$ называется *полулинейной формой* (или полулинейной функцией) на V, если выполнены следующие два условия:

- $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) \quad \forall \mathbf{u},\, \mathbf{v} \in V$;
- $f(\lambda \mathbf{v}) = \overline{\lambda} f(\mathbf{v}) \quad \forall \mathbf{v} \in V,\ \lambda \in \mathbb{C}$, где черта в $\overline{\lambda}$ обозначает комплексное сопряжение.

Определение 13.2. Функция $\alpha\colon V \times V \to \mathbb{C}$ называется *полуторалинейной формой* на V, если она линейна по второму аргументу и полулинейна по первому.

Другими словами, полуторалинейная форма α удовлетворяет условиям:

- $\alpha(\lambda \mathbf{u}_1 + \mu \mathbf{u}_2,\, \mathbf{v}) = \overline{\lambda}\alpha(\mathbf{u}_1,\, \mathbf{v}) + \overline{\mu}\alpha(\mathbf{u}_2,\, \mathbf{v}) \quad \forall \mathbf{u}_1,\, \mathbf{u}_2,\, \mathbf{v} \in V,\ \lambda,\, \mu \in \mathbb{C}$;
- $\alpha(\mathbf{u},\, \lambda \mathbf{v}_1 + \mu \mathbf{v}_2) = \lambda\alpha(\mathbf{u},\, \mathbf{v}_1) + \mu\alpha(\mathbf{u},\, \mathbf{v}_2) \quad \forall \mathbf{u},\, \mathbf{v}_1,\, \mathbf{v}_2 \in V,\ \lambda,\, \mu \in \mathbb{C}$.

Замечание 13.3. В некоторых книгах полуторалинейными формами называют функции, которые наоборот, линейны по первому аргументу и полулинейны по второму.

При перестановке аргументов полуторалинейной формы ее полулинейный и линейный аргументы меняются местами. Поэтому "наивный" способ определить понятие симметричной билинейной формы не проходит. Заметим, что операция комплексного сопряжения также меняет местами линейный и полулинейный аргументы.

Определение 13.4. Полуторалинейная форма $\alpha\colon V \times V \to \mathbb{C}$ называется *эрмитово симметричной* (кратко, *эрмитовой*), если для любых векторов $\mathbf{u},\, \mathbf{v} \in V$ выполнено тождество

$$\alpha(\mathbf{u},\, \mathbf{v}) = \overline{\alpha(\mathbf{v},\, \mathbf{u})}. \tag{112}$$

Определение 13.5. *Эрмитово квадратичной формой* называется функция $q\colon V \to \mathbb{C}$, для которой существует эрмитова форма α такая, что $q(\mathbf{v}) := \alpha(\mathbf{v},\, \mathbf{v}) \ \ \forall\, \mathbf{v} \in V$.

Заметим, что из предыдущего определения мгновенно следует, что *эрмитово квадратичная форма принимает вещественные значения*, то есть фактически является функцией $q\colon V \to \mathbb{R}$.

Заметим, что соотношения

$$\begin{cases} q(\mathbf{u}+\mathbf{v}) = q(\mathbf{u}) + \alpha(\mathbf{u},\, \mathbf{v}) + \alpha(\mathbf{v},\, \mathbf{u}) + q(\mathbf{v}) \\ q(\mathbf{u}+i\mathbf{v}) = q(\mathbf{u}) + i\alpha(\mathbf{u},\, \mathbf{v}) - i\alpha(\mathbf{v},\, \mathbf{u}) + q(\mathbf{v}) \end{cases} \tag{113}$$

позволяют восстановить α по q. А именно,

$$\alpha(\mathbf{u},\,\mathbf{v}) = \operatorname{Re}(\alpha(\mathbf{u},\,\mathbf{v})) + i\operatorname{Im}(\alpha(\mathbf{u},\,\mathbf{v})) =$$

$$= \frac{1}{2}\left(q(\mathbf{u}+\mathbf{v}) - q(\mathbf{u}) - q(\mathbf{v})\right) + \frac{1}{2}\left(q(\mathbf{u}+i\mathbf{v}) - q(\mathbf{u}) - q(\mathbf{v})\right).$$

Тем самым устанавливается биекция между эрмитовыми формами и эрмитово квадратичными формами. В частности, если $q \equiv 0$, то и $\alpha \equiv 0$.

Рассмотрим пару примеров.

Пример 13.6. Пусть $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ — некоторый базис в V, $\mathbf{v} = \sum v_i\mathbf{e}_i$ — разложение произвольного вектора по нему. Пусть $k,\ l \in \mathbb{N},\ k+l \leq n$. Тогда

$$\alpha(\mathbf{u},\,\mathbf{v}) = \sum_{i=1}^{k} \overline{u}_i v_i - \sum_{j=1}^{l} \overline{u}_i v_i, \quad q_\alpha(\mathbf{v}) = \sum_{i=1}^{k} |v_i|^2 - \sum_{j=1}^{l} |v_i|^2$$

— эрмитова и соответствующая ей эрмитова квадратичная формы. Как и для вещественной симметричной формы, для эрмитовой всегда существует базис, в котором она имеет такой вид (называемый *нормальным*).

Пример 13.7. Приведем пример эрмитовой формы на бесконечномерном пространстве. Пусть

$$V := \{f\colon [0,\,1] \to \mathbb{C} \mid f \ \text{ непрерывна}\}$$

— пространство непрерывных комплекснозначных функций на отрезке. Определим функцию $\alpha\colon V \times V \to \mathbb{C}$ формулой

$$\alpha(f,\,g) := \int_0^1 \overline{f(t)}g(t)\,dt \quad \forall f,\,g \in V.$$

Тогда легко проверить, что α — эрмитова форма на V.

Пусть $\alpha\colon V \times V \to \mathbb{C}$ — полуторалинейная форма на V, а $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ — некоторый базис в V. Тогда из определений легко следует, что

$$\alpha(\mathbf{u},\,\mathbf{v}) = \sum_{i=1}^{n} \alpha(\mathbf{e}_i,\,\mathbf{e}_j)\overline{u}_i v_j. \tag{114}$$

Если через v обозначить координатный столбец вектора $\mathbf{v} \in V$ в выбранном базисе, то равенство (114) можно переписать в виде

$$\alpha(\mathbf{u},\,\mathbf{v}) = \overline{u}^T G v,$$

где $G = G_\alpha := (\alpha(\mathbf{e}_i,\,\mathbf{e}_j)) \in \operatorname{Mat}_n(\mathbb{C})$ — матрица, у которой на (i,j)-м месте стоит число $\alpha(\mathbf{e}_i,\,\mathbf{e}_j) \in \mathbb{C}$ — называемая *матрицей полуторалинейной формы* (в выбранном базисе).

Если $\{\mathbf{e}'_1, \ldots, \mathbf{e}'_n\}$ — еще один базис в V, причем $C \in \mathrm{GL}_n(\mathbb{C})$ — матрица перехода к нему от первого базиса, то

$$G' = \overline{C}^T G C \tag{115}$$

— матрица полуторалинейной формы α в новом базисе.

Условие эрмитовой симметрии (112) переписывается при этом в виде

$$\alpha(e_i,\,e_j) = \overline{\alpha(e_j,\,e_i)},$$

то есть $G = \overline{G}^T$. Матрицы $G \in \operatorname{Mat}_n(\mathbb{C})$, удовлетворяющие последнему тождеству, называются *эрмитовыми*. Таким образом, *матрица эрмитовой формы в произвольном базисе эрмитова.*

Задача 13.8. *Докажите, что если матрица G эрмитова, то* $\det G \in \mathbb{R}$.

Здесь можно было бы развить общую теорию эрмитовых форм, которая, по-существу, параллельна теории вещественных симметричных форм; в частности, для них верен аналог теоремы инерции. Мы, однако, делать этого не будем, и ограничимся случаем положительно определенных эрмитовых форм.

Определение 13.9. Эрмитова форма $\alpha\colon V \times V \to \mathbb{C}$ называется *положительно определенной*, если $q_\alpha(\mathbf{v}) = \alpha(\mathbf{v}, \mathbf{v}) > 0 \ \ \forall \mathbf{v} \in V,\ \mathbf{v} \neq \mathbf{0}$.

Например, эрмитовы формы из примеров 13.6 при $k = n$ и 13.7 положительно определены.

Заметим, что из формулы (115) следует, что знак определителя матрицы эрмитовой формы не зависит от базиса. Далее мы докажем (см. Теорему 13.14), что для положительно определенной эрмитовой формы существует ортонормированный базис, в котором ее матрица равна E, поэтому определитель матрицы такой формы положителен. Имеет место аналог критерия Сильвестра: эрмитова форма положительно определена $\Leftrightarrow$ все главные миноры ее матрицы положительны.

Например, общая эрмитова матрица порядка 2 имеет вид

$$\begin{pmatrix} a & b+ci \\ b-ci & d \end{pmatrix}$$

(a, b, c, $d \in \mathbb{R}$), ее определитель равен $ad - (b^2 + c^2)$, она положительно определена тогда и только тогда когда $a > 0$ и $ad - (b^2 + c^2) > 0$. Очевидно, что вещественная часть эрмитовой матрицы симметрична, а мнимая — кососимметрична.

Замечание 13.10. Вообще, эрмитовы матрицы порядка n образуют *вещественное* векторное пространство размерности n^2. С другой стороны, их можно рассматривать как комплексный аналог симметричных матриц. Для вещественных матриц мы имеем разложение $\mathrm{Mat}_n(\mathbb{R}) = \mathrm{Mat}_n(\mathbb{R})^+ \oplus \mathrm{Mat}_n(\mathbb{R})^-$ пространства квадратных матриц в прямую сумму подпространств симметричных и кососимметричных матриц. Посмотрим, есть ли аналогичная конструкция в комплексном случае.

Для этого рассмотрим полулинейный оператор $\sigma\colon \mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C}),\quad \sigma(A) = \overline{A}^T$. Полулинейность σ означает, что $\sigma(A + B) = \sigma(A) + \sigma(B),\ \sigma(\lambda A) = \overline{\lambda}\sigma(A) \ \ \forall A, B \in \mathrm{Mat}_n(\mathbb{C}),\ \lambda \in \mathbb{C}$. Кроме того, $\sigma^2 = \mathrm{Id}_{\mathrm{Mat}_n(\mathbb{C})}$. Такие полулинейные операторы на комплексном векторном пространстве называются *полулинейными инволюциями*.

Положим

$$V^+ := \{A \in \mathrm{Mat}_n(\mathbb{C}) \mid \sigma(A) = A\},\quad V^- := \{A \in \mathrm{Mat}_n(\mathbb{C}) \mid \sigma(A) = -A\}.$$

Заметим, что V^+ и V^- — вещественные линейные подпространства в $\mathrm{Mat}_n(\mathbb{C})$ такие, что $V^+ \cap V^- = 0$. Более того, для любой матрицы $A \in \mathrm{Mat}_n(\mathbb{C})$ имеет место представление $A = A^+ + A^-$, где $A^+ \in V^+,\ A^- \in V^-$. Точнее,

$$A^+ = \frac{1}{2}(A + \sigma(A)),\ \ A^- = \frac{1}{2}(A - \sigma(A)).$$

Таким образом, $\mathrm{Mat}_n(\mathbb{C}) = V^+ \oplus V^-$ — разложение в прямую сумму вещественных линейных пространств.

Кроме того, $\iota\colon V^+ \to V^-,\ \ \iota(A) := iA$ — изоморфизм векторных пространств, значит, вещественная размерность пространств V^+ и V^- равна комплексной размерности пространства $\mathrm{Mat}_n(\mathbb{C})$, то есть n^2. Кроме того, $V^- = iV^+$. Значит,

$$\mathrm{Mat}_n(\mathbb{C}) = V^+ \oplus iV^+. \tag{116}$$

Легко видеть, что V^+ состоит из эрмитовых матриц. Матрицы из V^- называются *косоэрмитовыми*.

Заметим, что помимо разложения (116) есть также разложение $\mathrm{Mat}_n(\mathbb{C}) = \mathrm{Mat}_n(\mathbb{R}) \oplus i\mathrm{Mat}_n(\mathbb{R})$. К нему можно прийти, рассматривая вместо σ другую полулинейную инволюцию $\tau\colon \mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C}),\ \ \tau(A) = \overline{A}$. По довольно прозрачным причинам полулинейные инволюции на комплексном пространстве называют

вещественными структурами. Соответствующее вещественное подпространство состоит из неподвижных относительно инволюции элементов (ср. характеризацию вещественных чисел в $\mathbb{C}$ как таких, которые остаются на месте при комплексном сопряжении). Таким образом, мы определили две вещественные структуры на $\mathrm{Mat}_n(\mathbb{C})$: стандартную,[60] для которой роль вещественного подпространства играет $\mathrm{Mat}_n(\mathbb{R})$ и нестандартную, для которой вещественное подпространство образовано эрмитовыми матрицами V^+. Детали см. в [14].

Кстати, заметим, что $V^+ \cap \mathrm{Mat}_n(\mathbb{R})$ (соотв. $V^- \cap \mathrm{Mat}_n(\mathbb{R})$) — подпространство симметрических (соотв. кососимметрических) матриц в $\mathrm{Mat}_n(\mathbb{R})$.

13.2 Унитарные пространства

Как уже говорилось выше, комплексными аналогами евклидовых пространств являются унитарные пространства.

Определение 13.11. *Унитарным пространством* называется пара (V, α), состоящая из векторного пространства V над $\mathbb{C}$ и положительно определенной эрмитовой формы α на нем.

Из положительной определенности α (как и в вещественном симметричном случае) сразу следует ее невырожденность. Заметим, что для любого (комплексного) подпространства $U \subset V$ пара $(U, \alpha|_U)$ — унитарное пространство, где $\alpha|_U$ — ограничение эрмитовой формы α на подпространство $U \subset V$, которое также положительно определено и, значит, невырождено.

Пусть $U \subset V$ — произвольное подпространство унитарного пространства (V, α). Его *ортогональным дополнением* называется подпространство $U^\perp \subset V$, определяемое следующим образом:

$$U^\perp := \{\mathbf{v} \in V \mid \alpha(\mathbf{u}, \mathbf{v}) = 0 \ \forall \mathbf{u} \in U\}.$$

Заметим, что, несмотря на то, что эрмитова форма α по определению полулинейна по первому аргументу и линейна по второму, определение ортогонального дополнения симметрично по аргументам.

Следующие теоремы являются аналогами соответствующих теорем для евклидова пространства. Доказательства их также аналогичны.

Предложение 13.12. *Пусть U — подпространство унитарного пространства (V, α). Тогда $\dim U^\perp = \dim V - \dim U$, $(U^\perp)^\perp = U$.*

Доказательство. Как и в Предложении 10.26 здесь все следует из невырожденности α. Пусть $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ — базис в U. Тогда $U^\perp$ задается системой k линейных однородных уравнений

$$\begin{cases} \alpha(\mathbf{e}_1, \mathbf{v}) = 0 \\ \ldots\ldots\ldots\ldots \\ \alpha(\mathbf{e}_k, \mathbf{v}) = 0 \end{cases} \tag{117}$$

(относительно координат неизвестного вектора $\mathbf{v}$). Уравнения системы (117) линейно независимы, так как из

$$\sum_{i=1}^{k} \overline{\lambda}_i \alpha(\mathbf{e}_i, \mathbf{v}) = 0$$

[60] подчеркнем, что в произвольном комплексном линейном пространстве нет выделенной вещественной структуры.

для некоторого набора $\lambda_i \in \mathbb{C}$ и $\forall \mathbf{v} \in V$ следует, что

$$\alpha\left(\sum_{i=1}^{k} \lambda_i \mathbf{e}_i,\, \mathbf{v}\right) = 0,$$

откуда, в силу положительной определенности формы α имеем $\sum_{i=1}^{k} \lambda_i \mathbf{e}_i = \mathbf{0}$, а значит все $\lambda_i = 0$.

Поэтому ранг системы (117) равен k, и если $n := \dim V$, то размерность пространства решений равна $n - k$, то есть $\dim U^\perp = n - k$.

Вторая часть доказательства является дословным повторением соответствующего куска доказательства Предложения 10.26. ■

Теорема 13.13. *Если $U \subset V$ — произвольное подпространство унитарного пространства (V, α), то $V = U \oplus U^\perp$.*

Доказательство. Теорема следует из того, что ограничение α на любое подпространство в V невырождено (ср. Предложение 10.30).

Более подробно, пусть $\mathbf{v} \in U \cap U^\perp (= \operatorname{Ker} \alpha|_U)$. Тогда $\alpha(\mathbf{v}, \mathbf{v}) = q_\alpha(\mathbf{v}) = 0$. Так как по условию α положительно определена, то $\mathbf{v} = \mathbf{0}$. Значит, сумма подпространств U и $U^\perp$ в V прямая, $\dim(U + U^\perp) = \dim U + \dim U^\perp = k + n - k = n = \dim V$, и значит $V = U \oplus U^\perp$. ■

Теорема 13.14. *В любом унитарном пространстве (V, α) есть ортонормированный базис.*

Доказательство. Будем доказывать теорему индукцией по $n := \dim V$. Если $n = 1$, то теорема очевидна. Действительно, если $\mathbf{v} \in V$ — произвольный ненулевой вектор, то $q_\alpha(\mathbf{v}) =: a > 0$. Тогда $\{\mathbf{u}\}$ — ортонормированный базис, где $\mathbf{u} := \frac{1}{\sqrt{a}}\mathbf{v}$.

Пусть теорема верна для пространств размерности, не превосходящей $n - 1$. Выберем произвольный вектор $\mathbf{u} \in V$, $\mathbf{u} \neq \mathbf{0}$ и положим $U := \langle \mathbf{u} \rangle$. Тогда $V = U \oplus U^\perp$ и $\dim U^\perp = n - 1$; по предположению индукции в $U^\perp$ есть ортонормированный базис. Объединяя его с ортонормированным базисом в U, получаем ортонормированный базис в V. ■

То есть любое n-мерное унитарное пространство изометрически изоморфно арифметическому пространству $\mathbb{C}^n$ с эрмитовой формой $\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \overline{x}_i y_i$.

Заметим, что как и в евклидовом случае, предыдущую Теорему можно было бы доказать, используя модификацию алгоритма Грама-Шмидта для унитарных пространств. Отметим еще, что в унитарном случае формула (98) дает равенство для коэффициентов

$$\lambda_j = -\frac{(f_j, e_k)}{|f_j|^2},$$

причем порядок векторов в числителе важен из-за полуторалинейности эрмитова скалярного произведения.

Следствие 13.15. *Для любой положительно определенной эрмитовой матрицы $G \in \mathrm{Mat}_n(\mathbb{C})$ существует невырожденная матрица $C \in \mathrm{GL}_n(\mathbb{C})$ такая, что*

$$\overline{C}^T G C = E. \tag{118}$$

Доказательство. В произвольном базисе n-мерного комплексного пространства V формула

$$\alpha(\mathbf{u}, \mathbf{v}) = \overline{u} G v$$

задает положительно определенную эрмитову форму. Рассмотрим пару (V, α) как унитарное пространство. Согласно предыдущей теореме, в нем существует ортонормированный базис. Пусть C — матрица

перехода от исходного базиса к ортонормированному. Теперь все следует из (115) и того, что в ортонормированном базисе матрица положительно определенной эрмитовой формы единичная. ■

Кстати, из формулы (118) следует, что определитель матрицы положительно определенной эрмитовой формы положителен (выше уже отмечалось, что для эрмитовых форм имеет место аналог критерия Сильвестра).

Заметим, что базис $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ унитарного пространства (V, α) ортонормирован тогда и только тогда, когда матрица формы α в этом базисе единичная. Из (115) следует, что матрица C перехода между двумя ортонормированными базисами в (V, α) удовлетворяет тождеству $\overline{C}^T C = E$. Такие матрицы называются *унитарными* (они аналогичны ортогональным матрицам в вещественном случае). Очевидно, что определитель унитарной матрицы — (вообще говоря) комплексное число, равное 1 по модулю. Сопоставление базису матрицы перехода к нему от фиксированного базиса устанавливает биекцию между ортонормированными базисами в n-мерном унитарном пространстве и унитарными матрицами порядка n.

Начиная с этого момента упростим наши обозначения: эрмитову форму α из определения унитарного пространства (V, α) (напомним, что она линейна по второму аргументу и полулинейна по первому) будем обозначать круглыми скобками и называть (эрмитовым) *скалярным произведением*, и вместо $q_\alpha(\mathbf{v})(= \alpha(\mathbf{v}, \mathbf{v}))$ будем писать $|\mathbf{v}|^2$.

Как уже отмечалось выше, в унитарных пространствах имеют место аналоги неравенств Коши-Буняковского и треугольника. Приведем их доказательства (ср. раздел 11.4).

Определение 13.16. *Матрицей Грама* $G(v_1, \dots, v_k)$ системы векторов $\{v_1, \dots, v_k\}$ унитарного пространства V называется матрица $G = (g_{ij})$, $g_{ij} = (v_i, v_j)$, составленная из их попарных скалярных произведений.

Предложение 13.17. *Для любой системы векторов $\{v_1, \dots, v_k\}$ унитарного пространства V выполнено неравенство $\det G(v_1, \dots, v_k) \geq 0$, причем равенство нулю имеет место тогда и только тогда, когда система $\{v_1, \dots, v_k\}$ линейно зависима.*

Доказательство. Если система $\{v_1, \dots, v_k\}$ линейно независима, то она является базисом в своей линейной оболочке $U := \langle v_1, \dots, v_k \rangle$. Ограничение скалярного произведения на любое подпространство $U \subset V$ положительно определено, откуда (например, по формуле (118)) $\det G(v_1, \dots, v_k) > 0$.

Если система $\{v_1, \dots, v_k\}$ линейно зависима, то пусть $\sum_{i=1}^k \lambda_i v_i = 0$ — нетривиальная линейная зависимость. Скалярно умножая левую и правую части этого равенства на векторы v_j, $1 \leq j \leq k$, получаем $\sum_{i=1}^k \overline{\lambda}_i (v_i, v_j) = 0$, $1 \leq j \leq k$, что дает линейную зависимость между строками матрицы $G(v_1, \dots, v_k)$ с теми же коэффициентами. ■

Теорема 13.18. *(Неравенство Коши-Буняковского) Для любых векторов $\boldsymbol{u}$, $\boldsymbol{v}$ унитарного пространства V имеет место неравенство*

$$|(\boldsymbol{u}, \boldsymbol{v})|^2 \leq |\boldsymbol{u}|^2 |\boldsymbol{v}|^2, \tag{119}$$

причем равенство достигается тогда и только тогда, когда векторы $\boldsymbol{u}$ и $\boldsymbol{v}$ линейно зависимы.

Доказательство. 1-й способ. Согласно предыдущему Предложению,

$$\begin{pmatrix} |\mathbf{u}|^2 & (\mathbf{u}, \mathbf{v}) \\ (\mathbf{u}, \mathbf{v}) & |\mathbf{v}|^2 \end{pmatrix} = |u|^2 |v|^2 - |(u, v)|^2 \geq 0,$$

причем равенство имеет место тогда и только тогда, когда u и v линейно зависимы.

2-й способ. Для любого $\lambda \in \mathbb{C}$ имеет место неравенство

$$(\mathbf{u} + \lambda\mathbf{v},\, \mathbf{u} + \lambda\mathbf{v}) = |\mathbf{u}|^2 + \overline{\lambda}(\mathbf{v},\, \mathbf{u}) + \lambda(\mathbf{u},\, \mathbf{v}) + |\lambda|^2|\mathbf{v}|^2 \geq 0. \tag{120}$$

Если $(\mathbf{u},\, \mathbf{v}) = 0$, то (119) очевидно. В противном случае положим $\lambda = \frac{(\mathbf{v},\, \mathbf{u})}{|(\mathbf{u},\, \mathbf{v})|}t$, где $t \in \mathbb{R}$. Тогда (120) превратится в неравенство

$$|\mathbf{u}|^2 + 2|(\mathbf{u},\, \mathbf{v})|t + |\mathbf{v}|^2t^2 \geq 0,$$

верное для любого $t \in \mathbb{R}$. Значит, дискриминант квадратного трехчлена неотрицателен, что равносильно (119).

Доказательство второй части теоремы, касающейся равносильности условий достижения равенства и линейной зависимости векторов, оставим читателю. ■

Следствие 13.19. *Для любых двух непрерывных функций $f,\, g\colon [0,\, 1] \to \mathbb{C}$ имеет место неравенство*

$$\left|\int_0^1 \overline{f(t)}g(t)\,dt\right|^2 \leq \int_0^1 |f(t)|^2\,dt \int_0^1 |g(t)|^2\,dt,$$

причем равенство достигается тогда и только тогда, когда f и g пропорциональны.

Доказательство. Запишите неравенство Коши-Буняковского (119) для примера 13.7. ■

Следствие 13.20. *(Неравенство треугольника) Для любых векторов $\boldsymbol{u}$, $\boldsymbol{v}$ унитарного пространства V имеет место неравенство $|\boldsymbol{u} + \boldsymbol{v}| \leq |\boldsymbol{u}| + |\boldsymbol{v}|$.*

Доказательство следует из цепочки неравенств:

$$(|\mathbf{u}| + |\mathbf{v}|)^2 = |\mathbf{u}|^2 + 2|\mathbf{u}||\mathbf{v}| + |\mathbf{v}|^2 \geq |\mathbf{u}|^2 + 2|(\mathbf{u},\, \mathbf{v})| + |\mathbf{v}|^2 \geq |\mathbf{u}|^2 + 2\mathrm{Re}\,(\mathbf{u},\, \mathbf{v}) + |\mathbf{v}|^2 = |\mathbf{u} + \mathbf{v}|^2. \quad ■$$

Замечание 13.21. Если $\mathbf{u}$, $\mathbf{v}$ — ненулевые векторы унитарного пространства V, то из неравенства Коши-Буняковского следует, что

$$0 \leq \frac{|(\mathbf{u},\, \mathbf{v})|}{|\mathbf{u}||\mathbf{v}|} \leq 1.$$

Таким образом, существует единственный угол φ, $0 \leq \varphi \leq \frac{\pi}{2}$ такой, что

$$\cos\varphi = \frac{|(\mathbf{u},\, \mathbf{v})|}{|\mathbf{u}||\mathbf{v}|}.$$

Он называется *углом между векторами* $\mathbf{u}$ и $\mathbf{v}$. В математической модели квантовой механики $\cos^2\varphi$ имеет смысл вероятности (см. [17]).

13.3 Линейные преобразования унитарных пространств

Мы уже знаем, что в евклидовом пространстве V благодаря присутствию скалярного произведения каждому линейному оператору $\varphi\colon V \to V$ можно сопоставить его сопряженный $\varphi^*\colon V \to V$, и, соответственно, возникают понятия симметричного, или, что то же, самосопряженного ($\varphi^* = \varphi$), кососимметричного ($\varphi^* = -\varphi$) и ортогонального ($\varphi^{-1} = \varphi^*$) операторов. То же верно и для унитарного пространства, только несколько меняется терминология: самосопряженные называются еще эрмитовыми, аналоги кососимметричных — косоэрмитовыми, ортогональных — унитарными операторами.

Сопряженное преобразование.

Итак, пусть V — унитарное пространство, а $\varphi\colon V \to V$ — линейный оператор на нем.

Определение 13.22. Преобразование $\varphi^*\colon V \to V$ называется *сопряженным* к φ, если оно удовлетворяет тождеству

$$(\varphi(\mathbf{u}),\, \mathbf{v}) = (\mathbf{u},\, \varphi^*(\mathbf{v})) \quad \forall \mathbf{u},\, \mathbf{v} \in V$$

(напомним, что $(\cdot,\cdot)$ обозначает эрмитово скалярное произведение в V).

Во-первых, заметим, что если сопряженное преобразование существует, то оно *единственно*. В самом деле, пусть φ_1, φ_2 — два сопряженных к φ. Тогда $(\mathbf{u},\, (\varphi_1 - \varphi_2)(\mathbf{v})) = 0 \quad \forall \mathbf{u},\, \mathbf{v} \in V$. Фиксируя $\mathbf{v}$, из невырожденности эрмитова скалярного произведения получаем $(\varphi_1 - \varphi_2)(\mathbf{v}) = 0$; поскольку это выполнено для любого $\mathbf{v}$, то $\varphi_1 = \varphi_2$.

Во-вторых, заметим, что сопряженное преобразование *линейно*. В самом деле,

$$(\mathbf{u},\, \varphi^*(\mathbf{v}_1 + \mathbf{v}_2)) = (\varphi(\mathbf{u}),\, \mathbf{v}_1 + \mathbf{v}_2) = (\varphi(\mathbf{u}),\, \mathbf{v}_1) + (\varphi(\mathbf{u}),\, \mathbf{v}_2) =$$

$$(\mathbf{u},\, \varphi^*(\mathbf{v}_1)) + (\mathbf{u},\, \varphi^*(\mathbf{v}_2)) = (\mathbf{u},\, \varphi^*(\mathbf{v}_1) + \varphi^*(\mathbf{v}_2));$$

поскольку это выполнено для любого $\mathbf{u} \in V$, то $\varphi^*(\mathbf{v}_1 + \mathbf{v}_2) = \varphi^*(\mathbf{v}_1) + \varphi^*(\mathbf{v}_2)$. Далее,

$$(\mathbf{u},\, \varphi^*(\lambda\mathbf{v})) = (\varphi(\mathbf{u}),\, \lambda\mathbf{v}) = \lambda(\varphi(\mathbf{u}),\, \mathbf{v}) = \lambda(\mathbf{u},\, \varphi^*(\mathbf{v})) = (\mathbf{u},\, \lambda\varphi^*(\mathbf{v}))$$

и снова, поскольку это выполнено для любого $\mathbf{u} \in V$, то $\varphi^*(\lambda\mathbf{v}) = \lambda\varphi^*(\mathbf{v})$.

Существование сопряженного преобразования можно доказать по той же схеме что и в евклидовом случае. Например, приведем доказательство, использующее существование ортонормированных базисов в унитарном пространстве V. Пусть $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ — такой базис. Пусть оператор φ имеет в нем матрицу A. Рассмотрим оператор $\psi\colon V \to V$, который в этом базисе имеет матрицу $B := \overline{A}^T$. Тогда $(\varphi(\mathbf{u}),\, \mathbf{v}) = (\mathbf{u},\, \psi(\mathbf{v})) \;\; \forall \mathbf{u},\, \mathbf{v} \in V$. Действительно, последнее равенство в базисе имеет вид:

$$(\overline{Au})^T v = \overline{u}^T B v$$

и в силу определения B верно для любых столбцов u, v. Таким образом, в качестве φ^* нужно взять линейный оператор, который имеет матрицу $\overline{A}^T$ в базисе $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$.

Читателю предлагается проверить самостоятельно, что для базиса с матрицей Грама G матрица B сопряженного преобразования φ^* выражается через матрицу A преобразования φ по формуле $B = G^{-1}\overline{A}^T G$.

Далее так же как в случае евклидова пространства доказываются тождества (см. Предложение 12.4)

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*, \;\; (\varphi + \psi)^* = \varphi^* + \psi^*, \;\; \mathrm{Id}_V^* = \mathrm{Id}_V, \;\; \varphi^{**} = \varphi$$

с единственным отличием $(\lambda\varphi)^* = \overline{\lambda}\varphi^*$, для произвольного $\lambda \in \mathbb{C}$. В самом деле,

$$(\mathbf{u},\, (\lambda\varphi)^*(\mathbf{v})) = (\lambda\varphi(\mathbf{u}),\, \mathbf{v}) = \overline{\lambda}(\varphi(\mathbf{u}),\, \mathbf{v}) = \overline{\lambda}(\mathbf{u},\, \varphi^*(\mathbf{v})) = (\mathbf{u},\, \overline{\lambda}\varphi^*(\mathbf{v})).$$

Следующее Предложение — полный аналог Предложения 12.11 в евклидовом случае.

Предложение 13.23. *Пусть V — унитарное пространство, $\varphi\colon V \to V$ — линейный оператор на нем, $U \subset V$ — инвариантное относительно φ подпространство. Тогда подпространство $U^\perp \subset V$ инвариантно относительно φ^*.*

Доказательство. Для произвольных $\mathbf{u} \in U,\; \mathbf{v} \in U^\perp$

$$0 = (\varphi(\mathbf{u}),\, \mathbf{v}) = (\mathbf{u},\, \varphi^*(\mathbf{v})) \quad \Rightarrow \quad \varphi^*(\mathbf{v}) \in U^\perp. \quad \blacksquare$$

Самосопряженные преобразования.

Определение 13.24. Оператор $\varphi\colon V \to V$ на унитарном пространстве V называется *самосопряженным* или *эрмитовым*, если он равен своему сопряженному, $\varphi = \varphi^*$.

Из предыдущего следует такой результат:

Предложение 13.25. *Оператор на унитарном пространстве самосопряжен тогда и только тогда, когда его матрица в произвольном ортонормированном базисе эрмитова.*

Из Предложения 13.23 вытекает такое Следствие (ср. Предложение 12.13):

Следствие 13.26. *Ортогональное дополнение к инвариантному подпространству самосопряженного оператора инвариантно.*

Доказательство следующего результата в унитарном случае существенно проще, чем в евклидовом.

Предложение 13.27. *Все собственные значения самосопряженного оператора φ на унитарном пространстве V вещественны.*

Доказательство. Пусть $\lambda \in \mathbb{C}$ — собственное значение оператора φ. Тогда существует $\mathbf{v} \neq \mathbf{0}$ такой, что $\varphi(\mathbf{v}) = \lambda\mathbf{v}$. Тогда

$$\overline{\lambda}(\mathbf{v},\, \mathbf{v}) = (\lambda\mathbf{v},\, \mathbf{v}) = (\varphi(\mathbf{v}),\, \mathbf{v}) = (\mathbf{v},\, \varphi(\mathbf{v})) = (\mathbf{v},\, \lambda\mathbf{v}) = \lambda(\mathbf{v},\, \mathbf{v}).$$

Так как $(\mathbf{v},\, \mathbf{v}) \neq 0$, то $\lambda = \overline{\lambda}$. ■

Следствие 13.28. *Все корни характеристического многочлена $\chi_A(t) = \det(tE - A)$ эрмитовой матрицы A вещественны.*

Заметим, что симметричные вещественные матрицы — то же, что эрмитовы матрицы с вещественными элементами. Поэтому частным случаем предыдущего следствия является вещественность характеристических чисел вещественных симметричных матриц. Напомним, что вещественные симметричные матрицы — матрицы самосопряженных операторов в евклидовых пространствах в ортонормированных базисах. Тем самым мы получили третье (см. Предложение 12.16 и второе доказательство после Следствия 12.63) доказательство того, что у самосопряженного оператора в евклидовом пространстве положительной размерности есть собственный вектор. Напомним, что этот результат был сложной частью доказательства теоремы о том, что всякий самосопряженный оператор в евклидовом пространстве диагонализируется в некотором ортонормированном базисе. Следующая теорема является аналогом этой теоремы для унитарного случая.

Теорема 13.29. *(Теорема о каноническом виде эрмитового оператора). Линейный оператор φ в унитарном пространстве V самосопряжен $\Leftrightarrow$ он диагонализируется в некотором ортонормированном базисе и имеет вещественный спектр*[61].

Доказательство. Если оператор диагонализируется в ортонормированном базисе и имеет вещественный спектр, то его матрица в этом базисе диагональная с вещественными элементами на диагонали, значит она эрмитова. Мы уже знаем, что если оператор имеет эрмитову матрицу в некотором ортонормированном базисе, то он самосопряжен.

Обратно, пусть φ самосопряжен. Тогда, как мы уже выяснили, он имеет вещественный спектр. Существование ортонормированного базиса в V из его собственных векторов будем доказывать индукцией

[61] Спектром линейного оператора на конечномерном пространстве называется множество его собственных значений

по $\dim V$. Если $\dim V = 1$, то существование ортонормированного базиса очевидно. Пусть теорема верна для пространств размерности, не превосходящей $\dim V - 1$. Пусть $\mathbf{v}$ — произвольный собственный вектор оператора φ в V (любое линейное преобразование в комплексном пространстве имеет собственый вектор). Без ограничения общности можно предположить, что его длина равна 1. Подпространство $\langle \mathbf{v} \rangle \subset V$ инвариантно относительно φ. Значит, его ортогональное дополнение $\langle \mathbf{v} \rangle^\perp \subset V$ тоже инвариантно. Заметим, что $\dim \langle \mathbf{v} \rangle^\perp = n - 1$ и $V = \langle \mathbf{v} \rangle \oplus \langle \mathbf{v} \rangle^\perp$ — разложение в ортогональную прямую сумму. Кроме того, $\langle \mathbf{v} \rangle^\perp$ — унитарное пространство, а ограничение $\varphi|_{\langle \mathbf{v} \rangle^\perp}$ оператора φ на него — самосопряженный оператор на $\langle \mathbf{v} \rangle^\perp$. По предположению индукции в $\langle \mathbf{v} \rangle^\perp$ существует ортонормированный базис из собственных векторов оператора $\varphi|_{\langle \mathbf{v} \rangle^\perp}$. Добавляя к нему нормированный вектор $\mathbf{v}$, получаем искомый ортонормированный базис в V из собственных векторов оператора φ. ■

Заметим, что если λ — некоторое собственное значение оператора φ, то соответствующее собственное подпространство V_λ является линейной оболочкой собственных векторов из построенного в предыдущей теореме ортонормированного базиса, которые отвечают собственному значению λ. Таким образом, если $\lambda_1, \ldots, \lambda_k$ — все попарно различные собственные значения φ, то V раскладывается в *ортогональную* прямую сумму собственных подпространств, $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_k}$. Ортогональность собственных векторов самосопряженного оператора, отвечающих разным собственным значениям, легко проверить непосредственно: пусть $\varphi(\mathbf{u}) = \lambda \mathbf{u}$, $\varphi(\mathbf{v}) = \mu \mathbf{v}$, $\lambda \neq \mu$; тогда

$$\lambda(\mathbf{u}, \mathbf{v}) = (\varphi(\mathbf{u}), \mathbf{v}) = (\mathbf{u}, \varphi(\mathbf{v})) = \mu(\mathbf{u}, \mathbf{v});$$

так как $\lambda \neq \mu$, то $(\mathbf{u}, \mathbf{v}) = 0$.

Из предыдущей теоремы получаем следующее следствие.

Следствие 13.30. *Для любой эрмитовой матрицы A существует унитарная матрица U такая, что матрица $A' = \overline{U}^T A U$ диагональна с вещественными элементами на диагонали.*

Далее аналогично евклидовому случаю в унитарном пространстве устанавливается биекция между эрмитовыми формами и эрмитовыми операторами. Используя доказанные теоремы об эрмитовых операторах, доказывается существование ортонормированного базиса, в котором данная эрмитова форма имеет диагональный вид с вещественными числами на главной диагонали. Далее аналогично евклидовому случаю рассматривается задача о паре эрмитовых форм, одна из которых знакоопределена. Мы не будем делать это подробно, поскольку читатель, знакомый с евклидовым случаем, легко восстановит детали.

Унитарные преобразования.

Пусть V — унитарное пространство с эрмитовым скалярным произведением $(\cdot, \cdot)$.

Определение 13.31. Линейный оператор $\varphi\colon V \to V$ называется *унитарным*, если для любых $\mathbf{u}, \mathbf{v} \in V$

$$(\varphi(\mathbf{u}), \varphi(\mathbf{v})) = (\mathbf{u}, \mathbf{v}). \tag{121}$$

Таким образом, унитарные операторы — аналоги ортогональных и этим определяются их свойства. Унитарность оператора φ равносильна тождеству $\varphi^* = \varphi^{-1}$, в частности, любое унитарное преобразование обратимо. Для матрицы оператора в ортонормированном базисе оно превращается в условие $\overline{U}^T = U^{-1}$. Отсюда следует, что *оператор унитарный тогда и только тогда, когда в некотором (а значит в любом) ортонормированном базисе он имеет унитарную матрицу.*

Так же как в евклидовом случае доказывается (см. Предложение 12.36), что унитарные преобразования унитарного пространства образуют группу относительно операции композиции. Группа унитарных преобразований унитарного пространства V обозначается $\mathrm{U}(V)$. Она является подгруппой в $\mathrm{GL}(V)$ — группе всех обратимых линейных операторов на пространстве V относительно операции композиции — и

состоит в точности из тех преобразований, которые сохраняют фиксированное эрмитово скалярное произведение $(\cdot, \cdot)$. Выбор ортонормированного базиса определяет ее изоморфизм с группой $\mathrm{U}(n)$ унитарных матриц соответствующего размера. Определяется также подгруппа $\mathrm{SU}(V)$ группы $\mathrm{U}(V)$, состоящая из унитарных преобразований с определителем 1[62], изоморфная соответствующей подгруппе $\mathrm{SU}(n)$ группы $\mathrm{U}(n)$.

Получим теперь канонический вид унитарного преобразования $\varphi\colon V \to V$.

Предложение 13.32. *(ср. Предложение 12.38) Если $U \subset V$ является φ-инвариантным, то и $U^\perp \subset V$ является φ-инвариантным.*

Доказательство. Заметим, что $\varphi|_U\colon U \to U$ — унитарный (в частности, биективный) оператор на U. Значит, для любого $\mathbf{u} \in U$ $\exists \mathbf{u}' \in U$ такой, что $\varphi(\mathbf{u}') = \mathbf{u}$. Выберем произвольный $\mathbf{v} \in U^\perp$. Тогда

$$(\mathbf{u},\, \varphi(\mathbf{v})) = (\varphi(\mathbf{u}'),\, \varphi(\mathbf{v})) = (\mathbf{u}',\, \mathbf{v}) = 0. \quad \blacksquare$$

Предложение 13.33. *Если λ — собственное значение унитарного оператора φ, то $|\lambda| = 1$ (заметим, что λ, вообще говоря, комплексное число).*

Доказательство. Пусть $\mathbf{v} \in V$ — собственный вектор φ с собственным значением λ. Тогда

$$(\mathbf{v},\, \mathbf{v}) = (\varphi(\mathbf{v}),\, \varphi(\mathbf{v})) = |\lambda|^2 (\mathbf{v},\, \mathbf{v}).$$

Так как $(\mathbf{v},\, \mathbf{v}) \neq 0$, то $|\lambda|^2 = 1$. $\blacksquare$

Теорема 13.34. *Оператор $\varphi\colon V \to V$ является унитарным тогда и только тогда, когда он диагонализируется в ортонормированном базисе и имеет спектр, лежащий на единичной окружности в $\mathbb{C}$.*

Доказательство. Во-первых, заметим, что диагональная матрица с комплексными числами на главной диагонали, равными по модулю единице, унитарна.

Обратное утверждение (существование ортонормированного базиса из собственных векторов) будем доказывать индукцией по $\dim V$. Если $\dim V = 1$, то утверждение очевидно. Пусть $\dim V > 1$. Пусть $\mathbf{v}$ — собственный вектор унитарного преобразования φ (любое линейное преобразование в комплексном пространстве имеет собственый вектор). Без ограничения общности можно считать, что вектор $\mathbf{v}$ нормирован. Подпространство $\langle \mathbf{v} \rangle \subset V$ инвариантно, а значит инвариантно и его ортогональное дополнение $\langle \mathbf{v} \rangle^\perp$. По предположению индукции в $\langle \mathbf{v} \rangle^\perp$ существует требуемый базис для унитарного оператора $\varphi|_{\langle \mathbf{v} \rangle^\perp}$. Добавляя к нему нормированный вектор $\mathbf{v}$, получаем требуемый базис в V для φ. $\blacksquare$

Заметим, что легко доказать непосредственно, что собственные подпространства унитарного преобразования, отвечающие разным собственным значениям, ортогональны. В самом деле, пусть $\varphi(\mathbf{u}) = \lambda\mathbf{u}$, $\varphi(\mathbf{v}) = \mu\mathbf{v}$, $\lambda \neq \mu$. Тогда

$$(\mathbf{u},\, \mathbf{v}) = (\varphi(\mathbf{u}),\, \varphi(\mathbf{v})) = \overline{\lambda}\mu (\mathbf{u},\, \mathbf{v}).$$

Так как $\overline{\lambda}\mu \neq 1$ (здесь наряду с условием $\lambda \neq \mu$ мы используем $|\lambda| = 1 = |\mu|$), то $(\mathbf{u},\, \mathbf{v}) = 0$.

Заметим, что ортогональные матрицы порядка n — в точности унитарные матрицы того же порядка с вещественными элементами. Поэтому из предыдущей теоремы следует, что характеристические числа ортогональной матрицы лежат на единичной окружности в $\mathbb{C}$. Ранее этот результат был доказан несколько иначе (см. Следствие 12.65).

В заключении этого пункта сделаем несколько замечаний.

[62] Заметим, что определитель унитарной матрицы (унитарного оператора) — комплексное число, модуль которого равен 1.

Замечание 13.35. На понятии унитарного пространства, а также эрмитовых и унитарных операторов на нем основана математическая модель квантовой механики. Точнее, ненулевые векторы унитарного пространства (с точностью до умножения на ненулевое комплексное число) отвечают состояниям квантовой системы, в то время как эрмитовы операторы описывают наблюдаемые (такие как импульс, энергия или спин), а унитарные операторы — симметрии квантовой системы и ее эволюцию во времени. Подробности см. например в [17].

Замечание 13.36. Есть важная связь между эрмитовыми, косоэрмитовыми и унитарными операторами и матрицами. Как уже отмечалось, унитарные матрицы образуют группу по умножению. Эрмитовы и косоэрмитовы матрицы группы по умножению не образуют, они являются векторными пространствами над $\mathbb{R}$, переходящими друг в друга при умножении на i. Однако пространство косоэрмитовых матриц замкнуто относительно другой операции — взятия коммутатора. Получающаяся при этом структура называется *алгеброй Ли*. Она тесно связана с группой унитарных матриц, в частности, экспонента косоэрмитовой матрицы является унитарной матрицей. Аналогичная связь имеется между кососимметричными и ортогональными матрицами. Подробнее об этом можно прочитать например в [11], Гл. 12.

Замечание 13.37. Наконец, заметим, что для операторов в унитарном пространстве V имеет место полярное разложение. А именно, любой оператор φ можно представить в виде произведения неотрицательного (положительного для невырожденного φ) эрмитова и унитарного. Оно аналогично представлению комплексных чисел в показательной форме $z = re^{i\alpha}$, где $r, \alpha \in \mathbb{R}$, $r \geq 0$. При этом первому множителю отвечают неотрицательные эрмитовы операторы, а второму — унитарные. Доказательство аналогично евклидовому случаю.

Нормальные преобразования.

Читатель, вероятно, заметил общее свойство самосопряженных (эрмитовых) и унитарных преобразований: и те, и другие диагонализируются в некотором ортонормированном базисе. Они являются частными случаями так называемых *нормальных* преобразований унитарного пространства.

Предложение 13.38. *Следующие условия на линейный оператор φ на унитарном пространстве V эквивалентны:*

a) φ диагонализируется в ортонормированном базисе;

b) φ коммутирует со своим сопряженным φ^*.

Доказательство. Во-первых, из a) следует b). В самом деле, если $\varphi\colon V \to V$ имеет диагональную матрицу $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ в ортонормированном базисе $\{e_1, \ldots, e_n\}$ пространства V, то φ^* имеет в том же базисе диагональную матрицу $\operatorname{diag}(\overline{\lambda}_1, \ldots, \overline{\lambda}_n)$, а диагональные матрицы коммутируют.

Обратную импликацию b)⇒a) докажем индукцией по размерности $n = \dim V$. Случай $n = 1$ очевиден. Пусть $n > 1$ и доказываемое утверждение верно для пространств размерности меньше n. Для доказательства шага индукции рассмотрим собственное подпространство V_λ оператора φ. Из b) легко следует, что V_λ является φ^*-инвариантным (поскольку $\forall\, v \in V_\lambda\ \varphi(\varphi^*(v)) = \varphi^*(\varphi(v)) = \varphi^*(\lambda v) = \lambda\varphi^*(v)$), откуда в свою очередь непосредственно выводится (ср. Предложение 13.23), что подпространство $V_\lambda^\perp \subset V$ является одновременно φ и φ^*-инвариантным, причем ясно, что ограничения φ и φ^* на $V_\lambda^\perp$ коммутируют. По предположению индукции ограничение φ на $V_\lambda^\perp$ диагонализируемо в ортонормированном базисе, а так как то же верно и для ограничения φ на V_λ, то шаг индукции доказан. ■

Определение 13.39. Линейный оператор на унитарном пространстве, удовлетворяющий любому из эквивалентных условий a) или b) из формулировки предыдущего Предложения, называется *нормальным*.

Заметим, что, поскольку и для самосопряженного и для унитарного оператора выполнено условие b) предыдущего Предложения, мы еще раз доказали, что оба эти типа операторов диагонализируемы в ортонормированном базисе.

Задача 13.40. *Пусть V — конечномерное векторное пространство над полем $\mathbb{C}$. Верно ли, что для любого оператора $\varphi\colon V \to V$ найдутся многочлен $p(t) \in \mathbb{C}[t]$ и некоторый базис в V, в котором матрица A оператора φ удовлетворяет условию $\overline{A}^T = p(A)$?*

Решение. Допустим, для оператора φ такой базис существует; тогда для эрмитова скалярного произведения в V, для которого данный базис является ортонормированным, оператор φ^* коммутирует с φ, а значит является диагонализируемым, что в общем случае неверно. ■

14 Аффинные пространства и отображения

В курсе аналитической геометрии обычно рассматриваются пространства (точнее, плоскость и (трехмерное) пространство), элементами которых являются точки, а не векторы. (Свободные) векторы там появляются как классы эквивалентности упорядоченных пар точек. Точнее, с каждым "точечным" пространством ассоциируется линейное пространство свободных векторов. Например, декартова система координат в точечном пространстве состоит из фиксированной точки и базиса в ассоциированном пространстве свободных векторов. В этом разделе мы формализуем понятие точечного пространства из курса аналитической геометрии (по-научному называемого *аффинным пространством*) и связанного с этим понятием класса преобразований (которые называются *аффинными преобразованиями*).

Еще одну мотивировку рассмотрения аффинных пространств дает теория систем линейных уравнений. Мы знаем, что множество решений однородной системы линейных уравнений является линейным пространством (относительно операций сложения решений и умножения их на скаляры). Множество решений (даже совместной) неоднородной системы линейных уравнений линейным пространством уже не является; в то же время оно обладает некоторой структурой, поскольку ее общее решение есть сумма произвольного частного решения и общего решения соответствующей однородной системы. Геометрическую интерпретацию множества решений совместной неоднородной системы дают аффинные пространства.

14.1 Определение и примеры аффинных пространств

Определение 14.1. *Аффинным пространством* над полем $\mathbb{K}$ называется тройка $(S, V, +)$, где S — непустое множество (элементы которого мы будем называть "точками"), V — векторное пространство над полем $\mathbb{K}$ и

$$+\colon S \times V \to S, \quad (p, \mathbf{v}) \mapsto p + \mathbf{v} \in S \qquad p \in S, \mathbf{v} \in V$$

— операция сложения точки и вектора, обладающая свойствами:

1) $p + \mathbf{0} = p \ \ \forall p \in S$;

2) $p + (\mathbf{v} + \mathbf{w}) = (p + \mathbf{v}) + \mathbf{w} \ \ \forall p \in S, \forall \mathbf{v}, \mathbf{w} \in V$;

3) для любой упорядоченной пары (p, q) точек из S существует, причем единственный, вектор $\mathbf{v} \in V$ такой, что $q = p + \mathbf{v}$.

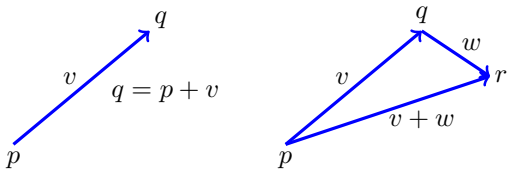
Если $p + \mathbf{v} = q$, положим $\overrightarrow{pq} := \mathbf{v}$. Если при этом $\mathbf{w} = \overrightarrow{qr}$, то свойство 2) тогда дает $p + (\overrightarrow{pq} + \overrightarrow{qr}) = (p + \overrightarrow{pq}) + \overrightarrow{qr} = q + \overrightarrow{qr} = r$ и из свойства 3) тогда следует, что $\overrightarrow{pq} + \overrightarrow{qr} = \overrightarrow{pr}$.

Кроме того, $\overrightarrow{qp} = -\overrightarrow{pq}$. Действительно, используя свойства 1) — 3) операции сложения точки и вектора, имеем:

$$q = p + \overrightarrow{pq} = (q + \overrightarrow{qp}) + \overrightarrow{pq} = q + (\overrightarrow{qp} + \overrightarrow{pq}) = q + \mathbf{0} \;\Rightarrow\; \overrightarrow{qp} + \overrightarrow{pq} = \mathbf{0} \;\Rightarrow\; \overrightarrow{qp} = -\overrightarrow{pq}.$$

Размерностью аффинного пространства $(S, V, +)$ называется размерность соответствующего векторного пространства V. Аффинные пространства размерности один и два называются соответственно *аффинной прямой* и *аффинной плоскостью* (также часто под *аффинным пространством* подразумевают трехмерное аффинное пространство).

Пример 14.2. Наиболее знакомый из курса аналитической геометрии пример — *аффинная плоскость* (для геометрической наглядности мы полагаем $\mathbb{K} = \mathbb{R}$). В этом случае S — множество точек плоскости, V — векторное пространство свободных векторов на плоскости, $+$ — операция откладывания представителя свободного вектора от точки



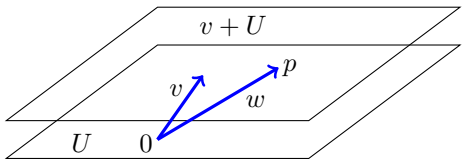
при этом сумма точки и вектора — точка, являющаяся концом отложенного вектора. Все свойства из Определения 14.1 легко проверяются.

Сейчас мы собираемся постоить модель n-мерного аффинного пространства с помощью линейной алгебры.

Пусть V — $n+1$-мерное линейное пространство, $U \subset V$ — его подпространство коразмерности 1. Пусть $v \in V$ — произвольный вектор, не лежащий в U; рассмотрим подмножество

$$v + U = \{v + u \mid u \in U\} \subset V$$

("сдвиг" подпространства U на вектор v). Заметим, что при условии $v \notin U$ подмножество $v + U \subset V$ не является линейным подпространством в V. Наглядно точки "n-мерной плоскости" $S := v + U$ можно представлять как концы векторов из подмножества $v+U \subset V$ (если эти векторы "откладывать от нулевого вектора" в V):



Покажем, что $(S, U, +)$ является аффинным пространством (здесь "$+$" обозначает операцию прибавления к вектору-точке из $S = v+U$ вектора из U в смысле линейной структуры в V). В самом деле, ясно, что прибавление любого вектора из U к точке из $v + U$ не выводит нас за пределы $v + U$; свойства 1) — 3) из Определения выше легко проверяются (точнее, следуют из аксиом линейного пространства).

Заметим, что подпространство U одноначно восстанавливается по подмножеству $S = v + U \subset V$: оно состоит из всех векторов вида $\overrightarrow{pq}$, где $p, q \in S$. Такое подпространство $U \subset V$ называется *направляющим подпространством* для $(S, U, +)$.

Определение 14.3. Тройка $(T,\, W,\, +)$ является *аффинным подпространством* аффинного пространства $(S,\, V,\, +)$, если $T \subset S$ — подмножество, $W \subset V$ — линейное подпространство, операция $T \times W \xrightarrow{+} T$ является ограничением операции $S \times V \xrightarrow{+} S$ и для $(T,\, W,\, +)$ выполнены аксиомы из Определения 14.1.

Аффинные подпространства в $(S,\, V,\, +)$ можно строить следующим образом. Пусть $W \subset V$ — произвольное линейное подпространство; фиксируем произвольную точку $p_0 \in S$. Положим

$$T := \{p_0 + \mathbf{w} \mid ; \mathbf{w} \in W\} \subset S.$$

Тогда $(T,\, W,\, +)$ — аффинное подпространство в $(S,\, V,\, +)$. Верно и обратное: любое аффинное подпространство в $(S,\, V,\, +)$ получается таким образом.

Одномерное аффинное подпространство естественно назвать (аффинной) прямой, двумерное — (аффинной) плоскостью и т.д.

Заметим, что пересечение аффинных подпространств в $(S,\, V,\, +)$ при условии, что оно непусто, снова является аффинным подпространством.

Подпространства линейного пространства можно задавать как линейные оболочки каких-то систем векторов. Для аффинного пространства есть аналогичное понятие — аффинная оболочка системы точек. Она определяется как наименьшее аффинное подпространство, содержащее данные точки.

Определение 14.4. Система точек $\{p_0,\, p_1, \ldots, p_k\}$ в аффинном пространстве $(S,\, V,\, +)$ называется *аффинно независимой*, если не существует $k-1$-мерного аффинного подпространства в $(S,\, V,\, +)$, которое их содержит.

Например, система из одной точки всегда аффинно независима, из двух — если они различны, из трех — если они не лежат на одной прямой, из четырех — если они не лежат в одной двумерной плоскости и т.д.

Вернемся к нашей модели n-мерного аффинного пространства $(S,\, U,\, +)$, где $S = v + U$. Пусть его точки $\{p_0,\, p_1, \ldots, p_k\}$ соответствуют векторам $\{v_0,\, v_1, \ldots, v_k\}$ в $v + U \subset V$ (то есть точка p_i — конец вектора v_i, "отложенного от $0 \in V$"). Положим также $u_i := v_i - v_0 \in U,\ 1 \leq i \leq k$ и $W := \langle u_1, \ldots, u_k \rangle \subset U$. Ясно, что $(p_0 + W,\, W,\, +)$ является наименьшим аффинным подпространством в $(v+U,\, U,\, +)$, содержащим все точки $p_i,\ 1 \leq i \leq k$ (поскольку $p_i = p_0 + u_i$ и $u_i = \overrightarrow{p_0 p_i}$).

Лемма 14.5. В предыдущих обозначениях система векторов $\{u_1, \ldots, u_k\}$ линейно независима тогда и только тогда, когда система векторов $\{v_0,\, v_1, \ldots, v_k\}$ линейно независима.

Доказательство. Пусть система $\{v_0,\, v_1, \ldots, v_k\}$ линейно зависима и $\sum_{i=0}^{k} \lambda_k v_k = 0$ — соответствующая нетривиальная линейная комбинация. Поскольку все $v_i \in v + U$, причем $v \notin U$, такое возможно только при условии $\sum_{i=0}^{k} \lambda_k = 0$. Поэтому $\lambda_0 = -\sum_{j=1}^{k} \lambda_j$ и

$$0 = \sum_{i=0}^{k} \lambda_k v_k = \sum_{j=1}^{k} \lambda_j v_j - \left(\sum_{j=1}^{k} \lambda_j \right) v_0 = \sum_{j=1}^{k} \lambda_j \,(v_j - v_0) = \sum_{j=1}^{k} \lambda_j u_j.$$

Обратно:

$$\sum_{j=1}^{k} \mu_j u_j = \sum_{j=1}^{k} \mu_j (v_i - v_0) = 0. \quad \blacksquare$$

Заметим, что условие линейной зависимости (или независимости) системы векторов $\{v_0,\, v_1, \ldots, v_k\}$ не зависит от их порядка, а значит линейная зависимость или независимость полученной из нее системы $\{v_0 - v_m,\, \ldots, v_{m-1} - v_m,\, v_{m+1} - v_m, \ldots, v_k - v_m\}$ не зависит от выбора вектора v_m.

Предложение 14.6. *Следующие условия эквивалентны:*

1) система точек $\{p_0, p_1, \ldots, p_k\}$ *аффинно независима;*

2) система векторов $\{u_1, \ldots, u_k\}$ *линейно независима.*

Доказательство. 1) $\Rightarrow$ 2): если система $\{u_1, \ldots, u_k\}$ линейно зависима, то $\dim W < k$ и все точки p_i, $1 \leq i \leq k$ лежат в $\dim W$-мерном аффинном подпространстве $p_0 + W$, то есть система точек $\{p_0, p_1, \ldots, p_k\}$ аффинно зависима.

2) $\Rightarrow$ 1): если система точек $\{p_0, p_1, \ldots, p_k\}$ аффинно зависима, то размерность направляющего подпространства $\langle\overrightarrow{p_0p_1}, \ldots, \overrightarrow{p_0p_k}\rangle$ их аффинной оболочки $< k$, откуда следует требуемое, поскольку $u_i = \overrightarrow{p_0p_i}$. ■

14.2 Декартовы системы координат

Пусть $(S, V, +)$ — аффинное n-мерное пространство.

Определение 14.7. *Декартовой системой координат* (кратко дск) в $(S, V, +)$ называется пара $o, \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$, состоящая из точки $o \in S$ и базиса $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ в V.

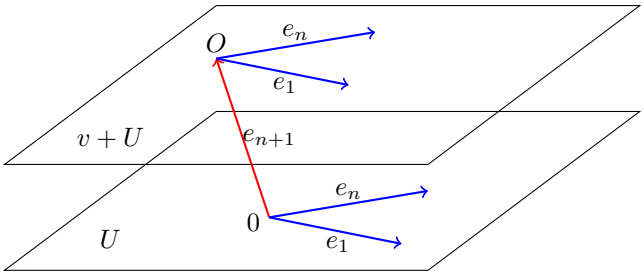
Если в пространстве $(S, V, +)$ задана дск $o, \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$, то координаты $(x_1, x_2, \ldots, x_n)^T$ произвольной точки $p \in S$ — это по определению координаты вектора $\overrightarrow{op} \in V$ в базисе $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$:

$$\overrightarrow{op} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \ldots + x_n\mathbf{e}_n.$$

Легко видеть, что координаты точки $q = p + \mathbf{v}$ равны суммам соответствующих координат точки p и вектора $\mathbf{v}$. Действительно, условие $q = p + \mathbf{v}$ превращается в $\overrightarrow{oq} = \overrightarrow{op} + \mathbf{v}$ и, как мы знаем, координаты вектора $\overrightarrow{oq}$ равны суммам соответствующих координат векторов $\overrightarrow{op}$ и $\mathbf{v}$. Отсюда получаем, что *координаты вектора* $\overrightarrow{pq}$ *равны разностям соответствующих координат точек* q *и* p.

Читателю предлагается убедиться, что прямые на плоскости и в пространстве, а также плоскости в пространстве имеют известные из курса аналитической геометрии уравнения.

Обратимся снова к введенной выше модели $(v + U, U, +)$ n-мерного аффинного пространства. Напомним, что U является n-мерным линейным подпространством $n+1$-мерного линейного пространства V. Выберем базис в V следующим образом: пусть $\{e_1, \ldots, e_n\}$ образуют базис в подпространстве U и $e_{n+1} \in v + U$. В этом базисе подмножество $v + U \subset V$ задается уравнением $x_{n+1} = 1$. Такой базис определяет некоторую декартову систему координат в $(v + U, U, +)$: в качестве точки $o \in v + U$ возьмем конец вектора e_{n+1}, а в качестве базиса в U — $\{e_1, \ldots, e_n\}$:



Тогда если вектор $w \in v + U$ имеет координаты $(x_1, \ldots, x_n, 1)^T$ в базисе $\{e_1, \ldots, e_n, e_{n+1}\}$ пространства V, то соответствующая ему точка в $(v + U, U, +)$ имеет координаты $(x_1, \ldots, x_n)^T$ в дск $o, \{e_1, \ldots, e_n\}$.

Подпространство $U \subset V$ характеризуется тем, что его векторы имеют нулевую $n+1$-ю координату, поэтому их прибавление к координатным столбцам $(x_1, \ldots, x_n, 1)^T$ не выводит за пределы указанного множества.

14.3 Аффинные отображения

Пусть $(S, V, +)$ и $(T, U, +)$ — аффинные пространства над одним и тем же полем $\mathbb{K}$.

Определение 14.8. *Аффинным отображением* $(S, V, +) \to (T, U, +)$ называется пара (f, φ), состоящая из отображения множеств $f\colon S \to T$ и линейного отображения $\varphi\colon V \to U$ такая, что $\forall\, p \in S$, $\forall\, \mathbf{v} \in V$

$$f(p + \mathbf{v}) = f(p) + \varphi(\mathbf{v}). \tag{122}$$

Заметим, что условие (122) равносильно условию коммутативности диаграммы

$$\begin{array}{ccc} S \times V & \xrightarrow{+} & S \\ {\scriptstyle f\times\varphi}\downarrow & & \downarrow{\scriptstyle f} \\ T \times U & \xrightarrow{+} & T \end{array}$$

Полезно также отметить, что линейное отображение φ восстанавливается по отображению f, удовлетворяющему условию (122). В самом деле, пусть $\mathbf{v} = \overrightarrow{pq}$, то есть $q = p + \mathbf{v}$; тогда $f(q) = f(p) + \varphi(\mathbf{v}) \Rightarrow \varphi(\mathbf{v}) = \overrightarrow{f(p)f(q)}$. Поэтому иногда мы будем для краткости записывать аффинное отображение просто как $f\colon S \to T$. Линейное отображение φ называется *дифференциалом* f, далее мы будем обозначать его df.

Наоборот, как непосредственно следует из (122), аффинное отображение f восстанавливается по своему дифференциалу df и образу $f(p) \in T$ произвольной точки $p \in S$.

Замечание 14.9. Заметим также, что выполнение свойства (122) достаточно потребовать для некоторой точки $p \in S$ и для любого вектора $\mathbf{v} \in V$, тогда оно будет верно для любой точки $q \in S$. Действительно, пусть $f(p + \mathbf{v}) = f(p) + df(\mathbf{v})\ \ \forall\, \mathbf{v} \in V$. Тогда

$$f(q + \mathbf{v}) = f((p + \overrightarrow{pq}) + \mathbf{v}) = f(p + (\overrightarrow{pq} + \mathbf{v})) = f(p) + df(\overrightarrow{pq} + \mathbf{v}) =$$
$$= f(p) + df(\overrightarrow{pq}) + df(\mathbf{v}) = f(p) + \overrightarrow{f(p)f(q)} + df(\mathbf{v}) = f(q) + df(\mathbf{v}).$$

Предложение 14.10. *Пусть $f\colon S \to T$, $g\colon T \to R$ — аффинные отображения. Тогда их композиция $g \circ f\colon S \to R$ — тоже аффинное отображение, причем $d(g \circ f) = (dg) \circ (df)$.*

Доказательство. Пусть $p \in S$, $\mathbf{v} \in V$. Тогда имеем:

$$(g \circ f)(p + \mathbf{v}) = g(f(p + \mathbf{v})) = g(f(p) + df(\mathbf{v})) = g(f(p)) + dg(df(\mathbf{v})) = (g \circ f)(p) + (dg \circ df)(\mathbf{v}),$$

откуда вытекает аффинность композиции $g \circ f$, так как композиция линейных отображений $dg \circ df$ линейна. ■

Оказывается, обратимость аффинного отображения полностью определяется его дифференциалом.

Предложение 14.11. *Аффинное отображение $f\colon S \to T$ биективно $\Leftrightarrow$ линейное отображение $df\colon V \to U$ биективно.*

Доказательство следует непосредственно из формулы $f(p + v) = f(p) + df(v)$ при фиксированном $p \in S$.

В самом деле, предположим, что f биективно. Тогда если df не инъективно, то есть существуют $v \neq w \in V$ такие, что $df(v) = df(w)$, то точки $p+v \neq p+w$ при применении f имеют одинаковые образы. С другой стороны, так как в силу сюръективности $f\ \ \forall\, q \in T$ уравнение $f(p+v) = q$ разрешимо относительно v при фиксированном p, то $\forall q \in T\ \exists v \in V$ такой, что $df(v) = \overrightarrow{f(p)q}$, что означает сюръективность df.

Предположим теперь что df биективно. Тогда если f не инъективно, то для некоторых $v \neq w \in V$ $f(p+v) = f(p+w)$, что противоречит инъективности df. С другой стороны, если $v \in V$ — прообраз вектора $\overrightarrow{f(p)q} \in U$ относительно df, то $f(p + v) = q$, то есть произвольная точка $q \in S$ лежит в образе f. ■

Как мы знаем, отображение, обратное к биективному линейному, тоже линейно. То же верно и для аффинных отображений.

Предложение 14.12. *Пусть $f\colon S \to T$ — биективное аффинное отображение. Тогда $f^{-1}\colon T \to S$ также аффинно, причем $d(f^{-1}) = (df)^{-1}$.*

Доказательство. Для биективного отображения f однозначно определено теоретико-множественное обратное f^{-1}. Докажем, что если f аффинно, то f^{-1} тоже аффинно, а именно что для любых точек p, $q \in S$ справедливо равенство

$$f^{-1}(q) = f^{-1}(p) + (df)^{-1}(\overrightarrow{pq}).$$

В самом деле,

$$f(f^{-1}(p) + (df)^{-1}(\overrightarrow{pq})) = f(f^{-1}(p)) + df(df^{-1}(\overrightarrow{pq})) = p + \overrightarrow{pq} = q = f(f^{-1}(q)),$$

откуда требуемое вытекает с учетом биективности f. ■

В качестве следствия из доказательства мы получили равенство $d(f^{-1}) = (df)^{-1}$ для биективного аффинного отображения f.

Определение 14.13. Два аффинных пространства $(S, V, +)$ и $(T, U, +)$ над одним и тем же полем *изоморфны* тогда и только тогда, когда существует биективное аффинное отображение $(f, df)\colon (S, V, +) \to (T, U, +)$.

Из доказанного выше следует, что на множестве всех аффинных пространств над данным полем отношение изоморфизма является отношением эквивалентности.

Теорема 14.14. *Аффинные пространства над данным полем изоморфны тогда и только тогда, когда они имеют одинаковую размерность.*

Доказательство. Из Предложения 14.11 следует, что если аффинные пространства изоморфны, то их размерности равны.

Докажем что верно обратное. Пусть $(S, V, +)$ и $(T, U, +)$ — аффинные пространства одинаковой размерности и $\varphi\colon V \to U$ — некоторый линейный изоморфизм. Выберем произвольные точки $p \in S$ и $q \in T$ и определим отображение $f\colon S \to T$ по формуле $f(p + v) = q + \varphi(v)$ $\forall v \in V$. Тогда из Замечания 14.9 следует, что так определенное f является аффинным; кроме того, $df = \varphi$, а значит по Предложению 14.11 f — изоморфизм. ■

В частности, любое n-мерное аффинное пространство изоморфно нашей модели $(v + U, U, +)$.

14.4 Аффинные преобразования

Определение 14.15. Аффинное отображение (f, df) из аффинного пространства $(S, V, +)$ в себя называется *аффинным преобразованием.*

Для краткости аффинное преобразование мы будем записывать просто $f\colon S \to S$.

Рассмотрим примеры аффинных преобразований.

Пример 14.16. Тождественное преобразование $f = \mathrm{Id}_S\colon S \to S$ является аффинным. Заметим, что его дифференциал — тождественное линейное преобразование $\mathrm{Id}_V\colon V \to V$.

Тождественное преобразование — частный случай классов преобразований из следующих двух примеров.

Пример 14.17. *Параллельный перенос на вектор* $\mathbf{v} \in V$ определяется следующим образом:

$$t_{\mathbf{v}} \colon S \to S, \quad t_{\mathbf{v}}(p) = p + \mathbf{v} \quad \forall\, p \in S.$$

Если $\mathbf{v} = \mathbf{0}$, то $t_{\mathbf{0}} = \mathrm{Id}_S$. Заметим, что дифференциал $dt_{\mathbf{v}} = \mathrm{Id}_V$. Действительно, если $\mathbf{w} = \overrightarrow{pq}$, то

$$dt_{\mathbf{v}}(\mathbf{w}) = dt_{\mathbf{v}}(\overrightarrow{pq}) = \overrightarrow{t_{\mathbf{v}}(p)t_{\mathbf{v}}(q)} = \overrightarrow{pq} = \mathbf{w}.$$

Обратно, пусть $f \colon S \to S$ — аффинное преобразование такое, что $df = \mathrm{Id}_V$. Покажем, что $f = t_{\mathbf{v}}$ для некоторого $\mathbf{v} \in V$. В самом деле, выберем некоторую точку $p \in S$ и положим $\mathbf{v} := \overrightarrow{pf(p)}$. Тогда для произвольной точки $q \in S$ имеем:

$$f(q) = f(p) + df(\overrightarrow{pq}) = f(p) + \overrightarrow{pq} = p + \mathbf{v} + \overrightarrow{pq} = p + \overrightarrow{pq} + \mathbf{v} = q + \mathbf{v} = t_{\mathbf{v}}(q).$$

Пример 14.18. *Гомотетией с центром в точке* $o \in S$ *и коэффициентом* λ называется аффинное преобразование, задаваемое формулой $f(o + \mathbf{v}) = o + \lambda\,\mathbf{v}$. Заметим, что из определения следует, что $df = \lambda\,\mathrm{Id}_V$.

Покажем, что, обратно, аффинное преобразование $f \colon S \to S$ такое, что $df = \lambda\,\mathrm{Id}_V$, $\lambda \neq 1$, есть гомотетия с центром в некоторой точке $o \in S$. Центр гомотетии o характеризуется тем, что это — неподвижная точка преобразования f, то есть $f(o) = o$. Покажем, что неподвижная точка в нашем случае действительно существует.

Пусть p — произвольная точка аффинного пространства S. Имеем:

$$f(o) = f(p + \overrightarrow{po}) = f(p) + df(\overrightarrow{po}) = f(p) + \lambda\,\mathrm{Id}_V(\overrightarrow{po}) = f(p) + \lambda\,\overrightarrow{po},$$

и если o — неподвижная точка, то $o = f(p) + \lambda\,\overrightarrow{po}$, то есть $\overrightarrow{po} = \overrightarrow{pf(p)} + \lambda\,\overrightarrow{po}$, тогда $\overrightarrow{po} = \frac{1}{1-\lambda}\overrightarrow{pf(p)}$. Проверим, что точка $o = p + \overrightarrow{po}$ неподвижна:

$$f(o) = f\left(p + \frac{1}{1-\lambda}\overrightarrow{pf(p)}\right) = f(p) + \frac{\lambda}{1-\lambda}\overrightarrow{pf(p)} =$$

$$= f(p) + \overrightarrow{f(p)p} + \frac{1}{1-\lambda}\overrightarrow{pf(p)} = p + \frac{1}{1-\lambda}\overrightarrow{pf(p)} = o.$$

Покажем теперь, что f — гомотетия с центром в неподвижной точке o. Пусть $q \in S$ — произвольная точка, тогда $f(q) = f(o + \overrightarrow{oq}) = f(o) + df(\overrightarrow{oq}) = o + \lambda\,\overrightarrow{oq}$, то есть f — действительно гомотетия с центром в точке o и коэффициентом λ.

Пример 14.19. Преобразование $f \colon S \to S$ такое, что $\forall\, q \in S$ $f(q) = p$, где $p \in S$ — фиксированная точка, является аффинным. Для него $df = 0$.

Вернемся к изучению общих свойств аффинных преобразований. Из результатов предыдущего параграфа легко выводится следующее

Следствие 14.20. *Биективные аффинные преобразования* $f \colon S \to S$ *образуют группу относительно операции композиции. Эта группа обозначается* $\mathrm{GA}(S)$ *и называется группой аффинных преобразований аффинного пространства* S.

Для аффинного пространства $(S, V, +)$ через $\mathrm{Trans}(S)$ обозначим подгруппу $\{t_{\mathbf{v}} \mid \mathbf{v} \in V\} \subset \mathrm{GA}(S)$ параллельных переносов (см. Пример 14.17). Очевидно, что сопоставление $\mathbf{v} \mapsto t_{\mathbf{v}}$ определяет изоморфизм $\mathrm{Trans}(S) \to (V, +)$ группы параллельных переносов с аддитивной группой $(V, +)$ пространства V.

Следствие 14.21. *Сопоставление* $f \mapsto df$ *задает гомоморфизм групп* $d \colon \mathrm{GA}(S) \to \mathrm{GL}(V)$ *с ядром* $\ker d = \mathrm{Trans}(S)$.

Доказательство. То, что d является гомоморфизмом групп, следует из Предложения 14.10.

Часть утверждения, касающаяся ядра, следует из Примера 14.17. ■

То, что подгруппа параллельных переносов является нормальной подгруппой в $\mathrm{GA}(S)$, можно проверить и непосредственно вычислением:

$$(ft_v f^{-1})(p) = f(f^{-1}(p) + v) = p + df(v) = t_{df(v)}(p)$$

для произвольных $f \in \mathrm{GA}(S)$ и $t_v \in \mathrm{Trans}(S)$.

Посмотрим теперь как аффинные преобразования задаются в декартовой системе координат. Пусть o, $\{e_1, \ldots, e_n\}$ — некоторая дск в аффинном пространстве $(S, V, +)$. Тогда из равенства $f(p) = f(o) + df(\overrightarrow{op})$ получаем равенство

$$(y_1, \ldots, y_n)^T = A(x_1, \ldots, x_n)^T + (b_1, \ldots, b_n)^T, \tag{123}$$

в котором $(y_1, \ldots, y_n)^T$, $(x_1, \ldots, x_n)^T$ и $(b_1, \ldots, b_n)^T$ — кординатные столбцы соответственно точек $f(p)$, p и $f(o)$ в дск o, $\{e_1, \ldots, e_n\}$, а A — матрица линейного преобразования df в базисе $\{e_1, \ldots, e_n\}$ пространства V. Другими словами, аффинное преобразование преобразует координатные столбцы точек по формуле $x \mapsto Ax + b$.

Вернемся теперь к нашей модели $(v+U, U, +)$ n-мерного аффинного пространства. Ее преимущество в том, что она хорошо демонстрирует связь между линейными и аффинными преобразованиями. А именно, мы собираемся доказать, что аффинные преобразования афинного пространства $(v + U, U, +)$ — это в точности ограничения на $v + U \subset V$ линейных преобразований объемлющего линейного пространства V, которые оставляют $v + U$ инвариантным.

Предложение 14.22. *Линейное преобразование $\varphi\colon V \to V$ оставляет подмножество $v + U \subset V$ инвариантным $\Leftrightarrow$ одновременно выполняются следующие условия:*

1) $\varphi(v) \in v + U$;

2) *подпротранство $U \subset V$ φ-инвариантно.*

Доказательство очевидно. ■

Пусть o, $\{e_1, \ldots, e_n\}$ — дск в $(v+U, U, +)$, отвечающая базису $\{e_1, \ldots, e_n, e_{n+1}\}$ в V (то есть $\{e_1, \ldots, e_n\}$ — базис в U, а начало координат $o \in v + U$ — конец вектора e_{n+1}). Тогда легко видеть, что матрица $\widetilde{A}$ оператора $\varphi\colon V \to V$ из предыдущего Предложения в базисе $\{e_1, \ldots, e_n, e_{n+1}\}$ имеет вид

$$\widetilde{A} = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}, \tag{124}$$

где A — матрица линейного оператора $\varphi|_U$ в базисе $\{e_1, \ldots, e_n\}$, а $\begin{pmatrix} b \\ 1 \end{pmatrix}$ — координатный столбец вектора $\varphi(e_{n+1})$ в базисе $\{e_1, \ldots, e_n, e_{n+1}\}$. Наоборот, любая матрица указанного вида является матрицей оператора на V, оставляющего $v + U$ инвариантным.

Заметим, что

$$\begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} Ax + b \\ 1 \end{pmatrix}. \tag{125}$$

Кроме того, напомним, что координаты точки из $v + U$ в дск o, $\{e_1, \ldots, e_n\}$ получаются из координат соответствующего вектора из $v+U$ в базисе $\{e_1, \ldots, e_n, e_{n+1}\}$ отбрасыванием последней единицы. Поэтому (125) равносильно формуле $x \mapsto Ax + b$ действия аффинного преобразования в координатах (ср. (123)).

Полученные результаты можно резюмировать в виде следующего Предложения.

Предложение 14.23. *Любое аффинное преобразование аффинного пространства $(v+U, U, +)$ получается ограничением линейного преобразования $\varphi\colon V \to V$ объемлющего пространства V, оставляющего $v+U \subset V$ инвариантным. При этом $\varphi|_U$ является дифференциалом соответствующего аффинного преобразования. Наоборот, ограничение на $v+U$ произвольного линейного преобразования $\varphi\colon V \to V$ объемлющего пространства V, оставляющего $v+U \subset V$ инвариантным, задает аффинное преобразование аффинного пространства $(v+U, U, +)$.*

Теперь например то, что композиция аффинных преобразований аффинна и дифференциал композиции равен композиции дифференциалов можно вывести из равенства

$$\begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} C & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AC & Ad+b \\ 0 & 1 \end{pmatrix}.$$

Кроме того, ясно, что матрица (124) обратима $\Leftrightarrow$ матрица A обратима, причем в последнем случае

$$\begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}b \\ 0 & 1 \end{pmatrix}.$$

Изучим теперь некоторые теоретико-групповые свойства группы $\mathrm{GA}(S)$, используя найденное нами ее матричное представление (в частности, с данного момента мы рассматриваем только обратимые аффинные преобразования).

Во-первых, гомоморфизм $d\colon \mathrm{GA}(S) \to \mathrm{GL}(U)$ в матричном виде выглядит как сопоставление

$$\begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \mapsto A.$$

Его ядром является подгруппа параллельных переносов, образованных матрицами вида $\begin{pmatrix} E & b \\ 0 & 1 \end{pmatrix}$ для всевозможных столбцов $b \in \mathbb{K}^n$. Значит, подгруппа параллельных переносов $\mathrm{Trans}(S)$ нормальна в $\mathrm{GA}(S)$ (см. Предложение 4.83).

Легко видеть, что матрицы вида $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$ образуют подгруппу в $\mathrm{GA}(S)$, изоморфную $\mathrm{GL}(U)$. Эта подгруппа состоит из всех аффинных преобразований аффиного пространства $(v+U, U, +)$, оставляющих точку o неподвижной, то есть является *стабилизатором* точки $o \in v+U$. Кроме того, равенство $\begin{pmatrix} E & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}$ показывает, что любой элемент из группы $\mathrm{GA}(S)$ является произведением параллельного переноса и элемента из стабилизатора, причем, как легко убедиться, это представление единственно (если произведение записывать в данном порядке). Это означает, что группа $\mathrm{GA}(S)$ является *полупрямым произведением* указанных подгрупп (о том, что это такое, можно почитать, например, в [11]).

Заметим, что точка $o \in v+U$ ничем не отличается от других точек аффинного пространства. Используя тот факт, что стабилизаторы разных точек одной орбиты действия группы сопряжены с помощью элемента, переводящего первую точку во вторую, найдем стабилизатор точки в $v+U$ с координатным столбцом $b \in \mathbb{K}^n$:

$$\begin{pmatrix} E & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} E & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & -Ab+b \\ 0 & 1 \end{pmatrix}.$$

То есть при любом фиксированном b матрицы вида $\begin{pmatrix} A & -Ab+b \\ 0 & 1 \end{pmatrix}$ для $A \in \mathrm{GL}_n(\mathbb{K})$ образуют подгруппу группы $\mathrm{GA}(S)$, изоморфную $\mathrm{GL}_n(\mathbb{K})$.

Задача 14.24. *Докажите, что композиция гомотетий с центрами в точках $p \neq q$ и коэффициентами λ, μ при $\lambda\mu \neq 1$ — гомотетия, а при $\lambda\mu = 1$ — нетривиальный[63] параллельный перенос.*

Задача 14.25. *Докажите, что группа преобразований аффинной плоскости S, порожденная гомотетиями с $\lambda \neq 0$ и параллельными переносами, допускает следующее описание. Ее элементами являются упорядоченные пары (b, λ), где $b \in \mathbb{K}^n$, $\lambda \in \mathbb{K}^*$, причем $(b, \lambda) \cdot (d, \mu) = (b + \lambda d, \lambda\mu)$. При этом роль нейтрального элемента играет $(0, 1)$, роль обратного — $(b, \lambda)^{-1} = (-\lambda^{-1}b, \lambda^{-1})$. (Таким образом, данная группа изоморфна полупрямому произведению $\mathrm{Trans}(S)$ и $\mathbb{K}^*$).*

Задача 14.26. *1) Докажите, что для одномерного аффинного пространства S над полем из трех элементов группа $\mathrm{GA}(S)$ изоморфна S_3. 2) Докажите, что для двумерного аффинного пространства S над полем из двух элементов группа $\mathrm{GA}(S)$ изоморфна S_4.*

Мы знаем, что для любых двух базисов в линейном пространстве V существует единственное линейное преобразование, переводящее первый базис во второй (с сохранением порядка векторов). Оно автоматически оказывается обратимым. Мы собираемся доказать аналогичное утверждение для аффинных пространств.

Предложение 14.27. *Пусть $\{p_0, \ldots, p_n\}$ — аффинно независимая система из $n+1$ точки в n-мерном аффинном пространстве $(S, V, +)$. Пусть $\{q_0, \ldots, q_n\}$ — произвольная система их $n+1$ точки в S. Тогда существует, причем единственное, аффинное преобразование $f\colon S \to S$ такое, что $f(p_i) = q_i$, $0 \leq i \leq n$, причем f биективно $\Leftrightarrow$ точки $\{q_0, \ldots, q_n\}$ аффинно независимы.*

Доказательство. Воспользуемся нашей моделью $(v+U, U, +)$ n-мерного аффинного пространства. Пусть системе точек $\{p_0, \ldots, p_n\}$ отвечает система векторов $\{v_0, \ldots, v_n\}$ объемлющего пространства V. Из аффинной независимости точек следует ее линейная независимость, то есть что $\{v_0, \ldots, v_n\}$ — базис в V. Аналогично, пусть точкам $\{q_0, \ldots, q_n\}$ отвечает система векторов $\{w_0, \ldots, w_n\}$ в V. Мы знаем, что тогда существует единственное линейное преобразование $\varphi\colon V \to V$ такое, что $\varphi(v_i) = w_i$, $0 \leq i \leq n$, причем оно будет изоморфизмом $\Leftrightarrow$ система $\{w_0, \ldots, w_n\}$ линейно независима, что равносильно аффинной независимости системы точек $\{q_0, \ldots, q_n\}$. Осталось заметить, что из условия следует, что $v + U$ инвариантно относительно φ. ■

В частности, из доказанного Предложения легко следует, что для любых двух дск в данном аффинном пространстве существует единственное аффинное преобразование, переводящее первую дск во вторую.

На этом мы завершаем наше краткое знакомство с аффинными пространствами. Далее можно было бы рассмотреть аффинные евклидова пространства $(S, V, +)$, для которых V не просто линейное, а евклидово пространство. В таких пространствах можно определить расстояние между точками (как $\mathrm{dist}(p, q) = |\overrightarrow{pq}|$), углы между подпространствами и т.д. В них можно рассматривать не просто дск, а прямоугольные декартовы системы координат (пдск). В группе аффинных преобразований такого пространства имеется подгруппа движений — преобразований, сохраняющих расстояния между точками. Аффинное преобразование f является движением тогда и только тогда, когда его дифференциал $df\colon V \to V$ является ортогональным преобразованием евклидова пространства V. Группа движений также является полупрямым произведением — группы параллельных переносов в S и группы ортогональных преобразований евклидова пространства V. В физике есть важный аналог этой группы: группа Пуанкаре, являющаяся полупрямым произведением группы параллельных переносов и группы Лоренца. Также можно было бы изучить и классифицировать аффинные квадрики. Некоторые дальнейшие результаты читатель сможет найти например в [11], [17].

[63] то есть на ненулевой вектор.

15 Тензоры

Тензор — общее понятие линейной алгебры, частными случаями которого являются векторы, линейные формы, линейные операторы, билинейные формы и множество других более сложных объектов.

При изучении линейной алгебры становится ясно, что с векторным пространством V связано множество других векторных пространств: двойственное пространство V^*, пространство $\mathcal{L}(V)$ линейных операторов на V, пространство $\mathcal{B}(V)$ билинейных форм на V, или, более общо, пространство k-линейных форм на V, можно также рассмотреть пространство всех линейных отображений $V \to \mathcal{L}(V)$ и т.д. Элементы этих пространств и являются тензорами разных типов на V.

Причем каждому базису $e = \{e_1, \ldots, e_n\}$ в V естественно сопоставляется некоторый базис в каждом из этих пространств (биортогональный к e базис в V^*, базис в $\mathcal{L}(V)$, состоящий из операторов ψ_{ij}, $1 \le i, j \le n$, переводящих e_i в e_j, а остальные базисные векторы — в нуль и т.п.). Значит, замена координат (отвечающая замене базиса) в V приводит к замене координат тензоров в каждом из этих пространств.

Тензорная (или полилинейная) алгебра — классический раздел линейной алгебры, давно вошедший в подробные учебники по этому предмету. Существуют разные подходы к ее изложению. Самый "элементарный" (но не самый прозрачный на наш взгляд) подход состоит в том, чтобы постулировать закон преобразования координат тензора при замене базиса. Недостатком его является то, что он не позволяет развить геометрическую интуицию. Чтобы обосновать этот тезис, приведем определения вектора и линейного оператора, как они выглядели бы при таком подходе (читатель легко убедится в эквивалентности этих определений "обычным").

> Вектором в n-мерном пространстве V называется множество упорядоченных наборов из n скаляров (v^i), по одному для каждого базиса в V, причем для двух базисов e и e', связанных матрицей перехода C, элементы второго набора выражаются через первый по формуле $v'^i = \sum_j d^i_j v^j$, где $D = (d^i_j)$ — матрица, обратная матрице перехода C[64].
>
> Линейный оператор на V — это множество наборов из n^2 скаляров (a^i_j), по одному для каждого базиса в V, причем для двух базисов e и e', связанных матрицей перехода C, элементы наборов связаны формулой $a'^k_l = \sum_{i,j} d^k_i a^i_j c^j_l$, где $C = (c^i_j)$ — матрица перехода, а $D = (d^i_j)$ — обратная к ней матрица[65].

Общий тензор на V при таком подходе выглядит как набор массивов $(a^{i_1 \ldots i_p}_{j_1 \ldots j_q})$ из n^{p+q} скаляров (которые можно записывать в "многомерные матрицы"), по одному массиву для каждого базиса в V, которые преобразуются по постулируемым формулам при переходе от одного базиса к другому (см. формулу (131)).

Второй способ определения тензора использует понятие полилинейной функции (или формы). Этот подход более геометричен и позволяет лучше понять идею тензора и более свободно с ней обращаться. От него легко перейти к координатной записи тензоров, если в этом возникает необходимость (как правило, при решении конкретных задач). Этого подхода достаточно для большинства классических применений, однако он все же не дает настолько глубокого понимания тензорной алгебры, какое дает третий подход — через тензорное произведение линейных пространств и его универсальное свойство.

Для данного текста мы выбрали изложение через полилинейные формы, параллельно приводя и координатную форму конструкций и результатов. Из известных автору учебников наиболее близкое к нашему

[64] В этой формуле читатель легко узнает закон (49) преобразования координат вектора при замене базиса. Заметим, что в этих обозначениях верхний индекс i элемента d^i_j матрицы обозначает номер строки, а нижний индекс j — номер столбца.

[65] В этой формуле читатель легко узнает закон (55) преобразования элементов матрицы линейного оператора при замене базиса.

изложение дается в [16]. Что касается тензорного произведения пространств, то оно излагается (в порядке возрастания сложности) в пособии [6] и учебниках [11], [17].

Тема "Тензоры" традиционно вызывает интерес у студентов, которые постоянно сталкиваются с этим понятием в физических приложениях. Мы надеемся, что данная глава заложит необходимую математическую основу для понимания этих приложений. Хотя в тексте разобрано довольно много примеров и задач, их, по-видимому, недостаточно для активного овладения теорией (особенно мало в тексте вычислительных задач). Поэтому наряду с данным текстом мы рекомендуем задачники [1] и [9]; в случае затруднений читатель может также обратиться к решебникам [8] и [12].

15.1 Определение тензора и примеры

Пусть V — конечномерное векторное пространство над полем $\mathbb{K}$.

Определение 15.1. *Тензором типа* $(p,\, q)$ *на* V называется полилинейное отображение

$$\varphi\colon \underbrace{V\times\ldots\times V}_{q\text{ штук}}\times\underbrace{V^*\times\ldots\times V^*}_{p\text{ штук}}\to\mathbb{K}.$$

Тензоры типа $(p,\, q)$ можно складывать и умножать на скаляры как полилинейные отображения. Точнее,

$$(\varphi_1+\varphi_2)(v_1,\ldots,v_q;\,f_1,\ldots,f_p):=\varphi_1(v_1,\ldots,v_q;\,f_1,\ldots,f_p)+\varphi_2(v_1,\ldots,v_q;\,f_1,\ldots,f_p)$$

и

$$(\lambda\varphi)(v_1,\ldots,v_q;\,f_1,\ldots,f_p):=\lambda\varphi(v_1,\ldots,v_q;\,f_1,\ldots,f_p)$$

для любых $v_i\in V,\ f_j\in V^*$ и $\lambda\in\mathbb{K}$.

Легко видеть, что относительно данных операций тензоры типа $(p,\, q)$ на V образуют линейное пространство, которое мы будем обозначать $\mathbf{T}^p_q(V)$.

Посмотрим, что из себя представляют тензоры типа $(p,\, q)$ для малых p и q.

Непосредственно из определения следует, что тензор типа $(0,\, 1)$ — линейная форма на V, то есть $\mathbf{T}^0_1(V)=V^*$. Линейная форма в тензорной алгебре часто называется также *ковектором.*

По определению, тензор типа $(1,\, 0)$ — линейное отображение $V^*\to\mathbb{K}$, то есть линейная форма на V^*. Ранее в параграфе 7.6 такие линейные формы мы отождествили с элементами пространства V, построив канонический изоморфизм $\vartheta\colon V\xrightarrow{\cong}V^{**}$ (см. Теорему 7.103).

Напоминание. Идея задания линейного отображения ϑ основана на двойственной природе записи $f(v)$, где $f\in V^*,\ v\in V$. А именно, если мы фиксируем f и меняем $v\in V$, то получаем линейную функцию на V (то есть f), а если фиксируем v и меняем $f\in V^*$, получаем линейную функцию на V^*, тем самым вектор v задает линейную функцию $\vartheta_v\in V^{**}$ на двойственном пространстве V^* по формуле $\vartheta_v(f)=f(v)\ \forall f\in V^*$. Более того, так как ϑ для конечномерного пространства V является изоморфизмом, то все линейные функции на V^* имеют вид ϑ_v для некоторого $v\in V$. То есть для любой линейной функции $\varepsilon\colon V^*\to\mathbb{K}$ существует такой единственный вектор $v=v(\varepsilon)\in V$, что $\varepsilon=\vartheta_v$.

Таким образом, произвольное линейное отображение $V^*\to\mathbb{K}$ отвечает вектору $v\in V$, и пространство тензоров $\mathbf{T}^1_0(V)$ (по определению совпадающее с пространством V^{**}) можно канонически отождествить с V. То есть тензоры типа $(1,\, 0)$ на V — векторы пространства V. С учетом этого отождествления вместо записи $\vartheta_v(f)$ можно также пользоваться записью $v(f)$ для $f\in V^*$, $v\in V$, отождествляя вектор v с тем линейным функционалом на V^*, который он определяет.

Далее, тензоры типа $(0,\, 2)$ по определению суть билинейные отображения $V\times V\to\mathbb{K}$, то есть пространство $\mathbf{T}^0_2(V)$ совпадает с пространством билинейных форм $\mathcal{B}(V)$ на V. Аналогично, пространство тензоров типа $(2,\, 0)$ отождествляется с пространством $\mathcal{B}(V^*)$ билинейных форм на V^*.

Менее тривиален вопрос о том, что представляет из себя простейший смешанный тензор — типа $(1,\, 1)$.

Предложение 15.2. *Существует канонический изоморфизм линейных пространств* $\mathbf{T}^1_1(V) \cong \mathcal{L}(V)$, *где* $\mathcal{L}(V)$ — *пространство линейных операторов на* V.

Доказательство. Во-первых, покажем как по тензору $\varphi \in \mathbf{T}^1_1(V)$ построить линейный оператор на V. Заметим, что при фиксированном v функция $\varphi(v,\, f)$ линейна по f и, значит, является линейной формой на V^*. Для любой линейной формы на V^* существует такой единственный вектор $w \in V$, что она совпадает с формой ϑ_w. То есть $\forall v \in V\ \exists! w = \psi(v) \in V$[66] такой, что $\varphi(v,\, f) = \vartheta_{\psi(v)}(f)\ \ \forall f \in V^*$. Напомним, что $\vartheta_{\psi(v)}(f) = f(\psi(v))$ в силу определения ϑ. То есть

$$\varphi(v,\, f) = f(\psi(v))\ \ \forall\, f \in V^*. \tag{126}$$

Покажем теперь, что вектор $\psi(v) \in V$ линейно зависит от $v \in V$, то есть является линейным оператором на V. Используя (126), получаем

$$f(\psi(v_1 + v_2)) = \varphi(v_1 + v_2,\, f) = \varphi(v_1,\, f) + \varphi(v_2,\, f) =$$

$$= f(\psi(v_1)) + f(\psi(v_2)) = f(\psi(v_1) + \psi(v_2)) \quad \forall f \in V^*,$$

откуда $\psi(v_1 + v_2) = \psi(v_1) + \psi(v_2)$. Аналогично,

$$f(\psi(\lambda v)) = \varphi(\lambda v,\, f) = \lambda\varphi(v,\, f) = \lambda f(\psi(v)) = f(\lambda\psi(v)) \quad \forall f \in V^*,$$

откуда $\psi(\lambda v) = \lambda\psi(v)$. Таким образом, ψ в самом деле является линейным оператором. Если потребуется подчеркнуть зависимость ψ от φ, мы будем его также обозначать ψ_φ.

Докажем, что отображение $\mathbf{T}^1_1(V) \to \mathcal{L}(V),\ \ \varphi \mapsto \psi_\varphi$, является линейным. Действительно,

$$f(\psi_{\varphi_1+\varphi_2}(v)) = (\varphi_1 + \varphi_2)(v,\, f) = \varphi_1(v,\, f) + \varphi_2(v,\, f) =$$

$$= f(\psi_{\varphi_1}(v)) + f(\psi_{\varphi_2}(v)) = f(\psi_{\varphi_1}(v) + \psi_{\varphi_1}(v)) \quad \text{для любых}\ \ v \in V,\, f \in V^*,$$

откуда $\psi_{\varphi_1+\varphi_2}(v) = \psi_{\varphi_1}(v) + \psi_{\varphi_1}(v)\ \ \forall\, v \in V$, то есть $\psi_{\varphi_1+\varphi_2} = \psi_{\varphi_1} + \psi_{\varphi_2}$, и аналогично для умножения на скаляры.

Обратно, пусть дан линейный оператор $\psi \in \mathcal{L}(V)$. Тогда $\varphi\colon V \times V^* \to \mathbb{K}$, $\quad \varphi(v,\, f) := f(\psi(v))$ — билинейное отображение, то есть $\varphi \in \mathbf{T}^1_1(V)$. Тем самым мы определили отображение $\mathcal{L}(V) \to \mathbf{T}^1_1(V)$. Из формулы (126) легко увидеть, что оно является обратным к ранее построенному отображению $\mathbf{T}^1_1(V) \to \mathcal{L}(V)$. ■

Задача 15.3. *Какому тензору типа* (1, 1) *отвечает тождественный оператор* $\mathrm{Id}_V \in \mathcal{L}(V)$*?*

Пример 15.4. Коротко обсудим тензоры типа (1, 2), то есть трилинейные отображения

$$\varphi\colon V \times V \times V^* \to \mathbb{K}.$$

Если в выражении $\varphi(v,\, w;\, f)$ зафиксировать первые два аргумента $v,\, w \in V$, то полученная функция от $f \in V^*$ будет линейной, и, значит, для $\forall v,\, w \in V\ \exists!\, \mu(v,\, w) \in V$ такой, что

$$\varphi(v,\, w;\, f) = f(\mu(v,\, w)) \tag{127}$$

(μ также зависит от φ). Легко проверяется, что вектор $\mu(v,\, w)$ линейно зависит от v и w. То есть $\mu\colon V \times V \to V$ — билинейное умножение на V. Обратно, имея такое умножение, по формуле (127) можно определить тензор φ типа (1, 2). То есть тензоры типа (1, 2) — билинейные умножения на V. С примерами таких умножений мы уже встречались: если V — трехмерное евклидово ориентированное пространство, то такой операцией является векторное произведение векторов, а если V — пространство квадратных матриц фиксированного порядка, то такой операцией является умножение матриц (или взятия их коммутатора $X,\, Y \mapsto [X,\, Y] := XY - YX$).

[66] Вектор $w \in V$ мы обозначили $\psi(v)$ чтобы подчеркнуть его зависимость от v.

Задача 15.5. *Постройте изоморфизм между пространством* $\mathcal{L}(V, V; V)$ *билинейных отображений* $V \times V \to V$ *и пространством* $\mathcal{L}(V; \mathcal{L}(V))$ *линейных отображений* $V \to \mathcal{L}(V)$.

Кроме того, по определению, тензоры типа (0, 0) отождествляются со скалярами, то есть $\mathbf{T}_0^0(V) = \mathbb{K}$.

Следует отметить, что тензоры высоких рангов естественно возникают не только в чистой математике, но и в ее приложениях. Например, тензор кривизны Римана, описывающий кривизну пространства (или пространства-времени), важный в общей теории относительности, имеет тип (1, 3).

15.2 Тензорное произведение тензоров

Если бы пространства $\mathbf{T}_q^p(V)$ при разных (p, q) были бы никак между собой не связаны, понятие тензора не представляло бы большого интереса: оно просто давало бы другие названия известным объектам линейной алгебры (векторам, билинейным формам, линейным операторам, ...). Однако на самом деле пространства $\mathbf{T}_q^p(V)$ при разных (p, q) связаны друг с другом множеством отображений, и тензорная алгебра систематически изучает связи между тензорами разных типов. Примерами таких связей являются изученные нами ранее в курсе линейной алгебры изоморфизмы между евклидовым пространством и его двойственным, а также между пространством линейных операторов и билинейных форм на евклидовом пространстве.

Основными операциями над тензорами являются их тензорное произведение и свертка (в частности, подъем и опускание индексов). На самом деле, на этом языке описываются все операции линейной алгебры (вычисление значения линейной формы или линейного оператора на векторе, композиция операторов и т.д.).

Мы уже встречались с тензорным произведением в очень частном случае, см. Пример 10.17.

Определение 15.6. *Тензорным произведением* тензоров $\varphi \in \mathbf{T}_q^p(V)$ и $\psi \in \mathbf{T}_s^r(V)$ называется тензор $\varphi \otimes \psi \in \mathbf{T}_{q+s}^{p+r}(V)$, определяемый формулой

$$(\varphi \otimes \psi)(v_1, \dots, v_{q+s};\, f_1, \dots, f_{p+r}) = \varphi(v_1, \dots, v_q;\, f_1, \dots, f_p)\psi(v_{q+1}, \dots, v_{q+s};\, f_{p+1}, \dots, f_{p+r}),$$

где $v_i \in V,\ f_j \in V^*$.

Тот факт, что тензорное произведение действительно представляет собой тензор указанного типа (полилинейное отображение), очевиден. Также просто проверяется, что тензорное произведение определяет билинейное отображение

$$\mathbf{T}_q^p(V) \times \mathbf{T}_s^r(V) \to \mathbf{T}_{q+s}^{p+r}(V),$$

то есть $(\varphi_1 + \varphi_2) \otimes \psi = \varphi_1 \otimes \psi + \varphi_2 \otimes \psi$, $(\lambda\varphi) \otimes \psi = \lambda(\varphi \otimes \psi)$ и т.д.

Из определения очевидна также ассоциативность тензорного произведения, то есть $(\varphi \otimes \psi) \otimes \chi = \varphi \otimes (\psi \otimes \chi)$. Однако тензорное произведение не коммутативно, то есть, вообще говоря, $\varphi \otimes \psi \neq \psi \otimes \varphi$. Чтобы убедиться в этом, возьмем две линейные формы $\varphi, \psi \in \mathbf{T}_1^0(V) = V^*$, где $\dim V \geq 2$ и рассмотрим две билинейные формы на V, $\varphi \otimes \psi$ и $\psi \otimes \varphi$. Тогда их значения на паре $(v, w) \in V \times V$ суть $\varphi(v)\psi(w)$ и $\psi(v)\varphi(w)$. Но легко подобрать такую пару линейных форм и такую пару векторов, что первый из рассматриваемых скаляров равен 1, а второй — 0 (детали предоставляются читателю).

Пример 15.7. Пусть, например, $w \in \mathbf{T}_0^1(V)$, $\alpha \in \mathbf{T}_1^0(V)$; тогда $\alpha \otimes w \in \mathbf{T}_1^1(V)$. По определению, $(\alpha \otimes w)(v, f) = \alpha(v)f(w) = f(\alpha(v)w)$ (последнее равенство следует из линейности f). Подставляя в формулу (126) $\varphi = \alpha \otimes w$, получаем $(\alpha \otimes w)(v, f) = f(\psi(v))$ для соответствующего $\alpha \otimes w$ линейного оператора ψ. Сравнивая две последние формулы получаем, что оператор $\psi\colon V \to V$, отвечающий тензору $\varphi = \alpha \otimes w \in \mathbf{T}_1^1(V)$ при каноническом изоморфизме $\mathbf{T}_1^1(V) \to \mathcal{L}(V)$, построенном в Предложении 15.2, действует на вектор $v \in V$ по формуле $\psi(v) = \alpha(v)w$.

Не следует думать, что любой оператор на V при $\dim V > 1$ получается приведенным выше способом: легко видеть, что ранг оператора $v \mapsto \alpha(v)w$ не превосходит 1. В то же время любой оператор ранга 1 является оператором такого вида (для соответствующих ковектора α и вектора w) и, значит, любой линейный оператор на V является линейной комбинацией таких.

Задача 15.8. *Пусть α, $\beta \in V^*$, $w \in V$. Какое билинейное отображение $\mu\colon V \times V \to V$ (см. Пример 15.4) отвечает тензору $\alpha \otimes \beta \otimes w$ типа $(1,2)$?*

Задача 15.9. *Всякий линейный оператор $\psi\colon V \to V$ ранга 1 имеет вид $v \mapsto \alpha(v)w \quad \forall\, v \in V$, где пара $\alpha \in V^*$, $w \in V$ определена оператором ψ однозначно с точностью до замены $\alpha \mapsto \lambda\,\alpha$, $w \mapsto \lambda^{-1}w$ для $\lambda \in \mathbb{K}^*$.*

Решение. $\operatorname{rk}\psi = \dim \operatorname{Im}\psi = 1 \quad \Leftrightarrow \quad \operatorname{Im}\psi = \langle w\rangle$ для некоторого $w \in V$, $\quad w \neq 0$. Тогда $\psi(v) = \alpha(v)w$, где $\alpha\colon V \to \mathbb{K}$ — некоторая функция, причем из линейности ψ следует, что $\alpha(v)$ линейно зависит от v, то есть является линейной формой.

Ясно, что вектор w такой, что $\operatorname{Im}\psi = \langle w\rangle$, определен оператором ψ однозначно с точностью до ненулевого множителя. Также ясно, что $\langle\alpha\rangle = (\operatorname{Ker}\psi)^0$[67], поэтому $\alpha \in V^*$ также определен ψ однозначно с точностью до ненулевого множителя. Дальнейшее очевидно. ■

15.3 Координаты тензора

Пусть V — конечномерное векторное пространство над полем $\mathbb{K}$. Тогда легко видеть, что для любых натуральных p, q $\mathbf{T}^p_q(V)$ является конечномерным векторным пространством над тем же полем. Действительно, полилинейное отображение $\varphi \in \mathbf{T}^p_q(V)$ однозначно определяется своими значениями на наборах, состоящих из q базисных векторов из V и p базисных векторов из V^*. В этом разделе мы построим важный класс базисов в $\mathbf{T}^p_q(V)$.

Зафиксируем некоторый базис $\{e_1, \dots, e_n\}$ в V. Пусть $\{e^1, \dots, e^n\}$ — биортогональный базис в V^*[68], то есть такой, что $e^j(e_i) = \delta^j_i = \begin{cases} 1, & \text{если } i = j; \\ 0, & \text{если } i \neq j. \end{cases}$

Тогда в $\mathbf{T}^p_q(V)$ определен набор n^{p+q} элементов $e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p}$, где i_k и j_l независимо пробегают значения $1, 2, \dots, n$. По определению тензорного произведения $\otimes$,

$$(e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p})(v_1, \dots, v_q;\, f_1, \dots, f_p) = e^{j_1}(v_1) \dots e^{j_q}(v_q) f_1(e_{i_1}) \dots f_p(e_{i_p}).$$

В частности,

$$(e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p})(e_{l_1}, \dots, e_{l_q};\, e^{k_1}, \dots, e^{k_p}) = \delta^{j_1}_{l_1} \dots \delta^{j_q}_{l_q} \delta^{k_1}_{i_1} \dots \delta^{k_p}_{i_p}. \tag{128}$$

Теорема 15.10. *Набор n^{p+q} элементов $\{e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p} \mid 1 \leq i_k, j_l \leq n\}$ пространства $\mathbf{T}^p_q(V)$ является базисом в $\mathbf{T}^p_q(V)$.*

Доказательство. Нужно проверить, что указанные тензоры линейно независимы и что любой тензор типа (p, q) представляется в виде их линейной комбинации.

Пусть полилинейная функция

$$\sum \lambda^{i_1 \dots i_p}_{j_1 \dots j_q} e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p}$$

[67] Напомним (см. (59)) что U^0 обозначает *аннулятор* подпространства $U \subset V$, $U^0 := \{f \in V^* \mid f(u) = 0\, \forall u \in U\} \subset V^*$.

[68] ранее обозначаемый нами $\{\varepsilon_1, \dots, \varepsilon_n\}$, см. Определение 7.99.

равна 0. Тогда, вычисляя ее значения на наборе $(e_{l_1}, \ldots, e_{l_q}; e^{k_1}, \ldots, e^{k_p})$ с помощью (128), получаем, что $\lambda_{l_1 \ldots l_q}^{k_1 \ldots k_p} = 0$. Таким образом, линейная независимость элементов набора доказана.

Для любого тензора $\varphi \in \mathbf{T}_q^p(V)$ определен набор n^{p+q} скаляров

$$\varphi_{j_1 \ldots j_q}^{i_1 \ldots i_p} := \varphi(e_{j_1}, \ldots, e_{j_q}; e^{i_1}, \ldots, e^{i_p}) \in \mathbb{K} \tag{129}$$

(набор значений полилинейного отображения φ на всевозможных наборах базисных векторов и ковекторов). Заметим также, что полилинейное отображение однозначно определяется своими значениями на таких наборах $(e_{j_1}, \ldots, e_{j_q}; e^{i_1}, \ldots, e^{i_p})$, то есть если значения двух полилинейных отображений на всех наборах $(e_{j_1}, \ldots, e_{j_q}; e^{i_1}, \ldots, e^{i_p})$ совпадают, то и полилинейные отображения совпадают. Отсюда следует, что полилинейное отображение

$$\phi := \sum \varphi_{j_1 \ldots j_q}^{i_1 \ldots i_p} e^{j_1} \otimes \ldots \otimes e^{j_q} \otimes e_{i_1} \otimes \ldots \otimes e_{i_p}$$

совпадает с φ, а значит указанный в условии теоремы набор тензоров является базисом в $\mathbf{T}_q^p(V)$. ■

Следствие 15.11. *Если* $\dim V = n$, *то* $\dim \mathbf{T}_q^p(V) = n^{p+q}$.

Базис в условии предыдущей теоремы называется *тензорным базисом пространства* $\mathbf{T}_q^p(V)$, отвечающим выбранному базису $\{e_1, \ldots, e_n\}$ в пространстве V, а скаляры (129) — *координатами* (или *компонентами*) *тензора* φ в этом тензорном базисе. Таким образом, тензорных базисов в $\mathbf{T}_q^p(V)$ столько же, сколько базисов в V (конечно, вообще говоря, не всякий базис в линейном пространстве $\mathbf{T}_q^p(V)$ является тензорным).

Пример 15.12. Рассмотрим пространство $\mathbf{T}_2^0(V)$ тензоров типа (0, 2), то есть билинейных функций на V. Пусть $\varphi\colon V \times V \to \mathbb{K}$ — такая функция, тогда $\varphi = \sum_{i,\,j} \varphi_{ij} e^i \otimes e^j$, причем $\varphi(v,\, w) = \sum \varphi_{ij} v^i w^j$ (здесь v^i и w^j — координаты векторов v и w в базисе $\{e_1, \ldots, e_n\}$ в V), в частности,

$$\varphi(e_k,\, e_l) = \sum_{i,\,j} \varphi_{ij} \delta_k^i \delta_l^j = \varphi_{kl}.$$

Значит, координаты φ_{ij} тензора α в тензорном базисе $\{e^i \otimes e^j \mid 1 \leq i,\, j \leq n\}$ суть матричные элементы матрицы билинейной формы φ в базисе $\{e_1, \ldots, e_n\}$ пространства V.

В частности, если $(V,\, \varphi)$ — евклидово пространство, а $\{e_1, \ldots, e_n\}$ — ортонормированный базис, то $\varphi = \sum_i e^i \otimes e^i$.

Пример 15.13. Рассмотрим пространство $\mathbf{T}_1^1(V)$ тензоров типа (1, 1) на V. Пусть $\varphi\colon V \times V^* \to \mathbb{K}$ — такой тензор. Тогда $\varphi = \sum_{i,j} \varphi_j^i e^j \otimes e_i$. Напомним, что для такого φ существует единственный линейный оператор $\psi\colon V \to V$ такой, что $\varphi(v,\, f) = f(\psi(v)) \ \ \forall v \in V,\, f \in V^*$. Имеем

$$\varphi(e_l,\, e^k) = \sum_{i,j} \varphi_j^i e^j(e_l) e^k(e_i) = \sum_{i,j} \varphi_j^i \delta_l^j \delta_i^k = \varphi_l^k = e^k(\psi(e_l)),$$

причем последнее выражение есть k-я координата вектора $\psi(e_l)$ в базисе $\{e_1, \ldots, e_n\}$ пространства V. Таким образом, если верхний индекс i рассматривать как номер строки, а нижний индекс j — как номер столбца, то $A_\psi := (\varphi_j^i)$ — матрица линейного оператора ψ в базисе $\{e_1, \ldots, e_n\}$. Иными словами, тензорные координаты тензора $\varphi \in \mathbf{T}_1^1(V)$ в тензорном базисе $\{e^j \otimes e_i \mid 1 \leq i,\, j \leq n\}$ суть не что иное как матричные элементы соответствующего линейного оператора ψ в базисе $\{e_1 \ldots, e_n\}$ пространства V. В частности, линейный оператор ψ в базисе $\{e_1, \ldots, e_n\}$ действует по формуле

$$\psi(e_l) = \sum_k \varphi_l^k e_k = \sum_k e_k \varphi_l^k, \ \ 1 \leq l \leq n,$$

что можно представить также как равенство $(\psi(e_1), \ldots, \psi(e_n)) = (e_1, \ldots, e_n) A_\psi$ (ср. определение матрицы линейного оператора в базисе).

Заметим, что тождественный оператор Id_V отвечает тензору $\sum_i e^i \otimes e_i \in \mathbf{T}_1^1(V)$ (для любого выбора базиса $\{e_1, \ldots, e_n\}$ в V).

Задача 15.14. [12] *Пусть* $\varphi\colon V\times V\times V^*\times V^*\to\mathbb{K}$ *— полилинейное отображение, заданное формулой*

$$\varphi(u,v;\alpha,\beta)=\det\begin{pmatrix}\alpha(u) & \beta(u)\\ \alpha(v) & \beta(v)\end{pmatrix}.$$

Найти разложение тензора $\varphi\in\mathbf{T}_2^2(V)$ *по базису* $\{e^i\otimes e^j\otimes e_k\otimes e_l\mid 1\le i,j,k,l\le\dim V\}$.

Решение. Полилинейность φ следует из линейности определителя по строкам и столбцам. Имеем

$$\varphi_{ij}^{kl}=\varphi(e_i,e_j;e^k,e^l)=\det\begin{pmatrix}e^k(e_i) & e^l(e_i)\\ e^k(e_j) & e^l(e_j)\end{pmatrix}=$$

$$=\det\begin{pmatrix}\delta_i^k & \delta_i^l\\ \delta_j^k & \delta_j^l\end{pmatrix}=\delta_i^k\delta_j^l-\delta_j^k\delta_i^l,$$

откуда

$$\varphi=\sum_{i,j,k,l}(\delta_i^k\delta_j^l-\delta_j^k\delta_i^l)e^i\otimes e^j\otimes e_k\otimes e_l=\sum_{i,j}(e^i\otimes e^j\otimes e_i\otimes e_j-e^i\otimes e^j\otimes e_j\otimes e_i).\quad\blacksquare$$

15.4 Изменение координат тензора при замене базиса

Как изменяются координаты тензора при изменении базиса $\{e_1,\dots,e_n\}$ в пространстве V? Заметим, что так как каждому базису в V отвечает единственный биортогональный базис в V^*, то замене базиса в V полностью определяет замену биортогональных им базисов в V^*.

Напомним, что замена базиса задается матрицей перехода. Итак, пусть даны два базиса $\{e_1,\dots,e_n\}$ и $\{e'_1,\dots,e'_n\}$ в V и C — матрица перехода от первого ко второму, то есть

$$(e'_1,\dots,e'_n)=(e_1,\dots,e_n)C.$$

Последнее равенство в наших новых обозначениях перепишется в виде $e'_i=\sum_j e_jc_i^j$ (напомним, что верхний индекс — номер строки, а нижний — столбца). Пусть

$$e'^i=\sum_j d_j^ie^j,\tag{130}$$

где $D=(d_j^i)$ — некоторая матрица порядка n. Имеем

$$\delta_j^i=e'^i(e'_j)=e'^i\left(\sum_k e_kc_j^k\right)=\sum_l d_l^ie^l\left(\sum_k e_kc_j^k\right)=\sum_{k,l}d_l^i\delta_k^lc_j^k=\sum_k d_k^ic_j^k$$

(произведение i-й строки матрицы D на j-й столбец матрицы C), откуда $D=C^{-1}$ (ср. Задачу 7.100). В матричном виде равенство (130) записывается так:

$$\begin{pmatrix}e'^1\\ \vdots\\ e'^n\end{pmatrix}=D\begin{pmatrix}e^1\\ \vdots\\ e^n\end{pmatrix}$$

(ср. формулу замены координат вектора при замене базиса).

Итак, пусть $\varphi\in\mathbf{T}_q^p(V)$ — некоторый тензор. Имеем

$$\varphi'^{k_1\dots k_p}_{l_1\dots l_q}=\varphi(e'_{l_1},\dots,e'_{l_q};e'^{k_1},\dots,e'^{k_p})=\varphi\left(\sum_{j_1}e_{j_1}c_{l_1}^{j_1},\dots,\sum_{j_q}e_{j_q}c_{l_q}^{j_q};\sum_{i_1}d_{i_1}^{k_1}e^{i_1},\dots,\sum_{i_p}d_{i_p}^{k_p}e^{i_p}\right)=$$

$$=\sum c_{l_1}^{j_1}\dots c_{l_q}^{j_q}d_{i_1}^{k_1}\dots d_{i_p}^{k_p}\varphi(e_{j_1},\dots,e_{j_q};e^{i_1},\dots,e^{i_p})=\sum c_{l_1}^{j_1}\dots c_{l_q}^{j_q}d_{i_1}^{k_1}\dots d_{i_p}^{k_p}\varphi^{i_1\dots i_p}_{j_1\dots j_q}.$$

Таким образом, получаем искомую формулу преобразования координат тензора:

$$\varphi'^{k_1\dots k_p}_{l_1\dots l_q} = \sum c^{j_1}_{l_1}\dots c^{j_q}_{l_q} d^{k_1}_{i_1}\dots d^{k_p}_{i_p}\varphi^{i_1\dots i_p}_{j_1\dots j_q}. \tag{131}$$

Запомнить ее можно так: при указанной замене базисов верхние индексы i_r преобразуются с помощью матричных элементов d^i_k матрицы $D = C^{-1}$, а нижние индексы j_s — с помощью матрицы C.

Последнюю формулу иногда берут за определение тензора. А именно, тензором на V типа (p, q) называют соответствие φ, относящее каждому базису пространства V систему из n^{p+q} скаляров $\varphi^{i_1\dots i_p}_{j_1\dots j_q}$ таким образом, что системы, отвечающие различным базисам, связаны между собой соотношениями (131). Убедиться в эквивалентности этих двух определений читателю предлагается самостоятельно.

Если $\varphi, \psi \in \mathbf{T}^p_q(V)$, то тензорными координатами линейной комбинации $\lambda\varphi + \mu\psi$ будут $\lambda\varphi^{i_1\dots i_p}_{j_1\dots j_q} + \mu\psi^{i_1\dots i_p}_{j_1\dots j_q}$. Операция тензорного умножения также может быть легко описана в терминах координат. Пусть $\varphi \in \mathbf{T}^p_q(V)$, $\psi \in \mathbf{T}^r_s(V)$ и $\chi := \varphi\otimes\psi \in \mathbf{T}^{p+r}_{q+s}(V)$. Тогда

$$\chi^{i_1\dots i_p k_1\dots k_r}_{j_1\dots j_q l_1\dots l_s} = \varphi^{i_1\dots i_p}_{j_1\dots j_q}\,\psi^{k_1\dots k_r}_{l_1\dots l_s}. \tag{132}$$

Полезно заметить, что правая часть последнего равенства действительно является тензором, так как преобразуется согласно (131) как тензор типа $(p + r, q + s)$. Заметим также, что если наборы тензорных координат тензоров одного типа совпадают в некотором тензорном базисе, то они совпадают и в любом другом, поскольку преобразуются по одинаковым формулам (131).

Пример 15.15. Из формулы (131) следует, что координаты тензора $\varphi \in \mathbf{T}^1_0(V)$ преобразуются по формуле $\varphi'^k = \sum_i d^k_i\varphi^i$, как и должны изменяться координаты вектора при замене базиса.

Пример 15.16. Из формулы (131) следует, что координаты тензора $\varphi \in \mathbf{T}^0_1(V)$ преобразуются по формуле $\varphi'_l = \sum_j c^j_l\varphi_j$, как и должны изменяться координаты ковектора (линейной формы) относительно биортогонального базиса. А именно, чтобы получить координатную строку линейной формы относительно нового базиса, нужно координатную строку в старом базисе умножить на матрицу перехода.

Пример 15.17. В случае тензоров типа (0, 2), то есть билинейных форм на V, читателю предлагается убедиться самостоятельно, что формула (131) дает формулу замены $B' = C^TBC$ матрицы билинейной формы при замене базиса (напомним, что в Примере 15.12 мы показали, что φ_{ij} — матричные элементы матрицы билинейной формы).

Пример 15.18. Рассмотрим случай тензоров типа (1, 1). Напомним (см. Пример 15.13), что если $\varphi \in \mathbf{T}^1_1(V)$, то φ^i_j — матричные элементы соответствующего линейного оператора ψ в базисе $\{e_1, \dots, e_n\}$. С одной стороны, имеем $\psi(e'_l) = \sum_k \varphi'^k_l e'_k$; с другой стороны,

$$\psi(e'_l) = \psi\left(\sum_j c^j_l e_j\right) = \sum_j c^j_l\psi(e_j) = \sum_{i,\,j} c^j_l\varphi^i_j e_i = \sum_{i,\,j,\,k} c^j_l\varphi^i_j d^k_i e'_k = \sum_{i,\,j,\,k} d^k_i\varphi^i_j c^j_l e'_k = \sum_k \varphi'^k_l e'_k,$$

откуда $\varphi'^k_l = \sum_{i,\,j} d^k_i\varphi^i_j c^j_l$ (что совпадает с (131) при $(p, q) = (1, 1)$). Полученная формула эквивалентна $A'_\psi = C^{-1}A_\psi C$, то есть формуле замены матрицы линейного оператора при замене базиса.

Например, очень легко убедиться, что сопоставление любому базису набора $\{\delta^i_j\}$ определяет тензор типа (1, 1), который отвечает тождественному линейному оператору.

Пример 15.19. Выше (см. Пример 15.4) мы убедились, что тензоры типа (1, 2) — билинейные умножения (структуры алгебры) на V. Пусть φ — такой тензор. Тогда легко получить, что его координаты φ^k_{ij} вычисляются из билинейного умножения $\cdot$[69] на базисных векторах e_i по формуле $e_i\cdot e_j = \sum_k \varphi^k_{ij}e_k$. Докажем независимо, что эти коэффициенты действительно преобразуются согласно закону преобразования

[69] Чтобы упростить обозначения из примера 15.4 мы полагаем $v\cdot w := \mu(v, w)$.

координат тензора типа (1, 2). Имеем

$$\sum_k \varphi'^k_{ij} e'_k = e'_i \cdot e'_j = \left(\sum_l c^l_i e_l\right) \cdot \left(\sum_m c^m_j e_m\right) = \sum_{l,\,m} c^l_i c^m_j e_l \cdot e_m = \sum_{l,\,m,\,r} c^l_i c^m_j \varphi^r_{lm} e_r =$$

$$= \sum_{l,\,m,\,r,\,k} c^l_i c^m_j \varphi^r_{lm} d^k_r e'_k.$$

Сравнивая коэффициенты перед e'_k, получаем $\varphi'^k_{ij} = \sum_{l,\,m,\,r} c^l_i c^m_j d^k_r \varphi^r_{lm}$, что совпадает с (131) в случае $(p,\,q) = (1,\,2)$. Тензор φ называется *тензором структурных констант* соответствующей алгебры.

Задача 15.20. *Покажите, что сопоставление каждому базису евклидова пространства матрицы, обратной матрице Грама этого базиса, определяет некоторый тензор типа* (2, 0). *Какое инвариантное определение имеет этот тензор?*

Решение. При замене базиса с матрицей перехода C обратная к матрице Грама G меняется согласно формуле $G'^{-1} = (C^T G C)^{-1} = C^{-1} G^{-1} C^{-T}$. Оставим читателю проверку того, что эта матричная формула задает закон преобразования координат тензора типа (2, 0).

Мы знаем, что тензор типа (2, 0) — билинейная функция на пространстве V^*. Напомним (см. Предложение 11.9), что для евклидова пространства V есть канонический изоморфизм $\alpha = \alpha_V \colon V \to V^*$, $\alpha(v) = (\,\cdot\,, v)$. Определим билинейную функцию $\psi \colon V^* \times V^* \to \mathbb{R}$, полагая

$$\psi(\alpha(v), \alpha(w)) = (v, w) \quad \forall\, v,\, w \in V. \tag{133}$$

Покажем, что тензор ψ — искомый.

Заметим, что изоморфизм $\alpha \colon V \to V^*$ в паре базисов $e := \{e_1, \dots, e_n\}$ и $\{e^1, \dots, e^n\}$ имеет матрицу, равную матрице Грама G базиса e. В самом деле,

$$\alpha(e_i)(e_j) = (e_j, e_i) = g_{ji} = g_{ki}\delta^k_j = (g_{ki} e^k)(e_j),$$

то есть $\alpha(e_i) = g_{ki} e^k$.

Пусть H — матрица билинейной функции ψ в базисе $\{e^1, \dots, e^n\}$, то есть $h^{ij} = \psi(e^i, e^j)$. Тогда если x, y — координатные столбцы векторов v и w в базисе e, то (133) перепишется в виде $(Gx)^T H G y = x^T G y$, откуда $H = G^{-1}$. ■

Тензор $\{\varphi^{i_1 \dots i_p}_{j_1 \dots j_q}\}$ называется *инвариантным*, если он имеет одинаковые координаты во всех тензорных базисах в $\mathbf{T}^p_q(V)$. Если V — евклидово пространство, то $\{\varphi^{i_1 \dots i_p}_{j_1 \dots j_q}\}$ называется *изотропным*, если он инвариантен относительно ортогональных преобразований V (т.е. имеет одинаковые координаты во всех тензорных базисах, получающихся друг из друга с помощью ортогональных преобразований V). Ясно, что всякий инвариантный тензор изотропен, но, вообще говоря, не наоборот.

Рангом тензора $\varphi \in \mathbf{T}^p_q(V)$ называют число $p + q$.

Задача 15.21. *a) Найти все инвариантные тензоры ранга* 2;

b) Найти все изотропные тензоры типа (0, 2).

Решение. a) Во-первых, заметим, что если ненулевой тензор $\varphi \in \mathbf{T}^p_q(V)$ инвариантен, то $p = q$. Действительно, рассмотрим замену базиса $e'_i = \lambda\, e_i$, $1 \leq i \leq n := \dim V$. Тогда из формулы замены координат тензора $\varphi'^{i_1 \dots i_p}_{j_1 \dots j_q} = \lambda^{q-p}\, \varphi^{i_1 \dots i_p}_{j_1 \dots j_q}$.

Таким образом, достаточно рассмотреть тензоры типа (1, 1). Ранее такие тензоры мы отождествили с линейными операторами на V, причем тогда координаты тензора типа (1, 1) в тензорном базисе $\{e^i \otimes e_j\}$ в $\mathbf{T}^1_1(V)$ — то же самое, что матричные элементы матрицы этого оператора в базисе $\{e_1, \dots, e_n\}$

пространства V. Таким образом, инвариантные тензоры типа (1, 1) отвечают линейным операторам, которые имеют одинаковые матрицы во всех базисах, то есть матрицы A, такие что $CA = AC$ для любой обратимой матрицы C. Легко видеть, что тогда $A = \lambda E$, то есть инвариантные тензоры типа (1, 1) — операторы $\lambda \operatorname{Id}_V$, кратные тождественному. Таким образом, инвариантный тензор φ типа (1, 1) имеет координаты $\varphi_i^j = \lambda\, \delta_i^j$.

b) Выше мы видели, что пространство тензоров типа (0, 2) отождествляется с пространством билинейных функций, при этом координаты такого тензора в тензорном базисе $\{e^i \otimes e^j\}$ в $\mathbf{T}_2^0(V)$ — то же, что матричные элементы матрицы соответствующей билинейной функции в базисе $\{e_1, \dots, e_n\}$ пространства V. Таким образом, нужно найти билинейные функции, имеющие одну и ту же матрицу во всех базисах, получаемых друг из друга ортогональной заменой.

Поскольку V — евклидово пространство, на нем уже задан тензор типа (0, 2) — положительно определенная симметричная билинейная функция g, задающая скалярное произведение. Пусть $\{e_1, \dots, e_n\}$ — ортонормированный базис в V. Рассмотрим ортогональную замену базиса $e_i' = -e_i,\ e_j' = e_j$ при $j \neq i$. Тогда при $i \neq j$ получаем $\varphi_{ij}' = -\varphi_{ij}$, то есть изотропный тензор в этом базисе должен иметь координаты $\{\lambda_i\, \delta_{ij}\}$. Далее, при ортогональной замене $e_i' = e_j,\ e_j' = e_i,\ e_k' = e_k$ при $k \neq i, j$ имеем $\varphi_{ii}' = \varphi_{jj},\ \varphi_{jj}' = \varphi_{ii}$. Таким образом, изотропный тензор $\{\varphi_{ij}\}$ имеет вид $\{\lambda\, \delta_{ij}\}$. То есть матрица соответствующей билинейной функции в ортонормированном базисе есть λE, и билинейная функция пропорциональна евклидовой структуре на V. ■

15.5 Свертка

Свертка тензора типа (p, q), где $p, q \geq 1$, по фиксированной паре индексов (один из которых верхний, а другой — нижний) — некоторое специальное линейное отображение $\mathbf{T}_q^p(V) \to \mathbf{T}_{q-1}^{p-1}(V)$.

Определим сначала частный случай свертки — для тензоров типа (1, 1). В этом случае свертка единственна (так как имеется только один верхний и один нижний индекс) и представляет собой линейное отображение $\mathbf{T}_1^1(V) \to \mathbb{K}$ (то есть линейный функционал на пространстве $\mathbf{T}_1^1(V)$), определяемый следующим образом. Выберем произвольный базис $\{e_1, \dots, e_n\}$ в V и для $\varphi\colon V \times V^* \to \mathbb{K},\ \ \varphi \in \mathbf{T}_1^1(V)$ рассмотрим отображение $\varphi \mapsto \widetilde{\varphi}$, где $\widetilde{\varphi} := \sum_i \varphi(e_i,\, e^i) = \sum_i \varphi_i^i$.

Покажем, что свертка корректно определена, то есть не зависит от выбора базиса $\{e_1, \dots, e_n\}$. Пусть $\{e_1', \dots, e_n'\}$ — другой базис в V и C — матрица перехода к нему от старого ("нештрихованного") базиса. Имеем

$$\sum_{k=1}^n \varphi(e_k',\, e'^k) = \sum_{k=1}^n \varphi_k'^k = \sum_{i,\,j,\,k} c_k^j d_i^k \varphi_j^i = \sum_{i,\,j} \left(\sum_{k=1}^n c_k^j d_i^k \right) \varphi_j^i = \sum_{i,\,j} \delta_i^j \varphi_j^i = \sum_j \varphi_j^j = \sum_{j=1}^n \varphi(e_j,\, e^j),$$

что и требовалось доказать. Легко видеть, что при отождествлении тензоров типа (1, 1) с линейными операторами свертка отождествляется со следом. В частности, только что доказанная корректность определения свертки равносильна инвариантности следа матрицы линейного оператора (его независимости от выбора базиса).

Задача 15.22. *На разложимых тензорах $\alpha \otimes v$ свертка совпадает с отображением $\alpha \otimes v \mapsto \alpha(v)$.*

Решение. Если $\alpha = 0$, то все очевидно. Иначе пусть $\operatorname{Ker} \alpha = \{v \in V \mid \alpha(v) = 0\} \subset V$. Выберем базис $\{e_1, \dots, e_n\}$ в V такой, что $\{e_2, \dots, e_n\}$ — базис в $\operatorname{Ker} \alpha$. Тогда

$$\widetilde{\varphi} = \sum_{k=1}^n \alpha(e_k) e^k(v) = \alpha(e_1) v^1 = \alpha(v),$$

где $v = \sum_i v^i e_i$. Так как свертка и значение $\alpha(v)$ не зависят от выбора базиса, то все доказано. ■

В общем случае свертка $\mathrm{tr}_s^r\varphi$ тензора φ типа $(p,\,q)$, где $p,\,q\geq 1$, по паре индексов $r,\,s$ $(1\leq r\leq p,\ 1\leq s\leq q)$ определяется как линейное отображение $\mathbf{T}_q^p(V)\to\mathbf{T}_{q-1}^{p-1}(V)$, заданное формулой

$$\varphi\mapsto \mathrm{tr}_s^r\varphi=\sum_{k=1}^n\varphi(\ldots,e_k,\ldots,e^k,\ldots),$$

где e_k принадлежит s-му сомножителю V, а e^k — r-му сомножителю V^*. Таким образом, $\mathrm{tr}_s^r\varphi$ является полилинейной функцией от $q-1$ векторных и $p-1$ ковекторных аргументов (обозначенных выше многоточием), то есть тензором типа $(p-1,\,q-1)$ на V.

Аналогично предыдущему проверяется независимость определения свертки от выбора базиса $\{e_1,\ldots,e_n\}$. В частности, в любом базисе верно равенство

$$(\mathrm{tr}_s^r\varphi)(e_{j_1},\ldots,e_{j_{q-1}};e^{i_1},\ldots,e^{i_{p-1}})=(\mathrm{tr}_s^r\varphi)_{j_1\ldots j_{q-1}}^{i_1\ldots i_{p-1}}=\sum_{k=1}^n\varphi_{j_1\ldots j_{s-1}kj_s\ldots j_{q-1}}^{i_1\ldots i_{r-1}ki_r\ldots i_{p-1}}.$$

Если после произведенной свертки у тензора остался хотя бы один верхний и хотя бы один нижний индекс, то можно выбрать пару таких индексов и произвести свертку по ним. Если после произведенных сверток остались либо только верхние, либо только нижние индексы (либо не осталось ни тех, ни других), то такая свертка называется *полной*. В частности, если тензор имел тип $(p,\,p)$, то сворачивая его по всем верхним и нижним индексам, получим скаляр. (Сколько различных полных сверток есть у тензора типа $(p,\,p)$?)

Многие операции линейной алгебры могут быть описаны как композиции тензорного произведения и свертки. Рассмотрим соответствующие примеры.

Пример 15.23. Пусть φ — тензор типа $(1,\,1)$ (линейный оператор) с компонентами φ_j^i относительно некоторого базиса, а v — тензор типа $(1,\,0)$ (вектор) с компонентами v^i в том же базисе. Тогда их тензорное произведение $\varphi\otimes v$ является тензором типа $(2,\,1)$ с компонентами $(\varphi\otimes v)_j^{ik}=\varphi_j^iv^k$ (см. (132)). Сворачивая его по нижнему индексу φ и единственному индексу v, получим тензор $\mathrm{tr}_1^2(\varphi\otimes v)$ типа $(1,\,0)$ с компонентами $(\mathrm{tr}_1^2(\varphi\otimes v))^i=\sum_j\varphi_j^iv^j$. Так как $\varphi(v)^i=\sum_j\varphi_j^iv^j$, то легко видеть, что этот вектор — результат применения оператора к вектору, то есть $\mathrm{tr}_1^2(\varphi\otimes v)=\varphi(v)$.

Пример 15.24. Пусть φ и ψ — тензоры типа $(1,\,1)$. Тогда $\varphi\otimes\psi$ — тензор типа $(2,\,2)$ с компонентами $(\varphi\otimes\psi)_{kl}^{ij}=\varphi_k^i\psi_l^j$. Читателю предлагается проверить, что $\mathrm{tr}_1^2(\varphi\otimes\psi)=\varphi\circ\psi$, в то время как $\mathrm{tr}_2^1(\varphi\otimes\psi)=\psi\circ\varphi$ (композиции линейных операторов). Далее, имеем две полные свертки $\mathrm{tr}_1^1(\mathrm{tr}_1^2(\varphi\otimes\psi))=\mathrm{tr}(\varphi\circ\psi)$ и $\mathrm{tr}_1^1(\mathrm{tr}_2^1(\varphi\otimes\psi))=\mathrm{tr}(\psi\circ\varphi)$ (следы линейных операторов).

Пример 15.25. Пусть $\alpha\in\mathbf{T}_2^0(V)$, то есть $\alpha\colon V\times V\to\mathbb{K}$ — билинейная форма на V. Пусть $u,\,v\in V$. Тогда $\alpha\otimes u\otimes v\in\mathbf{T}_2^2(V)$. Имеем две полные свертки: $\mathrm{tr}_1^1(\mathrm{tr}_1^1(\alpha\otimes u\otimes v))=\alpha(u,\,v)=\sum_{i,\,j}\alpha_{ij}u^iv^j$ и $\mathrm{tr}_1^1(\mathrm{tr}_1^2(\alpha\otimes u\otimes v))=\alpha(v,\,u)=\sum_{i,\,j}\alpha_{ij}u^jv^i$. Они совпадают тогда и только тогда, когда билинейная форма α симметрична.

Задача 15.26. [12] *Найти полную свертку тензора* $\varphi\in\mathbf{T}_2^2(V)$ *из Задачи 15.14 при условии* $\dim V=n$.

Решение. Так как у тензора два верхних и два нижних индекса, имеются две полные свертки: $\mathrm{tr}_1^1(\mathrm{tr}_1^1(\varphi))=\sum_{i,\,j}\varphi_{ij}^{ij}$ и $\mathrm{tr}_1^1(\mathrm{tr}_2^1(\varphi))=\sum_{i,\,j}\varphi_{ji}^{ij}$. Согласно Задаче 15.14, $\varphi_{kl}^{ij}=\delta_k^i\delta_l^j-\delta_l^i\delta_k^j$. Таким образом,

$$\varphi_{ij}^{ij}=\delta_i^i\delta_j^j-\delta_j^i\delta_i^j=\begin{cases}1, & \text{если } i\neq j;\\ 0, & \text{если } i=j.\end{cases}$$

Откуда $\mathrm{tr}_1^1(\mathrm{tr}_1^1(\varphi))=\sum_{i,\,j}t_{ij}^{ij}=n^2-n$.

Аналогично,

$$\varphi_{ji}^{ij}=\delta_j^i\delta_i^j-\delta_i^i\delta_j^j=\begin{cases}-1, & \text{если } i\neq j;\\ 0, & \text{если } i=j.\end{cases}$$

Таким образом, $\mathrm{tr}_1^1(\mathrm{tr}_2^1(\varphi)) = \sum_{i,\,j} \varphi_{ji}^{ij} = n - n^2$. ■

Операция свертки особенно полезна в случае евклидовых пространств, где она приводит к операциям опускания и подъема индекса. С ними мы познакомимся в одном из следующих параграфов.

15.6 Симметричные и кососимметричные тензоры

Пространство $\mathbf{T}_q^0(V)$ тензоров типа $(0,\,q)$ (то есть q-линейных форм) на V обозначим просто $\mathbf{T}_q(V)$.

Пусть S_q — группа перестановок на q элементах. Для всякой перестановки $\sigma \in S_q$ и q-линейной формы $\varphi\colon V \times \ldots \times V \to \mathbb{K}$ определим новую q-линейную форму $f_\sigma(\varphi)$

$$f_\sigma(\varphi)(v_1, \ldots, v_q) = \varphi(v_{\sigma(1)}, \ldots, v_{\sigma(q)}) \quad \forall\, v_1, \ldots, v_q \in V.$$

Вообще, легко видеть, что $\forall\, \sigma \in S_q$ f_σ является линейным оператором на $\mathbf{T}_q(V)$.

Определение 15.27. Тензор $\varphi \in \mathbf{T}_q(V)$ называется *симметричным*, если $f_\sigma(\varphi) = \varphi \quad \forall\, \sigma \in S_q$. Тензор $\varphi \in \mathbf{T}_q(V)$ называется *кососимметричным*, если $f_\sigma(\varphi) = \varepsilon(\sigma)\varphi \quad \forall\, \sigma \in S_q$, где $\varepsilon(\sigma) \in \{\pm 1\}$ — знак перестановки σ (обозначаемый иногда $\operatorname{sgn}\sigma$).

Легко проверяется, что симметричные (кососимметричные) тензоры в $\mathbf{T}_q(V)$ образуют подпространство. Обозначим его $\mathbf{T}_q^+(V)$ (соответственно $\mathbf{T}_q^-(V)$).

Читатель знакóм с понятиями симметричных и кососимметричных билинейных форм; примером трилинейной кососимметричной формы является смешанное произведение на трехмерном ориентированном евклидовом пространстве. Вообще, ориентированный объем в n-мерном ориентированном евклидовом пространстве является кососимметричной n-линейной формой.

Получим условие симметричности (кососимметричности) тензора в координатах. Пусть

$$\varphi = \sum \varphi_{i_1 \ldots i_q} e^{i_1} \otimes \ldots \otimes e^{i_q}, \quad \text{где} \quad \varphi_{i_1 \ldots i_q} = \varphi(e_{i_1}, \ldots, e_{i_q}).$$

Тогда

$$f_\sigma(\varphi)_{i_1 \ldots i_q} = f_\sigma(\varphi)(e_{i_1}, \ldots, e_{i_q}) = \varphi(e_{\sigma(i_1)}, \ldots, e_{\sigma(i_q)}) = \varphi_{\sigma(i_1) \ldots \sigma(i_q)}$$

и, значит,

$$f_\sigma(\varphi) = \sum \varphi_{\sigma(i_1) \ldots \sigma(i_q)} e^{i_1} \otimes \ldots \otimes e^{i_q}. \tag{134}$$

Тогда из единственности разложения по базису мы получаем следующее условие симметричности (кососимметричности) в координатах:

$$\varphi_{\sigma(i_1) \ldots \sigma(i_q)} = \varphi_{i_1 \ldots i_q} \quad \forall\, \sigma \in S_q$$

(соответственно

$$\varphi_{\sigma(i_1) \ldots \sigma(i_q)} = \varepsilon(\sigma)\varphi_{i_1 \ldots i_q} \quad \forall\, \sigma \in S_q).$$

Очевидно, что выполнение этих условий не зависит от выбора базиса.

Заметим, что из (134) получается следующая формула для действия перестановок на тензорном базисе:

$$f_\sigma(e^{i_1} \otimes \ldots \otimes e^{i_q}) = e^{\sigma^{-1}(i_1)} \otimes \ldots \otimes e^{\sigma^{-1}(i_q)}. \tag{135}$$

Пусть основное поле $\mathbb{K}$ имеет характеристику 0 (этому условию удовлетворяют поля, содержащие $\mathbb{Q}$ в качестве подполя, в частности, $\mathbb{R}$ и $\mathbb{C}$). В этом случае мы построим проекторы на подпространства $\mathbf{T}_q^+(V)$ и $\mathbf{T}_q^-(V)$, обобщающие проекторы $B \mapsto \frac{B+B^T}{2}$, $B \mapsto \frac{B-B^T}{2}$ на подпространства симметричных и кососимметричных билинейных форм при $q = 2$[70]. При проверке их свойств нам понадобится следующая

[70]Заметим, что $\mathbf{T}_2(V) = \mathbf{T}_2^+(V) \oplus \mathbf{T}_2^-(V)$, но при $q \neq 2$ это неверно, в чем проще всего убедиться, сравнивая размерности данных пространств (см. ниже).

Лемма 15.28. Пусть σ, $\tau \in S_q$ — две перестановки. Тогда $\forall \varphi \in \mathbf{T}_q(V)$

$$f_\tau(f_\sigma(\varphi)) = f_{\tau\sigma}(\varphi),$$

где $\tau\sigma$ — произведение (композиция) перестановок[71].

Доказательство. Действительно,

$$f_\tau(f_\sigma(\varphi))(v_1, \dots, v_q) = f_\sigma(\varphi)(v_{\tau(1)}, \dots, v_{\tau(q)}) = f_\sigma(\varphi)(w_1, \dots, w_q) =$$

$$= \varphi(w_{\sigma(1)}, \dots, w_{\sigma(q)}) = \varphi(v_{\tau\sigma(1)}, \dots, v_{\tau\sigma(q)}) = f_{\tau\sigma}(\varphi)(v_1, \dots, v_q)$$

(здесь для удобства мы сделали замену $w_i = v_{\tau(i)}$, тогда $w_{\sigma(j)} = v_{\tau\sigma(j)}$). ■

Определение 15.29. *Оператором симметрирования* на $\mathbf{T}_q(V)$ называется линейный оператор $\mathbf{S} = \mathbf{S}(q)\colon \mathbf{T}_q(V) \to \mathbf{T}_q(V)$, определяемый формулой

$$\mathbf{S}\varphi = \frac{1}{q!} \sum_{\sigma \in S_q} f_\sigma(\varphi), \quad \varphi \in \mathbf{T}_q(V)$$

(сумма по всем перестановкам $\sigma \in S_q$).

То, что $\mathbf{S}$ является линейным оператором, легко проверяется. Возможность деления на $q!$ обеспечивается условием на характеристику основного поля.

Приведем координатную запись симметрирования (которую легко получить из предыдущего):

$$(\mathbf{S}\varphi)_{i_1 \dots i_q} = \frac{1}{q!} \sum_{\sigma \in S_q} \varphi_{\sigma(i_1) \dots \sigma(i_q)}.$$

В литературе часто вместо $(\mathbf{S}\varphi)_{i_1 \dots i_q}$ пишут $\varphi_{(i_1 \dots i_q)}$ (“результат симметрирования по индексам $i_1 \dots i_q$”).

Теорема 15.30. *Оператор симметрирования* $\mathbf{S}\colon \mathbf{T}_q(V) \to \mathbf{T}_q(V)$ *имеет следующие свойства:*

1) $\operatorname{Im} \mathbf{S} = \mathbf{T}_q^+(V)$;
2) $\mathbf{S}^2 = \mathbf{S}$.

Таким образом, $\mathbf{S}$ *— проектор на подпространство* $\mathbf{T}_q^+(V) \subset \mathbf{T}_q(V)$.

Доказательство. Во-первых, $\operatorname{Im} \mathbf{S} \subset \mathbf{T}_q^+(V)$. Действительно, используя Лемму 15.28 и тот факт, что при фиксированном $\tau \in S_q$ когда σ пробегает все S_q по одному разу, то $\tau\sigma$ также пробегает все S_q по одному разу[72], имеем

$$f_\tau(\mathbf{S}\varphi) = f_\tau\left(\frac{1}{q!} \sum_{\sigma \in S_q} f_\sigma(\varphi)\right) = \frac{1}{q!} \sum_{\sigma \in S_q} f_\tau(f_\sigma(\varphi)) = \frac{1}{q!} \sum_{\sigma \in S_q} f_{\tau\sigma}(\varphi) = \frac{1}{q!} \sum_{\omega \in S_q} f_\omega(\varphi) = \mathbf{S}\varphi. \tag{136}$$

Обратное включение $\operatorname{Im} \mathbf{S} \supset \mathbf{T}_q^+(V)$ следует из того, что $\forall\, \varphi \in \mathbf{T}_q^+(V)$ $\mathbf{S}\varphi = \varphi$.

Из равенства (136) следует $\sum_{\tau \in S_q} f_\tau(\mathbf{S}\varphi) = q!\, \mathbf{S}\varphi$, откуда $\mathbf{S}^2\varphi = \mathbf{S}\varphi$. ■

Пусть $\varphi \in \mathbf{T}_q^-(V)$, тогда имеем

$$\mathbf{S}\varphi = \frac{1}{q!} \sum_{\sigma \in S_q} f_\sigma(\varphi) = \frac{1}{q!} \sum_{\sigma \in S_q} \varepsilon(\sigma)\varphi = 0.$$

[71] Таким образом, $\sigma \mapsto f_\sigma$ — линейное представление группы S_q в пространстве $\mathbf{T}_q(V)$.

[72] В силу однозначной разрешимости в группе уравнения $\tau\sigma = \omega$.

Вывод: $\mathbf{T}_q^-(V) \subset \operatorname{Ker} \mathbf{S}$.

Симметрический тензор $\mathbf{S}(e^{i_1} \otimes \ldots \otimes e^{i_q})$ обозначим $e^{i_1} \ldots e^{i_q}$. Формальное произведение $e^{i_1} \ldots e^{i_q}$ не меняется при перестановке индексов, и можно условиться выбирать в качестве единственной записи таких симметричных тензоров запись $(e^1)^{a_1} \ldots (e^n)^{a_n}$, где $a_i \geq 0,\ a_1 + \ldots + a_n = q$; здесь число a_i показывает, сколько раз ковектор e^i фигурирует в $e^{i_1} \otimes \ldots \otimes e^{i_q}$.

Предложение 15.31. *Тензоры $(e^1)^{a_1} \ldots (e^n)^{a_n} \in \mathbf{T}_q^+(V),\ a_i \geq 0,\ a_1 + \ldots + a_n = q$, образуют базис в пространстве $\mathbf{T}_q^+(V)$, которое, таким образом, можно отождествить с пространством однородных многочленов степени q от координатных функций на пространстве V.*

Доказательство. Так как тензоры вида $e^{i_1} \otimes \ldots \otimes e^{i_q}$ образуют базис в $\mathbf{T}_q(V)$, то из $\operatorname{Im} \mathbf{S} = \mathbf{T}_q^+(V)$ следует, что их симметризации $\mathbf{S}(e^{i_1} \otimes \ldots \otimes e^{i_q})$ порождают $\mathbf{T}_q^+(V)$. Поэтому достаточно доказать, что тензоры $(e^1)^{a_1} \ldots (e^n)^{a_n}$, отвечающие разным наборам $(a_1, \ldots, a_n),\ a_i \geq 0,\ a_1 + \ldots + a_n = q$, линейно независимы в $\mathbf{T}_q(V)$.

Если

$$\sum \lambda_{a_1 \ldots a_n} (e^1)^{a_1} \ldots (e^n)^{a_n} = 0,$$

то

$$\mathbf{S}\left(\sum \lambda_{a_1 \ldots a_n} \underbrace{e^1 \otimes \ldots \otimes e^1}_{a_1} \otimes \ldots \otimes \underbrace{e^n \otimes \ldots \otimes e^n}_{a_n} \right) = 0.$$

Приводя подобные слагаемые в левой части, убеждаемся, что слева стоит линейная комбинация элементов тензорного базиса пространства $\mathbf{T}_q(V)$ с коэффициентами $\lambda_{a_1 \ldots a_n}$, умноженными на ненулевые числа[73], откуда все $\lambda_{a_1 \ldots a_n}$ равны нулю. ■

Проиллюстрируем предыдущее доказательство примером для $q = 3$, $n = 2$. Тогда

$$(e^1)^3,\ (e^1)^2 e^2,\ e^1 (e^2)^2,\ (e^2)^3$$

образуют базис в $\mathbf{T}_q^+(V)$. В самом деле, пусть

$$\lambda_{30}(e^1)^3 + \lambda_{21}(e^1)^2 e^2 + \lambda_{12} e^1 (e^2)^2 + \lambda_{03}(e^2)^3 = 0.$$

Левая часть предыдущего равенства равна (см. формулу (135))

$$\mathbf{S}(\lambda_{30} e^1 \otimes e^1 \otimes e^1 + \lambda_{21} e^1 \otimes e^1 \otimes e^2 + \lambda_{12} e^1 \otimes e^2 \otimes e^2 + \lambda_{03} e^2 \otimes e^2 \otimes e^2) =$$

$$= \lambda_{30} e^1 \otimes e^1 \otimes e^1 + \frac{\lambda_{21}}{3}(e^1 \otimes e^1 \otimes e^2 + e^1 \otimes e^2 \otimes e^1 + e^2 \otimes e^1 \otimes e^1) +$$

$$+ \frac{\lambda_{12}}{3}(e^1 \otimes e^2 \otimes e^2 + e^2 \otimes e^1 \otimes e^2 + e^2 \otimes e^2 \otimes e^1) + \lambda_{03} e^2 \otimes e^2 \otimes e^2.$$

Если последнее выражение равно нулю, в силу линейной независимости тензорного базиса получаем, что $\lambda_{30} = \lambda_{21} = \lambda_{12} = \lambda_{03} = 0$.

Следствие 15.32. $\dim \mathbf{T}_q^+(V) = \binom{n+q-1}{q}$.

Рассмотрим теперь аналогичные конструкции для кососимметрических тензоров.

[73] например, тензор $\underbrace{e_1 \otimes \ldots \otimes e_1}_{a_1} \otimes \ldots \otimes \underbrace{e_n \otimes \ldots \otimes e_n}_{a_n}$ (и другие тензоры, получаемые из него перестановками) входит с коэффициентом $\frac{a_1! \ldots a_n!}{q!}$.

Определение 15.33. *Оператором альтернирования* на $\mathbf{T}_q(V)$ называется линейный оператор $\mathbf{A} = \mathbf{A}(q)\colon \mathbf{T}_q(V) \to \mathbf{T}_q(V)$, определяемый формулой

$$\mathbf{A}\varphi = \frac{1}{q!}\sum_{\sigma\in S_q} \varepsilon(\sigma) f_\sigma(\varphi), \quad \varphi \in \mathbf{T}_q(V)$$

(сумма по всем перестановкам $\sigma \in S_q$).

Приведем координатную запись альтернирования (которую легко получить из предыдущего):

$$(\mathbf{A}\varphi)_{i_1\dots i_q} = \frac{1}{q!}\sum_{\sigma\in S_q} \varepsilon(\sigma)\, \varphi_{\sigma(i_1)\dots\sigma(i_q)}.$$

В литературе часто вместо $(\mathbf{A}\varphi)_{i_1\dots i_q}$ пишут $\varphi_{[i_1\dots i_q]}$ (“результат альтернирования по индексам $i_1 \dots i_q$”).

Теорема 15.34. *Оператор альтернирования* $\mathbf{A}\colon \mathbf{T}_q(V) \to \mathbf{T}_q(V)$ *имеет следующие свойства:*

1) $\operatorname{Im}\mathbf{A} = \mathbf{T}_q^-(V)$;

2) $\mathbf{A}^2 = \mathbf{A}$.

Таким образом, $\mathbf{A}$ *— проектор на подпространство* $\mathbf{T}_q^-(V) \subset \mathbf{T}_q(V)$.

Доказательство. Во-первых, $\operatorname{Im}\mathbf{A} \subset \mathbf{T}_q^-(V)$. Действительно, используя Лемму 15.28, тождество $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ и тот факт, что при фиксированном $\tau \in S_q$ когда σ пробегает все S_q по одному разу, то $\tau\sigma$ также пробегает все S_q по одному разу, имеем

$$f_\tau(\mathbf{A}\varphi) = f_\tau\left(\frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma) f_\sigma(\varphi)\right) = \frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma) f_\tau(f_\sigma(\varphi)) =$$

$$= \varepsilon(\tau)\left(\frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\tau\sigma) f_{\tau\sigma}(\varphi)\right) = \varepsilon(\tau)\left(\frac{1}{q!}\sum_{\omega\in S_q}\varepsilon(\omega) f_\omega(\varphi)\right) = \varepsilon(\tau)\mathbf{A}\varphi. \tag{137}$$

Обратное включение $\operatorname{Im}\mathbf{A} \supset \mathbf{T}_q^-(V)$ следует из того, что $\forall\, \varphi \in \mathbf{T}_q^-(V)$ $\mathbf{A}\varphi = \varphi$. В самом деле,

$$\mathbf{A}\varphi = \frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma) f_\sigma(\varphi) = \frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma)^2\varphi = \varphi.$$

Из равенства (137) следует $\sum_{\tau\in S_q}\varepsilon(\tau) f_\tau(\mathbf{A}\varphi) = q!\,\mathbf{A}\varphi$, откуда $\mathbf{A}^2\varphi = \mathbf{A}\varphi$. ■

Пусть $\varphi \in \mathbf{T}_q^+(V)$, тогда имеем

$$\mathbf{A}\varphi = \frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma) f_\sigma(\varphi) = \frac{1}{q!}\sum_{\sigma\in S_q}\varepsilon(\sigma)\varphi = 0.$$

Вывод: $\mathbf{T}_q^+(V) \subset \operatorname{Ker}\mathbf{A}$.

Разложимые тензоры $e^{i_1}\otimes\dots\otimes e^{i_q}$, $1 \le i_1, \dots, i_q \le n$ образуют базис пространства $\mathbf{T}_q(V)$, а значит их антисимметризации $\mathbf{A}(e^{i_1}\otimes\dots\otimes e^{i_q})$ порождают пространство $\mathbf{T}_q^-(V)$. Заметим, что в отличие от симметрического случая выражение $\mathbf{A}(e^{i_1}\otimes\dots\otimes e^{i_q})$ меняет знак при перестановке любых двух ковекторов e^i. Отсюда следуют два вывода:

1) $\mathbf{A}(e^{i_1}\otimes\dots\otimes e^{i_q}) = 0$, если $i_k = i_l$ для некоторых $1 \le k, l \le q$, $k \ne l$;

2) пространство $\mathbf{T}_q^-(V)$ порождено тензорами вида $\mathbf{A}(e^{i_1}\otimes\dots\otimes e^{i_q})$, где $1 \le i_1 < i_2 < \dots < i_q \le n$.

Из этого, в частности, сразу же следует, что $\mathbf{T}_q^-(V) = 0$ при $q > n = \dim V$.

Предложение 15.35. *Тензоры* $\mathbf{A}(e^{i_1}\otimes\ldots\otimes e^{i_q})\in\mathbf{T}_q^-(V)$ *при* $q\le n$, $1\le i_1<i_2<\ldots<i_q\le n$ *образуют базис пространства* $\mathbf{T}_q^-(V)$.

Доказательство. В силу сказанного выше, достаточно проверить, что эти тензоры линейно независимы в $\mathbf{T}_q(V)$.

Если

$$\sum\lambda_{i_1\ldots i_q}\mathbf{A}(e^{i_1}\otimes\ldots\otimes e^{i_q})=0,$$

то

$$\mathbf{A}\left(\sum\lambda_{i_1\ldots i_q}e^{i_1}\otimes\ldots\otimes e^{i_q}\right)=0.$$

Но так как индексы $i_1,\ldots,i_q$ расположены в порядке строгого возрастания (в частности, среди них нет двух одинаковых), в результате их перестановок мы получим в сумме слева линейную комбинацию различных элементов тензорного базиса $\mathbf{T}_q(V)$ с коэффициентами вида $\pm\frac{1}{q!}\lambda_{i_1\ldots i_q}$. Эта сумма может быть равна нулю, только если все $\lambda_{i_1\ldots i_q}$ нулевые. ■

Следствие 15.36. $\dim\mathbf{T}_q^-(V)=\binom{n}{q}$.

Заметим, что из последнего Следствия и Следствия 15.32 получаем, в частности, что $\dim\mathbf{T}_3^+(V)+\dim\mathbf{T}_3^-(V)=\frac{n(n^2+2)}{3}<n^3=\dim\mathbf{T}_3(V)$ при $n>1$. Т.е. пространство $\mathbf{T}_3(V)$ не является суммой $\mathbf{T}_3^+(V)$ и $\mathbf{T}_3^-(V)$.

15.7 Симметрическая алгебра

Симметрирование позволяет определить симметрическое произведение симметричных тензоров, результат которого также является симметричным тензором.

Определение 15.37. Пусть $\varphi\in\mathbf{T}_q^+(V)$, $\psi\in\mathbf{T}_r^+(V)$. Тогда их *симметрическим произведением* $\varphi\vee\psi$ называется тензор $\mathbf{S}(\varphi\otimes\psi)\in\mathbf{T}_{q+r}^+(V)$ (здесь $\mathbf{S}=\mathbf{S}(q+r)\colon\mathbf{T}_{q+r}(V)\to\mathbf{T}_{q+r}(V)$).

Предложение 15.38. *Если* $\varphi\in\mathbf{T}_q^+(V)$, $\psi\in\mathbf{T}_r^+(V)$, *то*

$$(\varphi\vee\psi)(v_1,\ldots,v_{q+r})=\frac{q!\,r!}{(q+r)!}\sum\varphi(v_{i_1},\ldots,v_{i_q})\psi(v_{j_1},\ldots,v_{j_r}),$$

где суммирование справа происходит по всем перестановкам $\sigma=(i_1,\ldots,i_q,j_1,\ldots,j_r)$ *множества* $1,2,\ldots,q+r$ *таким, что* $i_1<\ldots<i_q$, $j_1<\ldots<j_r$.

Доказательство. Имеем

$$(\varphi\vee\psi)(v_1,\ldots,v_{q+r})=\frac{1}{(q+r)!}\sum_{\sigma\in S_{q+r}}f_\sigma(\varphi\otimes\psi)(v_1,\ldots,v_{q+r})=$$

$$=\frac{1}{(q+r)!}\sum_{\sigma\in S_{q+r}}\varphi(v_{\sigma(1)},\ldots,v_{\sigma(q)})\psi(v_{\sigma(q+1)},\ldots,v_{\sigma(q+r)}).$$

Каждое слагаемое $\varphi(v_{\sigma(1)},\ldots,v_{\sigma(q)})\psi(v_{\sigma(q+1)},\ldots,v_{\sigma(q+r)})$ отвечает некоторому разбиению множества индексов $\{1,2,\ldots,q+r\}$ на два подмножества $\{\sigma(1),\ldots,\sigma(q)\}$ и $\{\sigma(q+1),\ldots,\sigma(q+r)\}$, и при перестановке индексов внутри указанных подмножеств выражение $\varphi(v_{\sigma(1)},\ldots,v_{\sigma(q)})\psi(v_{\sigma(q+1)},\ldots,v_{\sigma(q+r)})$ не меняется из-за симметричности φ и ψ. Каждому разбиению отвечает $q!r!$ слагаемых и перестановки $\sigma=(i_1,\ldots,i_q,j_1,\ldots,j_r)$ множества $1,2,\ldots,q+r$ с условием что $i_1<\ldots<i_q$, $j_1<\ldots<j_r$ однозначно соответствуют разбиениям. ■

Изучим свойства операции $\vee\colon \mathbf{T}_q^+(V) \times \mathbf{T}_r^+(V) \to \mathbf{T}_{q+r}^+(V)$. Во-первых, она билинейна:

$$(\varphi_1 + \varphi_2) \vee \psi = \varphi_1 \vee \psi + \varphi_2 \vee \psi, \;\; (\lambda\varphi) \vee \psi = \lambda(\varphi \vee \psi),$$

и аналогично относительно второго аргумента. Это следует из билинейности операции $\otimes$ и линейности оператора $\mathbf{S}$.

Для доказательства ассоциативности операции $\vee$ нам понадобится следующая Лемма.

Лемма 15.39. Для любых $\varphi \in \mathbf{T}_q(V),\ \psi \in \mathbf{T}_r(V)$ выполнены равенства

$$\mathbf{S}(\varphi \otimes \psi) = \mathbf{S}((\mathbf{S}\varphi) \otimes \psi) = \mathbf{S}(\varphi \otimes (\mathbf{S}\psi)).$$

Доказательство. Определим инъективный гомоморфизм групп $\alpha\colon S_q \to S_{q+r}$, вкладывающий S_q в качестве подгруппы, оставляющей на месте последние r элементов множества $1, 2, \ldots, q+r$. Для произвольного $\tau \in S_q$ тогда имеем

$$\mathbf{S}(f_\tau(\varphi) \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} f_\sigma(f_\tau(\varphi) \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} f_\sigma(f_{\alpha(\tau)}(\varphi \otimes \psi)) =$$

$$= \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} f_{\sigma\alpha(\tau)}(\varphi \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} f_\sigma(\varphi \otimes \psi) = \mathbf{S}(\varphi \otimes \psi),$$

откуда

$$\mathbf{S}\left((\mathbf{S}\varphi) \otimes \psi\right) = \mathbf{S}\left(\left(\frac{1}{q!} \sum_{\tau \in S_q} f_\tau(\varphi)\right) \otimes \psi\right) =$$

$$= \frac{1}{q!} \sum_{\tau \in S_q} \mathbf{S}(f_\tau(\varphi) \otimes \psi) = \frac{1}{q!} q!\, \mathbf{S}(\varphi \otimes \psi) = \mathbf{S}(\varphi \otimes \psi).$$

Второе равенство доказывается аналогично. ■

Предложение 15.40. *Для произвольных $\varphi \in \mathbf{T}_q^+(V),\ \psi \in \mathbf{T}_r^+(V),\ \chi \in \mathbf{T}_s^+(V)$ выполнено тождество $(\varphi \vee \psi) \vee \chi = \varphi \vee (\psi \vee \chi)$. Другими словами, операция $\vee$ ассоциативна.*

Доказательство. С учетом предыдущей Леммы и ассоциативности операции $\otimes$ имеем

$$(\varphi \vee \psi) \vee \chi = \mathbf{S}(\mathbf{S}(\varphi \otimes \psi) \otimes \chi) = \mathbf{S}((\varphi \otimes \psi) \otimes \chi) =$$

$$= \mathbf{S}(\varphi \otimes (\psi \otimes \chi)) = \mathbf{S}(\varphi \otimes \mathbf{S}(\psi \otimes \chi)) = \varphi \vee (\psi \vee \chi). \quad \blacksquare$$

Наконец докажем, что операция $\vee$ коммутативна.

Предложение 15.41. *Для любых $\varphi \in \mathbf{T}_q^+(V),\ \psi \in \mathbf{T}_r^+(V)$ выполнено равенство $\varphi \vee \psi = \psi \vee \varphi$.*

Доказательство. Зададим перестановку $\kappa \in S_{q+r}$,

$$\kappa = \begin{pmatrix} 1 & 2 & \ldots & q & q+1 & q+2 & \ldots & q+r \\ r+1 & r+2 & \ldots & r+q & 1 & 2 & \ldots & r \end{pmatrix}.$$

Тогда имеем

$$f_\kappa(\varphi \otimes \psi)(v_1, \ldots, v_q, v_{q+1}, \ldots, v_{q+r}) = (\varphi \otimes \psi)(v_{\kappa(1)}, \ldots, v_{\kappa(q)}, v_{\kappa(q+1)}, \ldots, v_{\kappa(q+r)}) =$$

$$= (\varphi \otimes \psi)(v_{r+1}, \ldots, v_{r+q}, v_1, \ldots, v_r) = \varphi(v_{r+1}, \ldots, v_{r+q})\psi(v_1, \ldots, v_r) =$$

$$= (\psi \otimes \varphi)(v_1, \ldots, v_r, v_{r+1}, \ldots, v_{r+q}).$$

Таким образом,

$$f_\kappa(\varphi \otimes \psi) = \psi \otimes \varphi. \tag{138}$$

С учетом этого получаем

$$\varphi \vee \psi = \mathbf{S}(\varphi \otimes \psi) = \mathbf{S}(f_\kappa(\varphi \otimes \psi)) = \mathbf{S}(\psi \otimes \varphi) = \psi \vee \varphi. \quad \blacksquare$$

Таким образом, мы имеем набор линейных пространств $\{\mathbf{T}^+_q(V) \mid q \geq 0\}$ заданных вместе с билинейными отображениями $\vee\colon \mathbf{T}^+_q(V) \times \mathbf{T}^+_r(V) \to \mathbf{T}^+_{q+r}(V)$. С помощью следующей конструкции из них можно построить единый объект, который будет ассоциативной коммутативной алгеброй.

Пусть $\mathbf{S}(V^*) := \oplus_{q=0}^{\infty} \mathbf{T}^+_q(V)$. Напомним, что $\mathbf{T}^+_0(V) = \mathbb{K}$, $\mathbf{T}^+_1(V) = V^*$. Элементами $\mathbf{S}(V^*)$ являются конечные суммы $\varphi_0 + \varphi_1 + \varphi_2 + \ldots$, $\varphi_q \in \mathbf{T}^+_q(V)$. Используя симметрическое произведение, элементы $\mathbf{S}(V^*)$ можно перемножать:

$$(\varphi_0 + \varphi_1 + \varphi_2 + \ldots) \vee (\psi_0 + \psi_1 + \psi_2 + \ldots) = \chi_0 + \chi_1 + \chi_2 + \ldots, \quad \text{где } \chi_m = \sum_{q+r=m} \varphi_q \vee \psi_r.$$

Тем самым мы получаем ассоциативную коммутативную алгебру с единицей $1 \in \mathbb{K} = \mathbf{T}^+_0(V) \subset \mathbf{S}(V^*)$.

Определение 15.42. Алгебра $\mathbf{S}(V^*)$ называется *симметрической алгеброй пространства* V^*.

Заметим, что

$$\mathbf{S}(e^{i_1} \otimes e^{i_2} \otimes \ldots \otimes e^{i_q}) = \mathbf{S}(e^{i_1} \otimes \mathbf{S}(e^{i_2} \otimes \ldots \otimes e^{i_q})) =$$
$$= e^{i_1} \vee \mathbf{S}(e^{i_2} \otimes \ldots \otimes e^{i_q}) = \ldots = e^{i_1} \vee e^{i_2} \vee \ldots \vee e^{i_q}.$$

Упростим обозначения: обозначим $e^{i_1} \vee e^{i_2} \vee \ldots \vee e^{i_q}$ просто $e^{i_1} e^{i_2} \ldots e^{i_q}$ (ср. абзац перед Предложением 15.31).

Согласно Предложению 15.31 элементы $(e^1)^{a_1}(e^2)^{a_2} \ldots (e^n)^{a_n}$ для всевозможных наборов $(a_1, a_2, \ldots, a_n)$, $a_i \geq 0$ (включая набор $(0, 0, \ldots, 0)$, который отвечает 1), образуют базис в $\mathbf{S}(V^*)$.

Теорема 15.43. *Симметрическая алгебра $\mathbf{S}(V^*)$ изоморфна алгебре многочленов $\mathbb{K}[x_1, x_2, \ldots, x_n]$, где $n = \dim V$. (Более точно, сопоставление $e^i \mapsto x_i$, $1 \leq i \leq n$ продолжается до изоморфизма $\mathbf{S}(V^*) \cong \mathbb{K}[x_1, x_2, \ldots, x_n]$).*

Доказательство следует из правила умножения базисных элементов (см. параграф 5.2): очевидно, что

$$((e^1)^{a_1}(e^2)^{a_2} \ldots (e^n)^{a_n})((e^1)^{b_1}(e^2)^{b_2} \ldots (e^n)^{b_n}) = (e^1)^{a_1+b_1}(e^2)^{a_2+b_2} \ldots (e^n)^{a_n+b_n}. \quad \blacksquare$$

Если рассматривать $e^1, \ldots, e^n$ как координатные (линейные) функции на V, то алгебру $\mathbf{S}(V^*)$ можно интерпретировать как алгебру многочленов на V.

Замечание 15.44. Аналогичную конструкцию можно применить также к пространствам всех тензоров $\mathbf{T}_q(V)$ типа $(0, q)$, $q \geq 0$, так как на них тоже есть билинейная ассоциативная операция $\mathbf{T}_q(V) \times \mathbf{T}_r(V) \to \mathbf{T}_{q+r}(V)$, задаваемая тензорным произведением $\otimes$. Это приводит к тензорной алгебре $\mathbf{T}(V) := \oplus_{q=0}^{\infty} \mathbf{T}_q(V)$ пространства V^*. В отличие от симметрической алгебры, тензорная алгебра некоммутативна. Не следует думать, что симметрическая алгебра (так же как и обсуждаемая ниже внешняя алгебра) является подалгеброй в тензорной: на самом деле, это ее факторалгебра. Что это такое, читатель может узнать из более подробных учебников линейной алгебры, например [17].

15.8 Внешняя алгебра

Получим теперь аналогичные результаты для кососимметрических тензоров.

Определение 15.45. Пусть $\varphi \in \mathbf{T}_q^-(V)$, $\psi \in \mathbf{T}_r^-(V)$. Тогда их *внешним произведением* $\varphi \wedge \psi$ называется тензор $\frac{(q+r)!}{q!\,r!}\mathbf{A}(\varphi \otimes \psi) \in \mathbf{T}_{q+r}^-(V)$ (здесь $\mathbf{A} = \mathbf{A}(q+r)\colon \mathbf{T}_{q+r}(V) \to \mathbf{T}_{q+r}(V)$).

Замечание 15.46. В некоторых книгах множитель $\frac{(q+r)!}{q!\,r!}$ не рассматривают, то есть определяют внешнее произведение просто как $\mathbf{A}(\varphi\otimes\psi) \in \mathbf{T}_{q+r}^-(V)$, аналогично тому, как мы определяли симметрическое произведение. Мы остановились на определении с указанным множителем, принятым в книгах, использующих аппарат дифференциальных форм: дело в том, что при этом часто получаются более простые формулы, например в формуле (141) нет факториалов, как и в формуле из Предложения ниже. Заметим, что такие свойства внешнего произведения, как билинейность, ассоциативность, косокоммутативность при двух возможных определениях совпадают. Таким образом, оба определения дают изоморфные внешние алгебры (см. ниже).

Предложение 15.47. *Если* $\varphi \in \mathbf{T}_q^-(V)$, $\psi \in \mathbf{T}_r^-(V)$, *то*

$$(\varphi \wedge \psi)(v_1, \dots, v_{q+r}) = \sum \varepsilon(\sigma)\varphi(v_{i_1}, \dots, v_{i_q})\psi(v_{j_1}, \dots, v_{j_r}),$$

где суммирование справа происходит по всем перестановкам $\sigma = (i_1, \dots, i_q, j_1, \dots, j_r)$ *множества* $1, 2, \dots, q+r$ *таким, что* $i_1 < \dots < i_q$, $j_1 < \dots < j_r$.

Доказательство. Имеем

$$(\varphi \wedge \psi)(v_1, \dots, v_{q+r}) = \frac{(q+r)!}{q!\,r!}\frac{1}{(q+r)!}\sum_{\sigma\in S_{q+r}} \varepsilon(\sigma) f_\sigma(\varphi \otimes \psi)(v_1, \dots, v_{q+r}) =$$

$$= \frac{1}{q!\,r!}\sum_{\sigma\in S_{q+r}} \varepsilon(\sigma)\varphi(v_{\sigma(1)}, \dots, v_{\sigma(q)})\psi(v_{\sigma(q+1)}, \dots, v_{\sigma(q+r)}). \tag{139}$$

Каждое слагаемое $\varepsilon(\sigma)\varphi(v_{\sigma(1)}, \dots, v_{\sigma(q)})\psi(v_{\sigma(q+1)}, \dots, v_{\sigma(q+r)})$ отвечает некоторому разбиению множества индексов $\{1, 2, \dots, q+r\}$ на два подмножества $\{\sigma(1), \dots, \sigma(q)\}$ и $\{\sigma(q+1), \dots, \sigma(q+r)\}$. Заметим, что для любой перестановки $\sigma \in S_{q+r}$ существует такая единственная перестановка $\sigma' \in S_{q+r}$, что

$$\{\sigma(1), \dots, \sigma(q)\} = \{\sigma'(1), \dots, \sigma'(q)\},\ \ \{\sigma(q+1), \dots, \sigma(q+r)\} = \{\sigma'(q+1), \dots, \sigma'(q+r)\}$$

и

$$\sigma'(1) < \sigma'(2) < \dots < \sigma'(q),\ \ \sigma'(q+1) < \dots < \sigma'(q+r).$$

Перестановка σ' может быть получена из перестановки σ конечной последовательностью транспозиций внутри подмножеств $\{\sigma(1), \dots, \sigma(q)\}$ и $\{\sigma(q+1), \dots, \sigma(q+r)\}$, при этом выражение $\varepsilon(\sigma)\varphi(v_{\sigma(1)}, \dots, v_{\sigma(q)})\psi(v_{\sigma(q+1)}, \dots, v_{\sigma(q+r)})$ не меняется из-за кососимметричности φ и ψ. Таким образом, для каждого набора из $q!\,r!$ слагаемых в (139), отвечающих одному разбиению $\{1, 2, \dots, q+r\} = \{\sigma(1), \dots, \sigma(q)\}\bigcup\{\sigma(q+1), \dots, \sigma(q+r)\}$, их сумма в (139) равна $\varepsilon(\sigma')\varphi(v_{\sigma'(1)}, \dots, v_{\sigma'(q)})\psi(v_{\sigma'(q+1)}, \dots, v_{\sigma'(q+r)})$. ■

Заметим, что мы уже встречались с внешним произведением линейных функций в параграфе 10.7. Или например, для тензора φ из Задачи 15.14 $\varphi(u, v, \alpha, \beta) = (\alpha \wedge \beta)(u, v)$ – значение внешнего произведения $\alpha \wedge \beta$ линейных форм α, β на паре векторов u, v.

Изучим теперь свойства операции $\wedge\colon \mathbf{T}_q^-(V) \times \mathbf{T}_r^-(V) \to \mathbf{T}_{q+r}^-(V)$. Во-первых, она билинейна:

$$(\varphi_1 + \varphi_2) \wedge \psi = \varphi_1 \wedge \psi + \varphi_2 \wedge \psi,\ \ (\lambda\varphi) \wedge \psi = \lambda(\varphi \wedge \psi),$$

и аналогично относительно второго аргумента. Это следует из билинейности операции $\otimes$ и линейности оператора $\mathbf{A}$.

Для доказательства ассоциативности операции $\wedge$ нам понадобится следующая Лемма.

Лемма 15.48. Для любых $\varphi \in \mathbf{T}_q(V),\ \psi \in \mathbf{T}_r(V)$ выполнены равенства

$$\mathbf{A}(\varphi \otimes \psi) = \mathbf{A}((\mathbf{A}\varphi) \otimes \psi) = \mathbf{A}(\varphi \otimes (\mathbf{A}\psi)).$$

Доказательство. Определим инъективный гомоморфизм групп $\alpha\colon S_q \to S_{q+r}$, вкладывающий S_q в качестве подгруппы, оставляющей на месте последние r элементов множества $1, 2, \ldots, q+r$. Заметим, что $\varepsilon(\alpha(\tau)) = \varepsilon(\tau)\ \forall\, \tau \in S_q$. Для произвольного $\tau \in S_q$ тогда имеем

$$\mathbf{A}(\varepsilon(\tau) f_\tau(\varphi) \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma)\varepsilon(\tau) f_\sigma(f_\tau(\varphi) \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma\alpha(\tau)) f_\sigma(f_{\alpha(\tau)}(\varphi \otimes \psi)) =$$

$$= \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma\alpha(\tau)) f_{\sigma\alpha(\tau)}(\varphi \otimes \psi) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma) f_\sigma(\varphi \otimes \psi) = \mathbf{A}(\varphi \otimes \psi),$$

откуда

$$\mathbf{A}((\mathbf{A}\varphi) \otimes \psi) = \mathbf{A}\left(\left(\frac{1}{q!} \sum_{\tau \in S_q} \varepsilon(\tau) f_\tau(\varphi)\right) \otimes \psi\right) =$$

$$= \frac{1}{q!} \sum_{\tau \in S_q} \mathbf{A}(\varepsilon(\tau)(f_\tau\varphi) \otimes \psi) = \frac{1}{q!} q!\, \mathbf{A}(\varphi \otimes \psi) = \mathbf{A}(\varphi \otimes \psi).$$

Второе равенство доказывается аналогично. ■

Предложение 15.49. *Для произвольных $\varphi \in \mathbf{T}_q^-(V),\ \psi \in \mathbf{T}_r^-(V),\ \chi \in \mathbf{T}_s^-(V)$ выполнено тождество $(\varphi \wedge \psi) \wedge \chi = \varphi \wedge (\psi \wedge \chi)$. Другими словами, операция $\wedge$ ассоциативна.*

Доказательство. С учетом предыдущей Леммы и ассоциативности операции $\otimes$ имеем

$$(\varphi \wedge \psi) \wedge \chi = \frac{(q+r+s)!}{(q+r)!s!} \frac{(q+r)!}{q!r!} \mathbf{A}(\mathbf{A}(\varphi \otimes \psi) \otimes \chi) = \frac{(q+r+s)!}{q!r!s!} \mathbf{A}((\varphi \otimes \psi) \otimes \chi) =$$

$$= \frac{(q+r+s)!}{q!r!s!} \mathbf{A}(\varphi \otimes (\psi \otimes \chi)) = \frac{(q+r+s)!}{q!(r+s)!} \frac{(r+s)!}{r!s!} \mathbf{A}(\varphi \otimes \mathbf{A}(\psi \otimes \chi)) = \varphi \wedge (\psi \wedge \chi). \quad ■$$

Наконец докажем, что операция $\wedge$ косокоммутативна.

Предложение 15.50. $\forall \varphi \in \mathbf{T}_q^-(V),\ \psi \in \mathbf{T}_r^-(V)$ *выполнено равенство* $\psi \wedge \varphi = (-1)^{qr} \varphi \wedge \psi$.

Доказательство. Снова рассмотрим перестановку $\kappa \in S_{q+r}$,

$$\kappa = \begin{pmatrix} 1 & 2 & \ldots & q & q+1 & q+2 & \ldots & q+r \\ r+1 & r+2 & \ldots & r+q & 1 & 2 & \ldots & r \end{pmatrix}.$$

Подсчет числа инверсий показывает, что ее знак $\varepsilon(\kappa)$ как раз равен $(-1)^{qr}$. Выше мы уже доказали (см. (138)), что $f_\kappa(\varphi \otimes \psi) = \psi \otimes \varphi$. С учетом этого получаем

$$\mathbf{A}(\psi \otimes \varphi) = \mathbf{A}(f_\kappa(\varphi \otimes \psi)) = \frac{1}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma) f_\sigma(f_\kappa(\varphi \otimes \psi)) =$$

$$= \frac{\varepsilon(\kappa)}{(q+r)!} \sum_{\sigma \in S_{q+r}} \varepsilon(\sigma\kappa) f_{\sigma\kappa}(\varphi \otimes \psi) = \varepsilon(\kappa) \mathbf{A}(\varphi \otimes \psi). \quad ■$$

Пусть $\bigwedge(V^*) := \oplus_{q=0}^{\infty} \mathbf{T}_q^-(V)$. Напомним, что $\mathbf{T}_0^-(V) = \mathbb{K},\ \ \mathbf{T}_1^-(V) = V^*$, $\mathbf{T}_q^-(V) = 0$ при $q > n = \dim V$. Элементами $\bigwedge(V^*)$ являются суммы $\varphi_0 + \varphi_1 + \varphi_2 + \ldots + \varphi_n,\ \ \varphi_q \in \mathbf{T}_q^-(V)$. Используя внешнее произведение, элементы $\bigwedge(V^*)$ можно перемножать:

$$(\varphi_0 + \varphi_1 + \varphi_2 + \ldots) \wedge (\psi_0 + \psi_1 + \psi_2 + \ldots) = \chi_0 + \chi_1 + \chi_2 + \ldots, \quad \text{где } \chi_m = \sum_{q+r=m} \varphi_q \wedge \psi_r.$$

Тем самым мы получаем ассоциативную косокоммутативную алгебру с единицей $1 \in \mathbb{K} = \mathbf{T}_0^-(V) \subset \bigwedge(V^*)$.

Определение 15.51. Алгебра $\bigwedge(V^*)$ называется *внешней алгеброй пространства* V^*.

Данную алгебру иногда называют также *алгеброй Грассмана*.

Замечание 15.52. В алгебре $\bigwedge(V^*)$ можно рассмотреть два подпространства $\bigwedge(V^*)^0 := \oplus_{p=0}^{\infty}\mathbf{T}^-_{2p}(V)$ и $\bigwedge(V^*)^1 := \oplus_{p=0}^{\infty}\mathbf{T}^-_{2p+1}(V)$; ясно, что $\bigwedge(V^*) = \bigwedge(V^*)^0 \oplus \bigwedge(V^*)^1$ (прямая сумма подпространств), при этом

$$\bigwedge(V^*)^0 \bigwedge(V^*)^0 \subset \bigwedge(V^*)^0, \quad \bigwedge(V^*)^0 \bigwedge(V^*)^1 \subset \bigwedge(V^*)^1,$$

$$\bigwedge(V^*)^1 \bigwedge(V^*)^0 \subset \bigwedge(V^*)^1, \quad \bigwedge(V^*)^1 \bigwedge(V^*)^1 \subset \bigwedge(V^*)^0.$$

Приведенные равенства означают, что $\bigwedge(V^*)$ является примером *супералгебры* (определение и другие примеры см. например в [19]). В частности, $\bigwedge(V^*)^0$ является коммутативной подалгеброй в $\bigwedge(V^*)$.

В отличие от симметрической алгебры, внешняя алгебра конечномерного пространства конечномерна. Более точно, $\dim \bigwedge(V^*) = 2^n$, где $n = \dim V$ (см. Следствие 15.36)

Заметим, что

$$\mathbf{A}(e^{i_1} \otimes e^{i_2} \otimes \ldots \otimes e^{i_q}) = \mathbf{A}(e^{i_1} \otimes \mathbf{A}(e^{i_2} \otimes \ldots \otimes e^{i_q})) =$$
$$= \frac{1}{q}\, e^{i_1} \wedge \mathbf{A}(e^{i_2} \otimes \ldots \otimes e^{i_q}) = \ldots = \frac{1}{q!} e^{i_1} \wedge e^{i_2} \wedge \ldots \wedge e^{i_q}. \tag{140}$$

Из Предложения 15.35 мы знаем, что внешние произведения базисных ковекторов $e^{i_1} \wedge e^{i_2} \wedge \ldots \wedge e^{i_q}$ при фиксированном q, $0 \le q \le n$,[74] $1 \le i_1 < i_2 < \ldots < i_q \le n$, образуют базис пространства $\mathbf{T}^-_q(V)$, а значит указанные выражения при $0 \le q \le n$ образуют базис алгебры $\bigwedge(V^*)$.

Пример 15.53. Пусть $\dim V = 3$. Тогда в $\bigwedge(V^*)$ имеется базис

$$\{1,\, e^1, e^2, e^3,\, e^2 \wedge e^3, e^3 \wedge e^1, e^1 \wedge e^2,\, e^1 \wedge e^2 \wedge e^3\}.$$

Правила умножения базисных векторов по билинейности задают умножение во всей алгебре $\bigwedge(V^*)$. Например,

$$(e^1 + e^2 \wedge e^3) \wedge (e^1 + e^2) = e^1 \wedge e^2 \wedge e^3 + e^1 \wedge e^2.$$

Пример 15.54. Не следует думать, что кососоммутативность влечет равенство нулю любого произведения вида $\varphi \wedge \varphi$ для $\varphi \in \bigwedge(V^*)$. Например, это не так для $1 \in \bigwedge(V^*)$. Вот еще пример для V, $\dim V \ge 4$:

$$(e^1 \wedge e^2 + e^3 \wedge e^4) \wedge (e^1 \wedge e^2 + e^3 \wedge e^4) = 2e^1 \wedge e^2 \wedge e^3 \wedge e^4.$$

Следующий пример демонстрирует связь внешнего произведения с определителями.

Пример 15.55. Пусть $\varphi_1, \ldots, \varphi_q \colon V \to \mathbb{K}$ — набор линейных форм. Тогда из (140) следует, что их внешнее произведение $\varphi_1 \wedge \ldots \wedge \varphi_q \in \mathbf{T}^-_q(V)$ задается формулой

$$\varphi_1 \wedge \ldots \wedge \varphi_q(v_1, \ldots, v_q) = \sum_{\sigma \in S_q} \varepsilon(\sigma) \varphi_1(v_{\sigma(1)}) \ldots \varphi_q(v_{\sigma(q)}).$$

Заметим, что это — определитель матрицы $A = (a_{ij})$, где $a_{ij} = \varphi_i(v_j)$.[75] Например, кососимметричность определителя по строкам отвечает кососимметричности операции $\wedge$, а кососимметричность по столбцам — тому, что внешнее произведение линейных функций — кососимметричная полилинейная функция.

В частности, если $\{e_1, \ldots, e_n\}$ — некоторый базис в V, то

$$e^1 \wedge \ldots \wedge e^n(v_1, \ldots, v_n) = \sum_{(i_1 \ldots i_n) \in S_n} \operatorname{sgn}(i_1 \ldots i_n) v^1_{i_1} \ldots v^n_{i_n} = \det(v^i_j) \tag{141}$$

[74] На всякий случай заметим, что пустое произведение при $q = 0$ по определению равно 1.

[75] Последняя формула еще раз иллюстрирует роль множителя $\frac{(q+r)!}{q!\,r!}$ в Определении 15.45: без него в последней формуле появился бы множитель $\frac{1}{q!}$.

— определитель матрицы, составленной из координат векторов $v_1, \dots, v_n$ в базисе $\{e_1, \dots, e_n\}$. Если пространство V евклидово, а базис $\{e_1, \dots, e_n\}$ — правый ортонормированный[76], то это равно ориентированному n-мерному объему параллелепипеда, построенного на векторах $v_1, \dots, v_n$. Если $\{e'_1, \dots, e'_n\}$ — еще один базис, то поскольку $\dim \bigwedge^n V = 1$, то $e^1 \wedge \dots \wedge e^n$ и $e'^1 \wedge \dots \wedge e'^n$ различаются ненулевым множителем. Читатель легко проверит, что этот множитель — определитель матрицы перехода. Используя этот факт, нетрудно получить новое доказательство того, что определитель произведения матриц равен произведению определителей.

15.9 Тензоры в евклидовом пространстве

Евклидово пространство — это пара (V, g), состоящая из вещественного векторного пространства V и билинейной симметричной положительно определенной формы g на нем. То есть g является симметричным тензором типа $(0, 2)$. Наличие фиксированной невырожденной билинейной формы g приводит к ряду отображений между тензорами разных типов в евклидовом пространстве, которые отсутствуют в векторном пространстве без дополнительной структуры. Эти отображения возникают из сверток с g. В этом разделе нам будет удобнее вести изложение на классическом, координатном, языке.

Итак, рассмотрим примеры канонических изоморфизмов между пространствами тензоров разных типов в случае евклидова пространства. Один из них — изоморфизм α_V между евклидовым пространством V и его двойственным — мы рассмотрели в параграфе 11.3. Напомним, что он задается сопоставлением $v \mapsto g(\cdot, v) =: f(\cdot)$ вектору v линейной формы f, полученной из билинейной формы g подстановкой v в качестве второго аргумента. Приведем его описание на тензорном языке. Пусть $\{e_1, \dots, e_n\}$ — некоторый базис в V. Тогда изоморфизм между пространством $T^1_0(V) \cong V$ и $T^0_1(V) = V^*$ задается как композиция тензорного умножения вектора на g и сверткой полученного тензора по единственному верхнему и одному из нижних индексов (какому конкретно — неважно, ибо тензор g симметричен). То есть указанный изоморфизм — композиция

$$v^k \mapsto (g \otimes v)^k_{ij} = g_{ij} v^k \mapsto \sum_j g_{ij} v^j =: f_i.$$

По понятным причинам данная операция называется операцией опускания индекса.

Пусть g^{ij} — элементы обратной матрицы к матрице Грама формы g в данном базисе, $\sum_j g^{ij} g_{jk} = \delta^i_k$. Из Задачи 15.20 мы знаем, что они являются координатами некоторого тензора $\widehat{g}$ типа $(2, 0)$. Этот тензор позволяет задать обратный изоморфизм $V^* \to V$:

$$f_k \mapsto (\widehat{g} \otimes f)^{ij}_k = g^{ij} f_k \mapsto \sum_j g^{ij} f_j =: v^i.$$

Это — пример операции подъема индекса в евклидовом пространстве.

Далее, в параграфе 12.4 в евклидовом пространстве мы по линейному оператору строили билинейную форму (причем для самосопряженного оператора эта форма оказывалась симметричной). Эта операция — еще один пример операции опускания индекса:

$$a^k_l \mapsto (g \otimes a)^k_{ijl} = g_{ij} a^k_l \mapsto \sum_j g_{ij} a^j_l =: h_{il},$$

то есть для матриц $H = GA$, где $A = (a^i_j)$ — матрица оператора в данном базисе. Иначе, эта операция выглядит как сопоставление линейному оператору φ на V билинейной формы $(u, v) \mapsto g(u, \varphi(v))$.

Замечание 15.56. Заметим, что если базис ортонормированный, то есть $g_{ij} = \delta_{ij}$, то $A = H$. Кроме того, при ортогональных заменах базисов матрицы операторов и билинейных форм преобразуются одинаково. Вообще, если в евклидовом пространстве ограничиться только ортонормированными базисами, то разница между верхними и нижними индексами тензоров исчезает.

[76] Или просто такой, что ориентированный объем его фундаментального параллелепипеда равен 1.

В Примере 15.19 мы определили тензор структурных констант алгебры. В базисе он определяется из тождества $e_i \cdot e_j = \sum_k \varphi_{ij}^k e_k$. Пусть V — трехмерное ориентированное евклидово пространство. Рассмотрим его как алгебру относительно операции векторного произведения. Так как

$$\left[\sum_i v^i e_i, \sum_j w^j e_j\right] = \sum_{i,j,k} \varphi_{ij}^k v^i w^j e_k,$$

то

$$[v, w]^k = \sum_{i,j} \varphi_{ij}^k v^i w^j.$$

Если у φ опустить его единственный верхний индекс, то получится тензор, отвечающий смешанному произведению. Действительно,

$$\sum_{i,j,k,l} g_{il} \varphi_{jk}^l u^i v^j w^k = (u, [v, w]) = (u, v, w).$$

Обратно, задание трилинейной формы $V \times V \times V \to \mathbb{R}$ эквивалентно заданию билинейного отображения $V \times V \to V^*$, которое после взятия композиции с операцией подъема индекса $V^* \to V$ определяет билинейное умножение $V \times V \to V$. Применение этой конструкции к смешанному произведению дает векторное произведение.

Пусть ψ — тензор, задающий смешанное произведение (в координатах $\psi_{ijk} := \sum_l g_{il} \varphi_{jk}^l$). В правом ортонормированном базисе $\{e_1, e_2, e_3\}$ его координаты суть

$$\psi_{ijk} = (e_i, e_j, e_k) = \varepsilon_{ijk} := \begin{cases} 1, & \text{если перестановка } (ijk) \text{ четная;} \\ -1, & \text{если перестановка } (ijk) \text{ нечетная;} \\ 0, & \text{если среди индексов } ijk \text{ есть совпадающие.} \end{cases}$$

Трехмерный массив ε_{ijk} называется *символом Леви-Чивиты*. В обозначениях предыдущего параграфа $\psi = e^1 \wedge e^2 \wedge e^3$.

Посчитаем координаты ψ в новом базисе $\{e'_1, e'_2, e'_3\}$, связанным с исходным $\{e_1, e_2, e_3\}$ матрицей перехода $C = (c_j^i)$. Имеем

$$\psi'_{lmn} = \sum_{i,j,k} \varepsilon_{ijk} c_l^i c_m^j c_n^k = \begin{cases} \det C, & \text{если перестановка } (lmn) \text{ четная;} \\ -\det C, & \text{если перестановка } (lmn) \text{ нечетная;} \\ 0, & \text{если среди индексов } lmn \text{ есть совпадающие.} \end{cases}$$

То есть $\psi'_{ijk} = (\det C)\, \varepsilon_{ijk}$. Недостаток данной записи в том, что матрица перехода зависит не только от нового, но и от старого базиса. Однако заметим, что если исходный базис был ортонормированным, то матрица Грама G' нового базиса есть $C^T C$, то есть $|\det C| = \sqrt{\det G'}$. Знак же $\det C$ определяется так: если исходный базис был правым, то он "+", если новый базис также является правым и "−" в противном случае. В итоге мы получаем равенство $\psi'_{ijk} = \mathrm{or}(e')\sqrt{\det G'}\varepsilon_{ijk}$, где $\mathrm{or}(e')$ — число, определяемое базисом e' и равное 1, если он правый и -1 в противном случае.

Мы получили, что сопоставление произвольному базису e трехмерного ориентированного евклидова пространства набора $\mathrm{or}(e)\sqrt{\det G(e)}\varepsilon_{ijk}$ $(i, j, k \in \{1, 2, 3\})$ определяет тензор типа $(0, 3)$, значение которого на упорядоченной тройке векторов из V равно ориентированному объему параллелепипеда, построенного на этой тройке. Данный тензор называется *формой объема*. Это — элемент одномерного пространства $\mathbf{T}_3^-(V)$. Его определение очевидным образом обобщается с трехмерного пространства на случай ориентированного евклидова пространства произвольной размерности n.

Задача 15.57. *В случае четырехмерного ориентированного евклидова пространства V определить и изучить аналог векторного произведения, являющийся трилинейным умножением $V \times V \times V \to V$.*

Замечание 15.58. В связи с предыдущей задачей для любопытного читателя отметим, что если определить *векторное произведение* в n-мерном евклидовом пространстве V как такое билинейное отображение $V \times V \to V$, $(u,\, v) \mapsto u \times v$, что

- $(u,\, u \times v) = 0 = (u \times v,\, v)$ для любых $u,\, v \in V$;
- $|u \times v|^2 = |u|^2|v|^2 - (u,\, v)^2$,

то можно доказать, что ненулевое векторное произведение помимо 3-мерного существует только в 7-мерном евклидовом пространстве V [21].

В заключение докажем некоторые тождества с символом Леви-Чивиты, полезные в приложениях.

Задача 15.59. *Доказать формулы:*

1) $\varepsilon_{ijk}\varepsilon_{rst} = \begin{vmatrix} \delta_{ir} & \delta_{is} & \delta_{it} \\ \delta_{jr} & \delta_{js} & \delta_{jt} \\ \delta_{kr} & \delta_{ks} & \delta_{kt} \end{vmatrix}$;

2) $\sum_k \varepsilon_{ijk}\varepsilon_{rsk} = \delta_{ir}\delta_{js} - \delta_{is}\delta_{jr}$;

3) $\sum_{k,j} \varepsilon_{ijk}\varepsilon_{rjk} = 2\delta_{ir}$;

4) $\sum_{k,j,i} \varepsilon_{ijk}\varepsilon_{ijk} = 6$.

Решение. 1) Докажем, что для любых векторов u, v, w, x, y, z трехмерного ориентированного евклидова пространства V выполнено тождество

$$(u, v, w)(x, y, z) = \begin{vmatrix} (u,x) & (u,y) & (u,z) \\ (v,x) & (v,y) & (v,z) \\ (w,x) & (w,y) & (w,z) \end{vmatrix}. \tag{142}$$

Для этого заметим, что слева и справа стоят полилинейные функции $V^{\times 6} \to \mathbb{R}$, кососимметричные по $1, 2, 3$ и $4, 5$ и 6 аргументам. Из полилинейности следует, что это тождество достаточно проверить на наборах векторов, когда u, v, w, x, y, z пробегают элементы некоторого ортонормированного базиса $\{e_1, e_2, e_3\}$ в V, а из кососимметричности — что его достаточно проверить на наборе $u = x = e_1,\ v = y = e_2,\ w = z = e_3$, после чего в его справедливости легко убедиться. Подставляя теперь в (142) $u = e_i, v = e_j, w = e_k, x = e_r, y = e_s, z = e_t$, получаем 1).

Вот другой способ доказательства тождества 1). Имеем

$$\begin{vmatrix} g_{ir} & g_{is} & g_{it} \\ g_{jr} & g_{js} & g_{jt} \\ g_{kr} & g_{ks} & g_{kt} \end{vmatrix} = \varepsilon_{ijk} \begin{vmatrix} g_{1r} & g_{1s} & g_{1t} \\ g_{2r} & g_{2s} & g_{2t} \\ g_{3r} & g_{3s} & g_{3t} \end{vmatrix} = \varepsilon_{ijk}\varepsilon_{rst} \begin{vmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{vmatrix} = \varepsilon_{ijk}\varepsilon_{rst} \det G.$$

Осталось заметить, что это — просто инвариантная (верная не только в ортонормированных базисах) форма записи 1).

Докажем пункт 2). Для упрощения записи будем опускать знак суммы по k. Имеем

$$\varepsilon_{ijk}\varepsilon_{rsk} = \begin{vmatrix} \delta_{ir} & \delta_{is} & \delta_{ik} \\ \delta_{jr} & \delta_{js} & \delta_{jk} \\ \delta_{kr} & \delta_{ks} & \delta_{kk} \end{vmatrix} = \delta_{kr} \begin{vmatrix} \delta_{is} & \delta_{ik} \\ \delta_{js} & \delta_{jk} \end{vmatrix} - \delta_{ks} \begin{vmatrix} \delta_{ir} & \delta_{ik} \\ \delta_{jr} & \delta_{jk} \end{vmatrix} + \delta_{kk} \begin{vmatrix} \delta_{ir} & \delta_{is} \\ \delta_{jr} & \delta_{js} \end{vmatrix} =$$

$$= \begin{vmatrix} \delta_{is} & \delta_{ir} \\ \delta_{js} & \delta_{jr} \end{vmatrix} - \begin{vmatrix} \delta_{ir} & \delta_{is} \\ \delta_{jr} & \delta_{js} \end{vmatrix} + 3 \begin{vmatrix} \delta_{ir} & \delta_{is} \\ \delta_{jr} & \delta_{js} \end{vmatrix} = \begin{vmatrix} \delta_{ir} & \delta_{is} \\ \delta_{jr} & \delta_{js} \end{vmatrix}$$

Используя 2), докажем 3):

$$\sum_j (\delta_{ir}\delta_{jj} - \delta_{ij}\delta_{jr}) = 3\delta_{ir} - \delta_{ir} = 2\delta_{ir}.$$

Пункт 4) очевиден. ■

Замечание 15.60. Заметим, что тождество 2) из предыдущей задачи эквивалентно следующему тождеству векторной алгебры:

$$([u,v],[x,y]) = \begin{vmatrix} (u,x) & (u,y) \\ (v,x) & (v,y) \end{vmatrix},$$

из которого вытекает известная формула "бац минус цаб":

$$([u,v],[x,y]) = (x,y,[u,v]) = (x,[y,[u,v]]) = ((v,y)u - (u,y)v, x).$$

Замечание 15.61. Легко видеть, что в левых частях тождеств 1) — 4) из предыдущей задачи стоят изотропные тензоры рангов $6, 4, 2$ и 0, причем суммирование отвечает свертке (ср. Замечание 15.56). Это, например, позволяет решить пункт 3) почти без вычислений, если воспользоваться описанием изотропных тензоров, данным в Задаче 15.21. Действительно, из нее мы знаем, что любой изотропный тензор типа $(0,2)$ имеет вид $\lambda\,\delta_{ir}$, остается только определить константу λ. Для этого заметим, что пункт 4) очевиден непосредственно: $\sum_{i,j,k=1}^{3} \varepsilon_{ijk}^2 = 3! = 6$, тогда сворачивая $\lambda\,\delta_{ir}$ по i и r, получаем $3\lambda = 6$, откуда $\lambda = 2$.

15.10 Оператор Ходжа

В этом разделе рассмотрим одну важную операцию, которая определяется на внешней алгебре ориентированного евклидова (а также псевдоевклидова) линейного пространства. Эта операция переносится на алгебру дифференциальных форм на (псевдо)римановом многообразии и имеет важные применения в геометрии и физике.

Далее нам будет полезно еще одно понятие из линейной алгебры.

Определение 15.62. Пусть U, W — конечномерные линейные пространства над полем $\mathbb{K}$. *Спариванием* пространств U и W называется билинейное отображение

$$\alpha\colon U \times W \to \mathbb{K}.$$

Спаривание α называется *невырожденным*, если $\forall\, u \neq 0\ \exists\, w \in W$ такой, что $\alpha(u,\, w) \neq 0$ и $\forall\, w \neq 0\ \exists\, u \in U$ такой, что $\alpha(u,\, w) \neq 0$.

Мы уже знакомы с примером невырожденного спаривания $V \times V^* \to \mathbb{K}$, $\quad (v,\, f) \mapsto f(v)$.

По спариванию α определяются линейные отображения $\beta\colon U \to W^*$, $\gamma\colon W \to U^*$ по формулам $\beta(u) = \alpha(u,\, \cdot)$, $\gamma(w) = \alpha(\cdot,\, w)$.

Предложение 15.63. *Спаривание α невырождено тогда и только тогда, когда определенные выше линейные отображения β и γ являются изоморфизмами.*

Доказательство. Пусть α невырождено. Тогда легко видеть, что β и γ инъективны. Отсюда (в силу конечномерности U и W) следует, что $\dim U = \dim W$, а любое инъективное линейное отображение между конечномерными линейными пространствами одинаковой размерности — изоморфизм. В обратную сторону доказательство аналогично. ■

Определим теперь невырожденное спаривание

$$\langle\ ,\ \rangle\colon \bigwedge{}^k V \times \bigwedge{}^{n-k} V \to \mathbb{K}, \tag{143}$$

где V — n-мерное линейное пространство над полем $\mathbb{K}$. Для этого вспомним, что $\dim \bigwedge^n V = 1$, а значит $\bigwedge^n V \cong \mathbb{K}$ как линейные пространства над $\mathbb{K}$.

Предложение 15.64. *Для произвольного изоморфизма $\varepsilon\colon \bigwedge^n V \to \mathbb{K}$ спаривание (143), задаваемое формулой $\langle a, b\rangle = \varepsilon(a \wedge b)$, невырождено.*

Доказательство. Пусть $\{e_1, \ldots, e_n\}$ — базис в V. Пусть $e_{i_1} \wedge \ldots \wedge e_{i_k}$, $1 \leq i_1 < \ldots < i_k \leq n$ и $e_{j_1} \wedge \ldots \wedge e_{j_{n-k}}$, $1 \leq j_1 < \ldots < j_{n-k} \leq n$ — базисные элементы в $\bigwedge^k V$ и $\bigwedge^{n-k} V$ соответственно. Тогда требуемое утверждение следует из того, что

$$(e_{i_1}\wedge\ldots\wedge e_{i_k})\wedge(e_{j_1}\wedge\ldots\wedge e_{j_{n-k}}) = \begin{cases} \pm e_1 \wedge \ldots \wedge e_n \neq 0, & \text{если } \{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_{n-k}\} = \{1, 2, \ldots, n\}; \\ 0 & \text{в противном случае.} \end{cases}$$

■

Таким образом, зафиксировав изоморфизм ε, мы получаем изоморфизмы $\bigwedge^k V \to (\bigwedge^{n-k} V)^*$ и $\bigwedge^{n-k} V \to (\bigwedge^k V)^*$.

Пусть теперь V — n-мерное евклидово пространство. Тогда можно задать структуру евклидова пространства на его внешней алгебре $\bigwedge V$ следующим образом. Рассмотрим отдельно $\bigwedge^k V$ для некоторого k, $0 \leq k \leq n$. Пусть $\{e_1, \ldots, e_n\}$ — некоторый ортонормированный базис в V. Мы знаем, что тогда $\{e_{i_1} \wedge \ldots \wedge e_{i_k} \mid 1 \leq i_1 < \ldots < i_k \leq n\}$ образуют базис в $\bigwedge^k V$. Объявим этот базис ортонормированным в $\bigwedge^k V$ относительно искомого скалярного произведения, а объединение таких базисов при $0 \leq k \leq n$ — ортонормированным базисом в $\bigwedge V = \oplus_{k=0}^n \bigwedge^k V$. В частности, $\bigwedge^k V$ и $\bigwedge^l V$ при $k \neq l$ — ортогональные подпространства в $\bigwedge V$.

На первый взгляд, данное выше определение скалярного произведения в $\bigwedge V$ зависит от выбора ортонормированного базиса в V, а не только от евклидовой структуры в V. Чтобы показать, что это не так, дадим другое его описание.

Предложение 15.65. *Определенное выше скалярное произведение в $\bigwedge V$ на разложимых тензорах совпадает со следующим:*

$$(v_1 \wedge \ldots \wedge v_k,\, w_1 \wedge \ldots \wedge w_l) = 0 \quad \textit{при} \quad k \neq l \quad \textit{и}$$

$$(v_1 \wedge \ldots \wedge v_k,\, w_1 \wedge \ldots \wedge w_k) = \det(v_i,\, w_j). \tag{144}$$

Доказательство. Левая и правая части (144) являются полилинейными отображениями $V \times \ldots \times V \to \mathbb{R}$, поэтому равенство достаточно проверить для элементов некоторого базиса. Кроме того, обе части кососимметричны по первым и последним аргументам, поэтому равенство (144) достаточно проверять для наборов $(v_1, \ldots, v_k) = (e_{i_1}, \ldots, e_{i_k})$, $(w_1, \ldots, w_k) = (e_{j_1}, \ldots, e_{j_k})$ для произвольных наборов $1 \leq i_1 < \ldots < i_k \leq n$, $1 \leq j_1 < \ldots < j_k \leq n$, а в этом случае оно очевидно. ■

С разложимых тензоров скалярное произведение на всю внешнюю алгебру $\bigwedge V$ продолжается однозначно, поэтому его определение в самом деле инвариантно.

Таким образом, для евклидова пространства V пространства $\bigwedge V$ и $\bigwedge^k V$ также являются евклидовыми пространствами.

Евклидова структура на $\bigwedge^k V$ задает изоморфизм $\bigwedge^k V \to (\bigwedge^k V)^*$, $c \mapsto (\cdot, c)$. Беря его композицию с обратным к изоморфизму $\bigwedge^{n-k} V \to (\bigwedge^k V)^*$, определяемому невырожденным спариванием (143), получаем изоморфизм $\star\colon \bigwedge^k V \to \bigwedge^{n-k} V$. Как легко проверит читатель, явное определение $\star$ следующее: для $b \in \bigwedge^k V$ элемент $\star b$ — такой единственный элемент из $\bigwedge^{n-k} V$, что для любого $a \in \bigwedge^k V$ выполнено равенство $\varepsilon(a \wedge \star b) = (a, b)$.

Как можно задать конкретный изоморфизм $\varepsilon\colon \bigwedge^n V \to \mathbb{K}$? Для этого помимо евклидовой структуры на V достаточно задать ориентацию и объявить $\varepsilon(e_1 \wedge \ldots \wedge e_n) = 1$ для правого ортонормированного базиса $\{e_1, \ldots, e_n\}$ в V. Заметим, что $e'_1 \wedge \ldots \wedge e'_n = e_1 \wedge \ldots \wedge e_n$ для любого базиса $\{e'_1, \ldots, e'_n\}$ в V, ориентированный объем которого также равен 1. Обозначим $\omega := e_1 \wedge \ldots \wedge e_n$.

Определение 15.66. Определенный выше изоморфизм $\star\colon \bigwedge^k V \to \bigwedge^{n-k} V$ называется *оператором Ходжа* (или *звездочкой Ходжа*). Во введенных выше обозначениях он явно определяется формулой $a \wedge \star b = (a, b)\omega$ для произвольных $a, b \in \bigwedge^k V$.

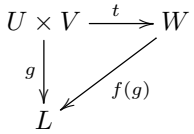
Задача 15.67. *Докажите следующие свойства оператора Ходжа $\star$:*

- $\star 1 = \omega, \ \ \star\omega = 1$;
- $\star(e_{i_1} \wedge \ldots \wedge e_{i_k}) = \pm e_{j_1} \wedge \ldots \wedge e_{j_{n-k}}$, *где* $\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_{n-k}\} = \{1, 2, \ldots, n\}$ *и знак* $\pm$ *совпадает со знаком перед* ω *в* $(e_{i_1} \wedge \ldots \wedge e_{i_k}) \wedge (e_{j_1} \wedge \ldots \wedge e_{j_{n-k}}) = \pm\omega$;
- $\star\star = (-1)^{k(n-k)}$ *на пространстве* $\bigwedge^k V$.

15.11 Тензорное произведение линейных пространств

Существует другой, более гибкий и общий подход к понятию тензора, основанный на определении тензорного произведения линейных пространств. В данном разделе мы дадим набросок частного случая соответствующей теории для конечномерных линейных пространств, отсылая заинтересованного читателя за подробностями, например, к учебнику [17].

Определение 15.68. Пусть U, V — векторные пространства над полем $\mathbb{K}$. Их *тензорным произведением* называется пара (W, t), которая состоит из векторного пространства W над тем же полем и билинейного отображения $t\colon U \times V \to W$, обладающая следующим *свойством универсальности*: для любого векторного пространства L над полем $\mathbb{K}$ и произвольного билинейного отображения $g\colon U \times V \to L$ существует, притом единственное, *линейное* отображение $f = f(g)\colon W \to L$ такое, что диаграмма



коммутативна, то есть $g = f(g) \circ t$.

Теорема 15.69. *Тензорное произведение двух*[77] *пространств существует.*

Доказательство. Доказательство заключается в предъявлении явной конструкции тензорного произведения, для которой нужно проверить выполнение универсального свойства. Предположим для простоты, что пространства U и V конечномерны, $\dim U = m, \ \ \dim V = n$.

1) Конструкция тензорного произведения. Пусть $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ и $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ — некоторые базисы в U и V соответственно. Определим пару (W, t) так: $t(\mathbf{u}_i, \mathbf{v}_j) =: \mathbf{w}_{ij}$, где $\{\mathbf{w}_{ij}\}_{1 \le i \le m,\, 1 \le j \le n}$ — базис в W. Тем самым билинейное отображение t однозначно определено:

$$t\left(\sum_i \lambda_i \mathbf{u}_i, \sum_j \mu_j \mathbf{v}_j\right) = \sum_{i,\,j} \lambda_i \mu_j \mathbf{w}_{ij}. \tag{145}$$

[77] А также любого конечного числа — в определении нужно просто заменить билинейные отображения полилинейными.

2) Проверка универсального свойства. Пусть $g\colon U \times V \to L$ — произвольное билинейное отображение. Линейное отображение $f(g)\colon W \to L$ зададим на базисе $\{\mathbf{w}_{ij}\}_{1\le i\le m,\ 1\le j\le n}$ пространства W формулой $f(g)(\mathbf{w}_{ij}) = g(\mathbf{u}_i, \mathbf{v}_j)$. Тем самым линейное отображение $f(g)$ корректно определено. Кроме того, ясно, что это — единственное линейное отображение со свойством $g = f(g) \circ t$. ■

Задача 15.70. *Пусть $\mathbb{K}^m$ и $\mathbb{K}^n$ — пространства столбцов высоты m и n соответственно. Докажите, что пара* $(\mathrm{Mat}_{m\times n}(\mathbb{K}), t)$, *где*

$$t\colon \mathbb{K}^m \times \mathbb{K}^n \to \mathrm{Mat}_{m\times n}(\mathbb{K}), \quad t(x, y) = xy^T,\ x \in \mathbb{K}^m,\ y \in \mathbb{K}^n$$

является тензорным произведением пространств $\mathbb{K}^m$ и $\mathbb{K}^n$.

Приведем пример тензорного произведения бесконечномерных (точнее, счетномерных) линейных пространств. Рассмотрим билинейное отображение

$$t\colon \mathbb{K}[x] \times \mathbb{K}[y] \to \mathbb{K}[x, y], \quad t(f, g)(x, y) := f(x)g(y).$$

Так как система $t(x^i, y^j) = x^i y^j$ $(i, j = 0, 1, 2, \ldots)$ образует базис в пространстве $\mathbb{K}[x, y]$, то легко видеть, что $(\mathbb{K}[x, y], t)$ — тензорное произведение пространств $\mathbb{K}[x]$ и $\mathbb{K}[y]$.

Может показаться, что приведенная конструкция тензорного произведения зависит от выбора базисов в пространствах U и V, но это не так. Например, пусть U и V конечномерны и $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ и $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ — выбранные базисы в них. Тогда, используя матрицы перехода, легко проверить (сделайте это!), что если $\mathbf{w}_{ij} = t(\mathbf{u}_i, \mathbf{v}_j)$ образуют базис в W, то и для любых базисов $\{\mathbf{u}'_1, \ldots, \mathbf{u}'_m\}$ и $\{\mathbf{v}'_1, \ldots, \mathbf{v}'_n\}$ в U и V векторы $\mathbf{w}'_{ij} := t(\mathbf{u}'_i, \mathbf{v}'_j)$ также образуют базис в W.

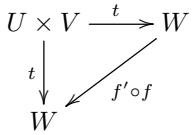
Существуют и другие конструкции тензорного произведения линейных пространств. Но обычно удобно работать не с конкретной реализацией тензорного произведения, а использовать его универсальное свойство.

Например, в следующей теореме из одного лишь свойства универсальности выводится утверждение о единственности тензорного произведения.

Теорема 15.71. *Тензорное произведение данных пространств единственно с точностью до канонического изоморфизма.*

Доказательство. Мы покажем, что если (W', t') — еще одно тензорное произведение пространств U и V, то существуют такие единственные линейные отображения $f\colon W \to W'$ и $f'\colon W' \to W$, что $f \circ t = t',\ f' \circ t' = t,\ f' \circ f = \mathrm{id}_W,\ f \circ f' = \mathrm{id}_{W'}$. Действительно, по свойству универсальности пар (W, t) и (W', t') существуют такие единственные $f\colon W \to W'$ и $f'\colon W' \to W$, что диаграммы

коммутативны, то есть $f \circ t = t',\ f' \circ t' = t$. Тогда диаграмма



коммутативна, но коммутативна также диаграмма, отличающаяся от предыдущей только тем, что в ней вместо $f' \circ f$ стоит id_W. В силу единственности $f' \circ f = \mathrm{id}_W$; аналогично доказывается $f \circ f' = \mathrm{id}_{W'}$. ■

То есть в указанном в теореме смысле тензорное произведение единственно ("с точностью до канонического изоморфизма") и не зависит от конкретной конструкции. Пространство W обычно обозначается $U \otimes V$ и часто само называется тензорным произведением U и V.

Следствие 15.72. $\dim(U \otimes V) = \dim U \cdot \dim V$.

Доказательство. В доказательстве теоремы 15.69 мы предъявили конструкцию тензорного произведения (W, t) пространств U и V, для которой $\dim W = \dim U \cdot \dim V$, а из единственности тензорного произведения с точностью до изоморфизма следует, что $\dim(U \otimes V)$ корректно определена (то есть не зависит от выбора конкретной конструкции тензорного произведения). ■

Элементы пространства $U \otimes V$ называются *тензорами*, а элементы $U \otimes V$, лежащие в образе t, — *разложимыми тензорами* и обозначаются $\mathbf{u} \otimes \mathbf{v} := t(\mathbf{u}, \mathbf{v})$. Как следует из предыдущего, множество разложимых тензоров содержит некоторый базис пространства $U \otimes V$. Отсюда, конечно, не следует, что всякий тензор разложим (за исключением случаев, когда одно из пространств U или V имеет размерность ≤ 1): нужно помнить, что отображение t не линейное, а билинейное, и его образ в общем случае не является линейным подпространством.

Заметим еще, что из билинейности универсального отображения $t\colon U \times V \to U \otimes V$ следуют соотношения

$$(\mathbf{u}_1 + \mathbf{u}_2) \otimes \mathbf{v} = \mathbf{u}_1 \otimes \mathbf{v} + \mathbf{u}_2 \otimes \mathbf{v}, \quad (\lambda \mathbf{u}) \otimes \mathbf{v} = \lambda(\mathbf{u} \otimes \mathbf{v})$$

и аналогичные соотношения для 2-го аргумента.

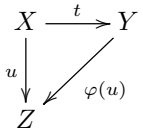
Введем дополнительные обозначения. Пространство билинейных отображений $U \times V \to L$ обозначим $\mathcal{L}(U, V; L)$, а пространство линейных отображений $W \to L$ — $\mathcal{L}(W; L)$.

Из определения тензорного произведения легко следует, что сопоставление $g \mapsto f(g)$ определяет канонический (то есть инвариантно определенный, не зависящий от базиса) изоморфизм линейных пространств

$$\mathcal{L}(U, V; L) \to \mathcal{L}(U \otimes V; L). \tag{146}$$

Так как читатель данного текста, скорее всего, впервые видит определение математической конструкции с помощью универсального свойства, приведём еще один пример подобного рода.

Пример 15.73. Пусть X — множество, на котором задано отношение эквивалентности $\sim$. *Фактормножеством* множества X по отношению эквивалентности $\sim$ называется пара (Y, t), состоящая из множества Y и постоянного на классах эквивалентности отображения $t\colon X \to Y$ (то есть такого, что из $x_1 \sim x_2$ следует $t(x_1) = t(x_2)$) такая, что для любой другой аналогичной пары (Z, u), состоящей из множества Z и постоянного на классах эквивалентности отображения $u\colon X \to Z$ существует единственное отображение $\varphi(u)\colon Y \to Z$ такое, что диаграмма



коммутативна. То есть для любого множества Z определена биекция между постоянными на классах эквивалентности отображениями $X \to Z$ и (просто) отображениями множеств $Y \to Z$, $u \mapsto \varphi(u)$. Неформально говоря, Y — "самое маленькое" множество, через которое пропускается любое отображение $X \to Z$, постоянное на классах эквивалентности.

Аргумент, аналогичный приведённому в доказательстве Теоремы 15.71 показывает, что если факторможество существует, то оно единственно с точностью до канонического изоморфизма. Осталось предъявить явную конструкцию факторможества, для которой выполнено универсальное свойство. Читатель легко проверит, что требуемым универсальным свойством обладает пара $(Y, t) = (X/\sim, \pi)$, где $X/\sim$ — факторможество, а $\pi\colon X \to X/\sim$ — факторотображение как они были определены в §1.2.

Читателю предлагается дать аналогичное (через универсальное свойство) определение факторпространства линейного пространства и (если он знаком с общей топологией) определение факторпространства топологического пространства.

Задача 15.74. *Докажите что представление ненулевого разложимого тензора* $\mathbf{w} \in U \otimes V$ *в виде* $\mathbf{u} \otimes \mathbf{v}$ *единственно с точностью до замен* $\mathbf{u} \mapsto \lambda \mathbf{u},\ \mathbf{v} \mapsto \lambda^{-1}\mathbf{v}\ \ (\lambda \in \mathbb{K}^*)$.

Решение. Пусть $\mathbf{w} = \mathbf{u}' \otimes \mathbf{v}'$ для некоторых $\mathbf{u}' \in U,\ \mathbf{v}' \in V$. Включим векторы $\mathbf{u}$ и $\mathbf{v}$ в базисы $\{\mathbf{u}_1 := \mathbf{u}, \mathbf{u}_2, \ldots\}$ и $\{\mathbf{v}_1 := \mathbf{v}, \mathbf{v}_2, \ldots\}$ пространств U и V. Пусть $\mathbf{u}' = \sum \lambda_i \mathbf{u}_i,\ \mathbf{v}' = \sum \mu_j \mathbf{v}_j$. Тогда $\mathbf{w} = \mathbf{u}_1 \otimes \mathbf{v}_1 = \mathbf{u}' \otimes \mathbf{v}' = \sum_{i,\,j} \lambda_i \mu_j \mathbf{u}_i \otimes \mathbf{v}_j$. Поскольку $\mathbf{u}_i \otimes \mathbf{v}_j\ \ (i,\, j = 1,\, 2, \ldots)$ образуют базис в $U \otimes V$, то $\lambda_1 \mu_1 = 1$ и $\lambda_i = \mu_j = 0$ при $i \neq 1,\ j \neq 1$. ■

Как связана конструкция тензорного произведения линейных пространств с данной нами ранее конструкцией тензоров типа $(p,\, q)$ как полилинейных отображений

$$\varphi\colon \underbrace{V \times \ldots \times V}_{q \text{ штук}} \times \underbrace{V^* \times \ldots \times V^*}_{p \text{ штук}} \to \mathbb{K}\,?$$

Ответ: $\mathbf{T}^p_q(V) \cong \underbrace{V^* \otimes \ldots \otimes V^*}_{q \text{ штук}} \otimes \underbrace{V \otimes \ldots \otimes V}_{p \text{ штук}}$ (канонический изоморфизм).

Для упрощения обозначений докажем сформулированное утверждение для $p = 1,\, q = 2$ (в общем случае доказательство аналогично).

Предложение 15.75. *Существует канонический изоморфизм* $\mathbf{T}^1_2(V) \cong V^* \otimes V^* \otimes V$.

Доказательство. Определим трилинейное отображение

$$\theta\colon V^* \times V^* \times V \to \mathbf{T}^1_2(V), \quad \text{где } \theta(f,\, g,\, v) \in \mathbf{T}^1_2(V) \text{ — такая трилинейная форма, что}$$

$$\theta(f,\, g,\, v)(u,\, w,\, h) = f(u)g(w)h(v)\ \ \forall\, u,\, w \in V,\, h \in V^*.$$

Тогда по универсальному свойству тензорного произведения существует такое единственное линейное отображение $\kappa = \kappa(\theta)\colon V^* \otimes V^* \otimes V \to \mathbf{T}^1_2(V)$, что диаграмма

$$\begin{array}{ccc} V^* \times V^* \times V & \xrightarrow{\ t\ } & V^* \otimes V^* \otimes V \\ \Big\downarrow{\scriptstyle \theta} & \swarrow{\scriptstyle \kappa} & \\ \mathbf{T}^1_2(V) & & \end{array}$$

коммутативна. Из коммутативности диаграммы $\kappa(f \otimes g \otimes v) = \theta(f,\, g,\, v)$. Теперь, беря в качестве $(f,\, g,\, v)$ всевозможные тройки $(e^i,\, e^j,\, e_k)$ для базиса $\{e_1, \ldots, e_n\}$ в V легко проверить, что образ линейного отображения κ содержит базис в $\mathbf{T}^1_2(V)$, а значит κ сюръективно, и, следовательно, изоморфизм. ■

Важным свойством тензорного произведения является то, что его можно определить не только для линейных пространств, но и для линейных отображений.

Пусть даны произвольные линейные отображения

$$\varphi\colon U \to L,\ \ \psi\colon V \to M.$$

Построим линейное отображение

$$\chi\colon U \otimes V \to L \otimes M,$$

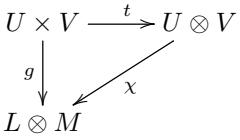
однозначно (поскольку разложимые тензоры содержат базис) задаваемое равенством

$$\chi(\mathbf{u} \otimes \mathbf{v}) = \varphi(\mathbf{u}) \otimes \psi(\mathbf{v})\ \ \forall \mathbf{u} \in U,\, \mathbf{v} \in V.$$

Для этого сначала определим билинейное отображение

$$g\colon U \times V \to L \otimes M,\ \ g(\mathbf{u},\, \mathbf{v}) = \varphi(\mathbf{u}) \otimes \psi(\mathbf{v}).$$

Тогда по универсальному свойству тензорного произведения существует единственное линейное отображение χ, превращающее диаграмму



в коммутативную. Очевидно, что χ — искомое. Его часто обозначают $\varphi \otimes \psi$ и называют *тензорным произведением линейных отображений* φ и ψ.

Если φ относительно выбранных базисов в U и L имеет матрицу A, а ψ — относительно базисов в V и M — матрицу B, то $\varphi \otimes \psi$ относительно тензорных произведений базисов в $U \otimes V$ и $L \otimes M$ (при соответствующем упорядочивании) имеет в качестве матрицы *кронекерово произведение* матриц $A \otimes B$.

Задача 15.76. *Пусть линейные операторы* $\varphi, \psi\colon V \to V$ *в базисе* $\{\mathbf{e}_1, \mathbf{e}_2\}$ *пространства* V *заданы матрицами*

$$A_\varphi = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}, \qquad A_\psi = \begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix}.$$

Найдите матрицу оператора $\varphi \otimes \psi\colon V \otimes V \to V \otimes V$ *в базисе* $\{\mathbf{e}_1 \otimes \mathbf{e}_1, \mathbf{e}_1 \otimes \mathbf{e}_2, \mathbf{e}_2 \otimes \mathbf{e}_1, \mathbf{e}_2 \otimes \mathbf{e}_2\}$.

Решение. Имеем

$$(\varphi \otimes \psi)(\mathbf{e}_1 \otimes \mathbf{e}_1) = \varphi(\mathbf{e}_1) \otimes \psi(\mathbf{e}_1) =$$

$$= (\mathbf{e}_1 - \mathbf{e}_2) \otimes (2\mathbf{e}_1 + 3\mathbf{e}_2) = 2\mathbf{e}_1 \otimes \mathbf{e}_1 + 3\mathbf{e}_1 \otimes \mathbf{e}_2 - 2\mathbf{e}_2 \otimes \mathbf{e}_1 - 3\mathbf{e}_2 \otimes \mathbf{e}_2;$$

аналогично

$$(\varphi \otimes \psi)(\mathbf{e}_1 \otimes \mathbf{e}_2) = \varphi(\mathbf{e}_1) \otimes \psi(\mathbf{e}_2) =$$

$$= (\mathbf{e}_1 - \mathbf{e}_2) \otimes (-\mathbf{e}_1 + \mathbf{e}_2) = -\mathbf{e}_1 \otimes \mathbf{e}_1 + \mathbf{e}_1 \otimes \mathbf{e}_2 + \mathbf{e}_2 \otimes \mathbf{e}_1 - \mathbf{e}_2 \otimes \mathbf{e}_2,$$

$$(\varphi \otimes \psi)(\mathbf{e}_2 \otimes \mathbf{e}_1) = \varphi(\mathbf{e}_2) \otimes \psi(\mathbf{e}_1) =$$

$$= (2\mathbf{e}_1 + 3\mathbf{e}_2) \otimes (2\mathbf{e}_1 + 3\mathbf{e}_2) = 4\mathbf{e}_1 \otimes \mathbf{e}_1 + 6\mathbf{e}_1 \otimes \mathbf{e}_2 + 6\mathbf{e}_2 \otimes \mathbf{e}_1 + 9\mathbf{e}_2 \otimes \mathbf{e}_2,$$

$$(\varphi \otimes \psi)(\mathbf{e}_2 \otimes \mathbf{e}_2) = \varphi(\mathbf{e}_2) \otimes \psi(\mathbf{e}_2) =$$

$$= (2\mathbf{e}_1 + 3\mathbf{e}_2) \otimes (-\mathbf{e}_1 + \mathbf{e}_2) = -2\mathbf{e}_1 \otimes \mathbf{e}_1 + 2\mathbf{e}_1 \otimes \mathbf{e}_2 - 3\mathbf{e}_2 \otimes \mathbf{e}_1 + 3\mathbf{e}_2 \otimes \mathbf{e}_2.$$

Таким образом,

$$A_{\varphi\otimes\psi} = \begin{pmatrix} 2 & -1 & 4 & -2 \\ 3 & 1 & 6 & 2 \\ -2 & 1 & 6 & -3 \\ -3 & -1 & 9 & 3 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} & 2\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} \\ -1\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} & 3\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} \end{pmatrix}$$

— кронекерово произведение матриц A_φ и A_ψ. ■

В заключении приведем несколько задач, цель которых — помочь читателю освоиться с понятием канонического изоморфизма.

Задача 15.77. *Постройте канонический изоморфизм*

$$U^* \otimes V^* \cong (U \otimes V)^*. \tag{147}$$

Решение. Во-первых, определим билинейное отображение

$$g\colon U^* \times V^* \to \mathcal{L}(U, V; \mathbb{K})$$

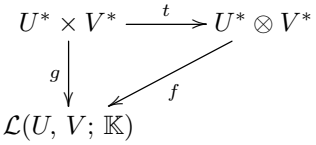
(где $\mathcal{L}(U, V; \mathbb{K})$ обозначает векторное пространство билинейных отображений $U \times V \to \mathbb{K}$) с помощью формулы

$$g(\alpha, \beta)(\mathbf{u}, \mathbf{v}) = \alpha(\mathbf{u})\beta(\mathbf{v}),$$

где $\alpha \in U^*$, $\beta \in V^*$, $\mathbf{u} \in U$, $\mathbf{v} \in V$. По универсальному свойству тензорного произведения тогда существует единственное линейное отображение

$$f\colon U^* \otimes V^* \to \mathcal{L}(U, V; \mathbb{K})$$

такое, что диаграмма



коммутативна. Беря композицию f с изоморфизмом (146) при $L = \mathbb{K}$, получим линейное отображение $\phi\colon U^* \otimes V^* \to (U \otimes V)^*$ (поскольку $\mathcal{L}(U \otimes V; \mathbb{K}) = (U \otimes V)^*$).

Покажем, что ϕ — изоморфизм. Очевидно, достаточно доказать, что f — изоморфизм. Более того, так как f — линейное отображение между пространствами одинаковой размерности, достаточно установить сюръективность f. Покажем, что

$$g(\mathbf{u}^i, \mathbf{v}^j) = f(\mathbf{u}^i \otimes \mathbf{v}^j), \quad 1 \leq i \leq m, 1 \leq j \leq n$$

составляют базис в $\mathcal{L}(U, V; \mathbb{K})$, где $\{\mathbf{u}^1, \ldots, \mathbf{u}^m\}$ — базис в U^*, биортогональный базису $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ в U, а $\{\mathbf{v}^1, \ldots, \mathbf{v}^n\}$ — базис в V^*, биортогональный базису $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ в V. Действительно, по определению g имеем

$$g(\mathbf{u}^i, \mathbf{v}^j)(\mathbf{u}_k, \mathbf{v}_l) = \mathbf{u}^i(\mathbf{u}_k)\mathbf{v}^j(\mathbf{v}_l) = \delta^i_k \delta^j_l,$$

где

$$\delta^i_j = \begin{cases} 1, & i = j; \\ 0, & i \neq j \end{cases}$$

— символ Кронекера. Если $h \in \mathcal{L}(U, V; \mathbb{K})$ — произвольная билинейная форма, то $h = \sum_{i,\,j} h_{ij} g(\mathbf{u}^i, \mathbf{v}^j)$, где $h_{ij} := h(\mathbf{u}_i, \mathbf{v}_j) \in \mathbb{K}$ — единственное разложение h по $g(\mathbf{u}^i, \mathbf{v}^j) \in \mathcal{L}(U, V; \mathbb{K})$. Тем самым сюръективность f доказана, поскольку это — линейное отображение, образ которого содержит базис. ■

Задача 15.78. *Постройте канонический изоморфизм*

$$U^* \otimes V \cong \mathcal{L}(U; V). \tag{148}$$

Решение. Для этого, во-первых, определим билинейное отображение

$$g\colon U^* \times V \to \mathcal{L}(U, V)$$

с помощью формулы

$$g(\alpha, \mathbf{v})(\mathbf{u}) = \alpha(\mathbf{u})\mathbf{v},$$

где $\alpha \in U^*$, $\mathbf{u} \in U$, $\mathbf{v} \in V$. Согласно универсальному свойству тензорного произведения, существует, причем единственное, линейное отображение $f\colon U^* \otimes V \to \mathcal{L}(U; V)$, которое превращает диаграмму

$$\begin{array}{ccc} U^* \times V & \xrightarrow{\ t\ } & U^* \otimes V \\ {\scriptstyle g}\big\downarrow & \swarrow{\scriptstyle f} & \\ \mathcal{L}(U; V) & & \end{array} \tag{149}$$

в коммутативную.

Покажем, что f — изоморфизм. Снова, в силу равенства размерностей, достаточно доказать его сюръективность. Из равенства $g(\mathbf{u}^i, \mathbf{v}_j)(\mathbf{u}_k) = \delta^i_k \mathbf{v}_j$ легко получить, что матрица оператора $f(\mathbf{u}^i \otimes \mathbf{v}_j)$ в выбранных в пространствах U, V базисах есть E_{ji}, причем когда i пробегает числа от 1 до m, а j — от 1 до n, матрицы E_{ji} пробегают некоторый базис пространства $\mathcal{L}(U; V)$. Тем самым сюръективность установлена. ■

Интересно отметить, что образ $\operatorname{im} t$ универсального билинейного отображения t из диаграммы (149) ("разложимые тензоры") состоит в точности из линейных отображений ранга ≤ 1, в частности, отображение t не сюръективно, хотя его образ содержит базис $U^* \otimes V$. Это, конечно, связано с тем, что t является не линейным, а билинейным отображением.

В частном случае $U = V$ мы имеем канонический изоморфизм

$$f\colon V^* \otimes V \to \mathcal{L}(V; V) =: \mathcal{L}(V). \tag{150}$$

Заметим, что в $\mathcal{L}(V)$ есть выделенный элемент, а именно тождественный оператор id_V. Какой элемент $V^* \otimes V$ ему отвечает при каноническом изоморфизме из формулы (150)? Легко видеть, что $f^{-1}(\mathrm{id}_V) = \sum_i \mathbf{v}^i \otimes \mathbf{v}_i$[78] для любой пары двойственных базисов $\{\mathbf{v}_i\}$, $\{\mathbf{v}^j\}$.

На пространстве $\mathcal{L}(V)$ имеется канонический линейный функционал следа $tr\colon \mathcal{L}(V) \to \mathbb{K}$, сопоставляющий линейному оператору его след. С другой стороны, на векторном пространстве $V^* \otimes V$ есть линейный функционал $c\colon V^* \otimes V \to \mathbb{K}$, называемый *сверткой*. Это — линейное отображение, которое на разложимых тензорах $\alpha \otimes \mathbf{v} \in V^* \otimes V$ определяется как вычисление значения линейного функционала α на векторе $\mathbf{v}$, то есть $c(\alpha \otimes \mathbf{v}) = \alpha(\mathbf{v}) \in \mathbb{K}$.

Задача 15.79. *Покажите, что при отождествлении пространства $\mathcal{L}(V)$ с $V^* \otimes V$ посредством изоморфизма (150) след переходит в свертку, то есть $tr \circ f = c$.*

Решение. При изоморфизме (150) тензор $\sum_{i,j} t^j_i \, \mathbf{v}^i \otimes \mathbf{v}_j$ отождествляется с линейным оператором $T\colon V \to V$, имеющим в базисе $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ матрицу (t^j_i) (таким образом, верхний индекс — номер строки, нижний — номер столбца). След — линейный функционал $(t^j_i) \mapsto \sum_i t^i_i$, инвариантный относительно замен базиса. Он отвечает сопоставлению тензору $\sum_{i,j} t^j_i \mathbf{v}^i \otimes \mathbf{v}_j$ числа $\sum_i t^i_i$. С другой стороны,

$$c\left(\sum_{i,j} t^j_i \mathbf{v}^i \otimes \mathbf{v}_j\right) = \sum_{i,j} t^j_i \mathbf{v}^i(\mathbf{v}_j) = \sum_{i,j} t^j_i \delta^i_j = \sum_i t^i_i. \quad ■$$

[78] С использованием указанного изоморфизма в квантовой механике тождественный оператор в дираковских обозначениях записывается в виде $\sum_i |i\rangle\langle i|$.

Список литературы

[1] Алания Л.А. и др. Сборник задач по аналитической геометрии и линейной алгебре /под редакцией Ю.М. Смирнова — М.: МЦНМО, 2016.—384 с.

[2] Алексеев В.Б. Теорема Абеля в задачах и решениях. Библиотечка “Квант” выпуск 137. — М.: МЦНМО, 2017. — 216 стр.

[3] Арнольд В.И. Геометрия комплексных чисел, кватернионов и спинов. — М.: МЦНМО, 2002.— 40 с.

[4] Арнольд В.И. Математические методы классической механики: учебное пособие. Изд. 5-е, стереотипное. — М.: Эдиториал УРСС, 2003.—416 с.

[5] Арнольд В.И. Лекции об уравнениях с частными производными. — М.: МЦНМО, 2017. — 182 с.

[6] Арутюнов А.А., Ершов А.В. Дополнительные задачи по линейной алгебре: Учеб. пособие. — М.: МЦНМО, 2020. — 256 с.

[7] Беклемишев Д.В. Курс аналитической геометрии и линейной алгебры: Учеб. для вузов. — 13-е изд., испр. — СПб.: Издательство “Лань”, 2015 — 448 с.

[8] Беклемишев Д.В. Решение задач из курса аналитической геометрии и линейной алгебры. — М.: Физматлит, 2014 — 192 с.

[9] Беклемишева Л.А., Петрович А.Ю., Чубаров И.А. Сборник задач по аналитической геометрии и линейной алгебре: Учебн. пособие / Под ред. Д.В. Беклемишева, 2-е изд., перераб. — М.: ФИЗМАТЛИТ, 2012.— 496 с.

[10] Веселов А.П., Троицкий Е.В. Лекции по аналитической геометрии. — М.: МЦНМО, 2016. — 150 с.

[11] Винберг Э.Б. Курс алгебры. — 2-е изд., стереотип. — М.: МЦНМО, 2013. — 592 с.

[12] Гайфуллин А.А., Пенской А.В., Смирнов С.В. Задачи по линейной алгебре и геометрии. — М.: МЦНМО, 2014. — 152 с.

[13] Гельфанд И.М. Лекции по линейной алгебре. — Издание четвертое, дополненное. — М.: Наука, 1971 — 272 с.

[14] Городенцев А.Л. Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — 488 с.

[15] Кожевников П.А. Введение в линейную алгебру. (неопубл.)

[16] Кострикин А.И. Введение в алгебру: Ч. II: Линейная алгебра. — Второе издание, стереотип. — М.: МЦНМО, 2012.— 368 с.

[17] Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. — М.: Изд-во Моск. ун-та, 1980. — 320 с.

[18] Новиков С.П., Тайманов И.А. Современные геометрические структуры и поля. — М.: МЦНМО, 2005.— 584 с.

[19] Шафаревич И.Р. Основные понятия алгебры. Изд. 3-е, испр. М.: ЛЕНАНД, 2019. — 408 с.

[20] Этингоф П. и др. Введение в теорию представлений. — М.: МЦНМО; НМУ, 2019. — 224 с.

[21] Massey W. S. Cross products of vectors in higher dimensional Euclidean spaces. — The American Mathematical Monthly. Mathematical Association of America. 90 (10): 697–701.

[22] Wildon Mark A short proof of the existence of Jordan Normal Form.— http://www.ma.rhul.ac.uk/~uvah099/Maths/JNFfinal.pdf