АЛГЕБРА И ГЕОМЕТРИЯ

Т.В. Дубровина, Н.И. Дубровин

Владимир 2002

Оглавление

Предисловие

Настоящее учебное пособие предназначено для студентов математических специальностей. Полный объем этого (годового) курса составляет 85 лекционных часов. Здесь представлены первые три главы, соответствующие первому семестру. Оставшиеся, не вошедшие в данное учебное пособие главы, – "Аффинные пространства", "Квадратичные формы и поверхности второго порядка", "Комплексные числа и многочлены", "Элементы теории групп". Предварительных знаний, кроме школьной математики, не требуется. Однако предполагается, что параллельно с этим курсом студенты проходят курс математического анализа, где определяется поле действительных чисел, важнейшие элементарные функции, производная, интеграл и т. п. Для успешного освоения курса нужны и практические занятия в объеме не меньшем, чем лекционные.

Очень часто стройное логическое изложение математической теории дается в порядке, если не совершенно, то частично противоположном к её историческому развитию. Безусловно это затрудняет понимание. Для того, что бы хотя бы как-то снять это противоречие, научные работы, книги порой читают с конца, возвращаясь к началу по мере необходимости. Не следует принимать это буквально, но пользоваться этим принципом при чтении данного пособия не только можно, но и нужно. Вспомогательную и весьма абстрактную главу 1 можно пропустить сначала, обращаясь к ней как к справочному материалу. Теорию линейных пространств (глава 3) без усвоения матричной алгебры и систем линейных уравнений (глава 2) читать бесполезно. Эти две главы – центральная часть пособия.

Изложение теоретического материала чередуется с задачами. Эти задачи не проверочные и не тестовые; они предназначены для глубокого усвоения теории. Наиболее трудные из них отмечены звездочкой.

Формулы нумеруются внутри каждой главы; а теоремы, предложения и определения – внутри каждого параграфа. Определяемые слова, так же, как и строгие формулировки утверждений, выделяются курсивом. Часто используемые обозначения указаны в начале.

Список условных обозначений

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – множества натуральных, целых, рациональных, действительных и комплексных чисел

$\mathbb{N}_0$ – множество неотрицательных целых чисел

$m \in M$ – принадлежность элемента m множеству M

$\subseteq$ – нестрогое включение множеств

$\subset$ – строгое включение множеств

$f \circ g$ – операция композиции двух отображений

$M \times N$ – декартово произведение множеств M и N

$f : M \to N$ – отображение множества M в множество N

$\{x_1, x_2, \ldots, x_n\}$ – множество, состоящее из элементов x_1, x_2, …, x_n

$(x_1, x_2, \ldots, x_n)$ – строка, состоящая из компонент x_1, x_2, …, x_n

S_n – группа подстановок

A_n – группа четных подстановок

$\mathcal{M}at\,(K)$ – множество всех матриц над полем K

$\mathcal{M}at_{\,n\times m}(K)$ – множество всех $n \times m$-матриц над полем K

E – единичная матрица

$\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ – диагональная квадратная матрица

$\det A$ – определитель матрицы A

$\overrightarrow{AB}$ – вектор с началом в точке A и концом в точке B

$\mathcal{V}(\mathbb{E}^3)$, $\mathcal{V}(\mathbb{E}^2)$ – линейные евклидовы пространства геометрических векторов

$\mathbf{ab}$ – скалярное произведение двух векторов

$\mathbf{a} \times \mathbf{b}$ – векторное произведение двух векторов

$\mathbf{a} \wedge \mathbf{b}$ – бивектор, внешнее произведение двух векторов

$(\mathbf{a}, \mathbf{b}, \mathbf{c})$ – смешанное произведение трех векторов

$|x|$ – абсолютная величина действительного или комплексного числа, длина вектора

$\|z\|$ – норма комплексного числа, норма кватерниона

$|AB|$ – длина отрезка AB

Глава 1

Логика и множества

Эта глава вводная, изложение здесь поверхностное. Цель этой главы – достаточно быстро познакомить с языком, на котором излагается вся математика, а также раз и навсегда определить алгебраические структуры (группы, кольца, поля) и действия над ними (подструктуры, декартовы произведения, фактор-структуры). Изложение весьма абстрактное; к этим определениям и конструкциям придется не раз возвращать-ся в более конкретной ситуации. Вторая цель этой главы – как можно скорее познакомить с важнейшими алгебраическими объектами – группой подстановок, полем комплексных чисел.

1.1 Элементы логики

Математический текст состоит из повествовательных предложений, которые называются *высказываниями* и про которые можно сказать, истинны они или ложны. Повествовательное предложение содержит подлежащее, сказуемое и дополнительные члены предложения. В математическом тексте роль подлежащего играют математические объекты (числа, функции, геометрические фигуры и тела и т. д.), о которых что-либо говорится. Например,

- Для любого действительного числа x имеет место неравенство $x^2 + 1 > 0$.
- $\int_0^2 x\,dx = 2$.
- Существует треугольник, сумма углов которого равна 100^0.

Повествовательные предложения предназначены для выражения законченной мысли; они могут быть как *истинными* (первое и второе предложение), так и *ложными* (третье предложение). Прежде чем говорить о смысле высказывания и, в частности, о его истинности и ложности, нужно научиться конструировать одни высказывания из других по правилам математической логики.

Пусть $\mathcal{A}$ и $\mathcal{B}$ – два высказывания. Тогда можно образовать следующие высказывания:

- $\mathcal{A}$ или $\mathcal{B}$

- не $\mathcal{A}$ (отрицание утверждения $\mathcal{A}$)
- $\mathcal{A}$ и $\mathcal{B}$
- $\mathcal{A} \Rightarrow \mathcal{B}$ (из $\mathcal{A}$ следует $\mathcal{B}$)
- $\mathcal{A} \Leftrightarrow \mathcal{B}$ ($\mathcal{A}$ *равносильно* $\mathcal{B}$; другими словами, утверждение $\mathcal{A}$ верно тогда и только тогда, когда верно утверждение $\mathcal{B}$)

Эти процедуры соединения предложений с помощью *логических операций*

$$\textbf{не}, \quad \textbf{или}, \quad \textbf{и}, \quad \Rightarrow, \quad \Leftrightarrow$$

можно многократно повторять.

Рассмотрим следующее предложение $\mathcal{A}\langle x\rangle$: $x^2 - 3x + 2 > 0$. Оно не является высказыванием, так как невозможно оценить его истинность. Но если вместо *переменной* x подставить конкретное число, например, -1, то получаем верное высказывание. Если же подставить число $3/2$, то получим ложное высказывание. Иными словами, $\mathcal{A}\langle -1\rangle$ – истинное высказывание, а $\mathcal{A}\langle 3/2\rangle$ – ложное. Такого рода предложения будем называть *высказывательными формами.*

Пусть $\mathcal{A}\langle x\rangle$ – произвольная высказывательная форма, содержащая переменную x. Её называют *незамкнутой* в том смысле, что $A\langle x\rangle$ можно *замкнуть*, образовав новое высказывание одним из двух способов:

- Существует x такой, что $\mathcal{A}\langle x\rangle$.
- Для любого x верно $\mathcal{A}\langle x\rangle$.

Эти логические конструкции столь часто применяются в математике, что им придумано обозначение:

- $\exists x : \mathcal{A}\langle x\rangle$
- $\forall x \Rightarrow \mathcal{A}\langle x\rangle$

Знаки $\exists$ и $\forall$ называются *квантором существования* и *квантором всеобщности.* Предположим, что у нас есть только конечное число способов подстановки вместо x конкретных значений – x_1, x_2,..., x_n. Тогда $\exists x : \mathcal{A}\langle x\rangle$ эквивалентно следующему высказыванию:

$$\mathcal{A}\langle x_1\rangle\textbf{или } \mathcal{A}\langle x_2\rangle\textbf{или } \ldots \mathcal{A}\langle x_n\rangle$$

а $\forall x \Rightarrow \mathcal{A}\langle x\rangle$ эквивалентно высказыванию

$$\mathcal{A}\langle x_1\rangle\textbf{и } \mathcal{A}\langle x_2\rangle\textbf{и } \ldots \mathcal{A}\langle x_n\rangle$$

Иными словами, квантор существования – это многократно повторяемая операция **или**, а квантор всеобщности – многократно повторяемая логическая операция **и**.

Истинность сложного высказывания определяется истинностью его составляющих высказываний по следующей таблице

$\mathcal{A}$	И	Л	И	Л
$\mathcal{B}$	И	И	Л	Л
$\mathcal{A}$ или $\mathcal{B}$	И	И	И	Л
$\mathcal{A}$ и $\mathcal{B}$	И	Л	Л	Л
не $\mathcal{A}$	Л	И	Л	И
$\mathcal{A} \Rightarrow \mathcal{B}$	И	И	Л	И
$\mathcal{A} \Leftrightarrow \mathcal{B}$	И	Л	Л	И

Особенно трудно воспринимается предпоследняя строка этой таблицы. Так, например,

(0=1) $\quad\Rightarrow\quad$ "сумма углов любого треугольника равна 180^0"
(0=1) $\quad\Rightarrow\quad$ "сумма углов любого треугольника равна 100^0"

– истинные высказывания.

С импликацией связано единственное правило вывода, допустимое в математике, – modus ponents.

(MP) *Если $\mathcal{A}$, а также $\mathcal{A} \Rightarrow \mathcal{B}$ – истинные утверждения, то и $\mathcal{B}$ верно.*

Нетрудно понять, что обосновывая истинность одних высказываний посредством других истинных высказываний, мы доберемся до первичных высказываний, в истинность которых нужно просто поверить. Такие высказывания называются *аксиомами математической теории.* Например, в теории натуральных чисел такими аксиомами могут быть следующие (см. [М, стр. 115]):

(AN1) $\forall n \Rightarrow S(n) \neq 0$

(AN2) $\forall n, m (S(n) = S(m) \Rightarrow n = m)$

(AN3) (*метод математической индукции*) Пусть $\mathcal{A}\langle x\rangle$ – какая-либо высказывательная форма с переменной x. Если $\mathcal{A}\langle 0\rangle$ верно и для любого натурального n из $\mathcal{A}\langle n\rangle$ вытекает $\mathcal{A}\langle S(n)\rangle$, то утверждение $\mathcal{A}\langle n\rangle$ верно для всех натуральных n.

Здесь S – неопределяемый функциональный символ, играющий роль прибавления единицы. Аксиомы теории множеств намного сложнее, и это тема отдельного параграфа (см. §1.3).

Выводом или *доказательством* в математике называется ряд высказываний $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3, \ldots$ такой, что каждое из $\mathcal{A}_i$-х является либо аксиомой, либо ему в этом ряду предшествуют высказывания вида $\mathcal{A}_k$, $\mathcal{A}_k \Rightarrow \mathcal{A}_i$ $(k < i)$. *Выводимым утверждением*, или *теоремой*, называется высказывание, которое может быть включено в какое-либо доказательство. Поскольку доводить до первичных аксиом доказательство какого-либо мало-мальски содержательного утверждения технически непосильная задача, то поступают так: развивая теорию и доказывая очередную теорему, допускают ссылку не только на аксиомы, но и на доказанные ранее теоремы. В этом случае полное доказательство какого-либо утверждения выглядит уже в виде древовидной структуры, корень которого – доказываемое утверждение, а крайние ветви – аксиомы. Оно так и называется – *дерево доказательства*. Точно по такой же схеме образуются новые понятия: каждое последующее определяется через предыдущие. Именно так мы поступаем в родной речи, когда объясняем кому-либо непонятное слово. Так, если считать, что понятия "место сидения", "подлокотник", "спинка", "человек", "один" известны, то *стул* можно определить как место для сидения одного человека без подлокотников и со спинкой.

Может так случиться, что в конструируемой теории выводимо какое-либо утверждение, а также его отрицание. Такая теория называется *противоречивой*; в ней все утверждения истинны и одновременно ложны. Пример такой теории нетрудно построить; достаточно взять в качестве аксиом произвольное утверждение вместе с его отрицанием. А что известно про непротиворечивость общеупотребительных математических теорий, например арифметики? Немало, – за несколько тысяч лет ее развития не найдено ни одного противоречия. Доказать строго математически непротиворечивость арифметики средствами самой арифметики невозможно; этот результат установил в 1933 году австрийский математик Курт Гедель.

1.2 Методы доказательств.

1.2.1 Метод математической индукции

Пусть $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots$ – серия утверждений, зависящих от натурального параметра n.

Предположим, что

- $\mathcal{P}_1$ *верное утверждение*
- *Для любого натурального n из справедливости утверждения $\mathcal{P}_n$ следует $\mathcal{P}_{n+1}$.*

Тогда все $\mathcal{P}_n$ истинны.

Продемонстрируем изложенный *принцип математической индукции* на примере доказательства равенства

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

Подставляя в эту формулу $n = 1$ убеждаемся в ее справедливости для этого частного случая. Это основание индукции. Предположим, что формула справедлива для какого-либо натурального n. Тогда

$$1 + 2 + 3 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)((n+1)+1)}{2}$$

Тем самым эта формула верна и для $n+1$. Мы обосновали индукционный переход и тем самым доказали полностью утверждение.

Иногда метод математической индукции удобно применять в следующей интерпретации: *если $\mathcal{P}_1$ истинное утверждение, и для любого натурального $n > 1$ из справедливости всех утверждений $\mathcal{P}_k$ при $k < n$ следует $\mathcal{P}_n$, то все утверждения $\mathcal{P}_n$ верны.*

Докажем, пользуясь методом математической индукции в вышеприведенной формулировке, что любое натуральное число $n > 1$ можно разложить в произведение простых чисел. База индукции здесь – случай $n = 2$. Тогда утверждение очевидным образом верно. Предположим теперь, что утверждение верно для всех натуральных чисел $k > 1$, меньших, чем n. Если число n не разложимо на натуральные множители, меньшие, чем n, то n – простое число, и доказывать нечего. В противном случае $n = mk$, где $1 < m < n$ и $1 < k < n$. Тогда применимо индукционное предположение, и числа m и k представимы в виде произведения простых чисел. Следовательно, n раскладывается в произведение простых чисел.

Задача 1. Выведите закон индукции во второй формулировке, пользуясь законом индукции в первой формулировке. Решите обратную задачу.

Пользуясь индукцией, можно не только доказывать, но и конструировать математические объекты и определять операции над ними. Уже операции сложения и умножения над натуральными числами определяются индукционно:

$$m + 1 := S(m) \text{ и } m + (n+1) := (m+n) + 1 \text{ для любого } n \in \mathbb{N};$$

$$m \cdot 1 := m \text{ и } m \cdot (n+1) := m \cdot n + m \text{ для любого } n \in \mathbb{N}.$$

Такая важная функция как *факториал* также определяется по индукции:

$$0! := 1 \text{ и } (n+1)! := n!(n+1) \text{ для любого } n \in \mathbb{N}.$$

Задача о биномиальных коэффициентах. Определим *биномиальный коэффициент* C_n^m для любых целых m и n таких, что $0 \le m \le n$ следующим образом:

$$C_n^0 = 1; \quad C_{n+1}^m = C_n^{m-1} + C_n^m.$$

Доказать, что $C_n^m = \frac{n!}{m!(n-m)!}$

1.2.2 Метод от противного

Логическая схема этого метода следующая: чтобы доказать некоторое утверждение $\mathcal{P}$, принимается на веру его отрицание **не** $\mathcal{P}$ и, пользуясь этим отрицанием как дополнительной аксиомой, приходим к противоречию, т. е. доказываем какое-либо утверждение $\mathcal{B}$ вместе с его отрицанием **не** $\mathcal{B}$. Тогда утверждение $\mathcal{P}$ следует. Действительно, имеем:

$$\textbf{не}\,\mathcal{P} \Rightarrow (\mathcal{B}\ \textbf{и}\ (\textbf{не}\,\mathcal{B}))\ \text{отсюда следует}\ \textbf{не}\,(\mathcal{B}\,\textbf{и}\,(\textbf{не}\,\mathcal{B})) \Rightarrow \textbf{не}\,(\textbf{не}\,\mathcal{P})$$

Это эквивалентно **не** $\mathcal{B}$ **или не** (**не** $\mathcal{B}$) $\Rightarrow \mathcal{P}$ или

$$\textbf{не}\,\mathcal{B}\ \textbf{или}\ \mathcal{B} \Rightarrow \mathcal{P} \tag{1.1}$$

Но **не** $\mathcal{B}$ **или** $\mathcal{B}$ это то же самое, что и $\mathcal{B} \Rightarrow \mathcal{B}$ – тождественная истина. Применяя modus ponents к (1.1), получаем, что $\mathcal{P}$ верно.

Докажем, например, что *простых чисел бесконечно много* ($\mathcal{P}$). Предположим противное, т. е. что простых чисел конечное число (**не** $\mathcal{P}$). Пусть p – наибольшее среди них. Рассмотрим число $m = p\,! + 1$. Сейчас мы выведем отсюда отрицание к известному факту: *любое натуральное число, большее единицы, делится хотя бы на одно простое число* ($\mathcal{B}$). Действительно, для любого простого числа q имеем: $q \le p$. Следовательно, q делит $p\,!$ и, значит, не делит m. Полученное противоречие ($\mathcal{B}$ **и** (**не** $\mathcal{B}$)) означает, что наше предположение **не** $\mathcal{P}$ было неверным. Следовательно, верно отрицание **не** (**не** $\mathcal{P}$), т. е. верно $\mathcal{P}$ ="простых чисел бесконечно много".

1.2.3 Метод разделения случаев

Пусть мы доказываем некоторое утверждение $\mathcal{P}$ или решаем уравнение или неравенство. Предположим, что мы выдвинули несколько гипотез $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ так, что в любом случае одна из этих гипотез имеет место, т. е. утверждение $\mathcal{H}_1$ **или** ... **или** $\mathcal{H}_n$ истинно. Предположим также, что, принимая на веру каждую из гипотез $\mathcal{H}_k$, нам удалось доказать утверждение $\mathcal{P}$. Тогда $\mathcal{P}$ – верное утверждение. Обоснуем этот *принцип разделения случаев*. Вначале докажем лемму.

Лемма 1 (законы де Моргана). *Высказывание* **не** ($\mathcal{A}$ **или** $\mathcal{B}$) *эквивалентно высказыванию* **не** $\mathcal{A}$ **и не** $\mathcal{B}$, *а высказывание* **не** ($\mathcal{A}$ **и** $\mathcal{B}$) *эквивалентно* **не** $\mathcal{A}$ **или не** $\mathcal{B}$).

Доказательство. Действительно, перебирая четыре возможных случая истинностных оценок высказываний $\mathcal{A}$ и $\mathcal{B}$ – ИИ, ИЛ, ЛИ, ЛЛ ("И" – истина, "Л" – ложь), получаем, что как высказывание **не** ($\mathcal{A}$ **или** $\mathcal{B}$) так и высказывание **не** $\mathcal{A}$ **и не** $\mathcal{B}$ верны, если и только, если $\mathcal{A}$ и $\mathcal{B}$ – ложь. Аналогично, $\mathcal{A}$ **и** $\mathcal{B}$ и **не** (**не** $\mathcal{A}$ **или не** $\mathcal{B}$) верны в том и только том случае, когда $\mathcal{A}$ и $\mathcal{B}$ истинны. Следовательно, **не** ($\mathcal{A}$ **и** $\mathcal{B}$) и **не** (**не** (**не** $\mathcal{A}$ **или не** $\mathcal{B}$)) эквивалентны. Остается учесть, что для любого высказывания
$\mathcal{P}$, **не** (**не** $\mathcal{P}$) эквивалентно $\mathcal{P}$ (*принцип двойного отрицания*). □

Перейдём к обоснованию метода разделения случаев. Имеем:

$$\forall k(\mathcal{H}_k \Rightarrow \mathcal{P}), \quad \text{т. е. } \forall k((\textbf{не}\,\mathcal{H}_k)\,\textbf{или}\,\mathcal{P})$$

Тогда следующее утверждение истинно

$$((\textbf{не}\,\mathcal{H}_1)\,\textbf{или}\,\mathcal{P})\,\textbf{и}\,\ldots\,\textbf{и}\,((\textbf{не}\,\mathcal{H}_n)\,\textbf{или}\,\mathcal{P}).$$

Следовательно, истинно и утверждение

$$(\textbf{не}\,(\mathcal{H}_1\,\textbf{или}\,\ldots\,\textbf{или}\,\mathcal{H}_n))\,\textbf{или}\,\mathcal{P}$$

(многократно пользуемся леммой 1). Значит, $\mathcal{H}_1\,\textbf{или}\,\ldots\,\textbf{или}\,\mathcal{H}_n \Rightarrow \mathcal{P}$. Так как по предположению утверждение $\mathcal{H}_1\,\textbf{или}\,\ldots\,\textbf{или}\,\mathcal{H}_n$ верно, то согласно modus ponents утверждение $\mathcal{P}$ также верно.

Пример 1. Доказать, что число $n(n+1)(n+2)$ делится на 6 при любом целом n. Рассмотрим шесть исчерпывающих случаев-гипотез, и в каждом из них докажем данное утверждение:

$$\begin{array}{ccccc}
n = 6m & \Rightarrow & 6|n & \Rightarrow & 6|A \\
n = 6m+1 & \Rightarrow & 2|n+1 \ \text{ и } \ 3|n+2 & \Rightarrow & 6|A \\
n = 6m+2 & \Rightarrow & 2|n \ \text{ и } \ 3|n+1 & \Rightarrow & 6|A \\
n = 6m+3 & \Rightarrow & 3|n \ \text{ и } \ 2|n+1 & \Rightarrow & 6|A \\
n = 6m+4 & \Rightarrow & 6|n+2 & \Rightarrow & 6|A \\
n = 6m+5 & \Rightarrow & 6|n+1 & \Rightarrow & 6|A
\end{array}$$

Если речь идет о решении уравнения или неравенства, то общий ответ получается объединением ответов, полученных в предположении каждой из гипотез $\mathcal{H}_k$.

Пример 2. Решить неравенство $\sqrt{x^2+x-2} > x$.

Сначала находим область допустимых значений: – $(-\infty, -2]\cup[1, +\infty)$. Далее рассмотрим два исчерпывающих случая: 1) $x \leq -2$ и 2) $x \geq 1$. В первом случае неравенство очевидным образом верно при любых x, так как слева стоит неотрицательное число, а справа отрицательное. Во втором случае неравенство эквивалентно следующему: $x^2+x-2 > x^2$, и это дает решение $x > 2$. Следовательно, ответ: $(-\infty; -2] \cup (2, +\infty)$.

1.3 Множества

1.3.1 Основные определения и аксиомы

Множество - неопределяемое понятие. Синонимами этого слова являются: совокупность, собрание, коллектив, набор и т. п. *Отношение принадлежности* элемента x множеству M (записывается как $x \in M$) также неопределяемое понятие. При этом термин *элемент* с математической точки зрения эквивалентен термину "множество". Если мы хотим сказать, что элемент x не принадлежит множеству M, то пишем $x \notin M$. Два *множества M и N равны*, если они состоят из одних и тех же элементов, т.е.

$$M = N \quad \Leftrightarrow \quad \forall x (x \in M \Leftrightarrow x \in N).$$

Это одна из аксиом теории множеств. Другие аксиомы являются фактически правилами построения множеств из уже имеющихся. В частности, постулируется существование *пустого множества* $\emptyset$. Это множество не содержит ни одного элемента, т. е. $\forall x \quad \Rightarrow \quad x \notin \emptyset$.

Для множества M постулируется существование *множества $\mathcal{P}(M)$ всех его подмножеств*. При этом множество N называется *подмножеством* множества M, если всякий элемент из N является также и элементом множества M; символически:

$$N \subseteq M \quad \Leftrightarrow \quad \forall x\, (x \in N \Rightarrow x \in M).$$

Кроме этого, с множествами можно осуществлять операции объединения, пересечения, разности и декартова произведения.

- *Объединением множеств* M и N называется множество $M \cup N$, состоящее из всех элементов, принадлежащих либо M, либо N (не исключающее "либо").

- *Пересечением множеств* M и N называется множество $M \cap N$, состоящее из всех элементов, принадлежащих M и N одновременно.

- *Разностью множеств M и N* или *дополнением множества N до множества M* называется множество $M \setminus N$, состоящее из всех элементов, принадлежащих M, но не N.

Упорядоченная пара, или просто *пара* элементов (m, n), это одна из фундаментальных конструкций в математики. Представлять её можно как полочку с двумя местами – первым и вторым. Очень часто в математике неважно как "на самом деле" устроен тот или иной объект, а важны правила обращения с ним. Подобно этому при игре в шахматы совершенно неважно из чего сделаны фигуры и какой они в точности формы, – важны лишь правила игры. Правило обращения с парой одно:

$$(m, n) = (m', n') \quad \Leftrightarrow \quad m = m' \text{ и } n = n'.$$

Далее индукцией можно строить упорядоченные тройки элементов, четверки элементов и т. д.:

$$(m, n, k) = ((m, n), k), \qquad (m, n, k, q) = ((m, n, k), q), \ldots$$

Декартовым произведением $M \times N$ двух множеств M и N называется множество всех пар (m, n), где m пробегает M, а элемент n пробегает N. Существование пары элементов и существование декартова произведения – очередные аксиомы теории множеств.

Заметим, что мы не ставим своей целью перечислить все аксиомы теории множеств (см. [Б]). Для наших целей достаточно будет задаться *универсальным множеством* U, а все другие множества получать как множества элементов $x \in U$, удовлетворяющих некоторому условию $\mathcal{A}\langle x\rangle$. Такое множество будем записывать как $\{x \in U \mid \mathcal{A}\langle x\rangle\}$.

1.3.2 Отношения

Отношением $\mathcal{R}$ на множестве M называется правило, в силу которого по любой упорядоченной паре элементов $a, b \in M$ можно установить, находится ли a в отношении $\mathcal{R}$ к b или нет. Запись $a\mathcal{R}b$ означает, что элемент a находится в отношении $\mathcal{R}$ к элементу b. Приведенное объяснение не является строгим математическим определением, так как ранее не были определены понятия "правила" и "возможность установить". Строгое математическое определение *отношения* $\mathcal{R}$ *между множеством* M *и множеством* N следующее: это упорядоченная тройка (M, N, G), где $G \subseteq M \times N$. При этом множество G называется *графиком отношения* $\mathcal{R}$ и считается, что $m\mathcal{R}n$ тогда и только тогда, когда $(m, n) \in G$. Далее снова речь будет идти об *отношении на множестве* M, это тот случай, когда $N = M$.

Отношение $\mathcal{R}$ называется *рефлексивным*, если $a\mathcal{R}a$ для любого элемента $a \in M$, и называется *транзитивным* , если из соотношений $a\mathcal{R}b$ и $b\mathcal{R}c$ вытекает, что $a\mathcal{R}c$. Говорят, что отношение $\mathcal{R}$ *антисимметрично*, если из того, что a находится в отноше-нии $\mathcal{R}$ к b, и, наоборот, b находится в отношении $\mathcal{R}$ к a, вытекает, что $a = b$.

Частичный порядок на множестве - это рефлексивное, транзитивное и антисимметричное отношение. В подавляющем большинстве случаев это отношение обозначается всем хорошо известным знаком $\leq$ (нестрогого) неравенства; при этом говорят об отношении "быть больше" или "быть меньше". Если для любой пары $a, b \in M$ имеет место одно из двух соотношений $a \leq b$ или $b \leq a$, то $\leq$ называют *отношением линейного порядка*, а $M, \leq$ – линейно упорядоченным множеством.

Вернемся снова к абстрактному отношению $\mathcal{R}$. Его называют *симметричным*, если $a\mathcal{R}b$ тогда и только тогда , когда $b\mathcal{R}a$. Симмметричное, рефлексивное и транзитивное отношение называется *отношением эквивалентности* и очень часто обозначается символом "$\sim$". Например, эквивалентность бесконечно малых величин - это отношение эквивалентности в указанном выше смысле.

Теорема 1. *Пусть " $\sim$ " - отношение эквивалентности на множестве M. Для любого элемента $m \in M$ обозначим через $[m]$ класс эквивалентности, т.е. множество всех элементов $b \in M$ таких, что $m \sim b$. Тогда M разбивается в объединение множеств $[m]$, т.е. $M = \cup_{m\in M}[m]$; причем два класса $[m]$ и $[m']$ либо совпадают, либо не пересекаются. Наоборот, предположим, что $M = \cup_{i\in I}X_i$ - разбиение множества M. Тогда отношение*

$$m \approx m' \Leftrightarrow \exists i \in I : \ m, m' \in X_i$$

является отношением эквивалентности.

Доказательство. Предположим, что классы $[m]$ и $[m']$ имеют общий элемент n. Тогда $m \sim n$ и $m' \sim n$; откуда $n \sim m$ в силу симметричности $\sim$. Если $x \in [m]$ - произвольный элемент, то имеем $m \sim x$. Следовательно, применяя транзитивность к цепочке соотношений $m' \sim n$, $n \sim m$, $m \sim x$, получаем, что $m' \sim x$ и тем самым $x \in [m']$. Доказано включение $[m] \subseteq [m']$; обратное включение доказывается аналогично. Отсюда следует равенство $[m] = [m']$. Итак, два класса либо совпадают, либо не пересекаются. Так как $m \in [m]$ в силу рефлексивности, то первое утверждение теоремы доказано.

Доказываем обратное утверждение. Рефлексивность и симметричность отношения $\approx$ - тривиальность, проверим транзитивность. Предположим, что $m \approx n$ и $n \approx k$. Тогда найдутся такие индексы i и j, что $m, n \in X_i$ и $n, k \in X_j$. В этом случае n - общий элемент множеств X_i и X_j; значит $X_i = X_j$ по определению разбиения. Следовательно, все три элемента m, n, k лежат в одном и том же множестве X_i, поэтому $m \approx k$. $\square$

1.3.3 Отображения

Отображением f множества M в множество N (обозначается $f : M \to N$) называется правило, в силу которого каждому элементу $x \in M$ ставится в соответствие единствен-ный элемент $f(x) \in N$. При этом множество M называется *областью определения*, N - *областью значений*, x - *аргументом*, а $f(x)$ - *значением отображения* f *на элементе* x или *образом элемента* x при отображении f. Как и выше, эта фраза не может служить строгим математическим определением. Строго говоря, *отображение* $f : M \to N$ это отношение (M, N, G) такое, что для любого элемента $m \in M$ найдется единствен-ный элемент $n \in N$ такой, что $(m, n) \in G$ (в этом случае $n = f(m)$). Говорят, что отображение f *взаимно однозначно*, если разным значениям аргумента соответствуют разные значения отображения f. Это эквивалентно следующему условию:

$$\forall x_1, x_2 \in M\, (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

Отображение f называется *отображением "на" (множество N)*, если всякий элемент $y \in N$ имеет *праобраз*, т.е. элемент x такой, что $f(x) = y$. Взаимно однозначное отображение "на" называется *биективным*, или *биекцией*. Если мы сопоставим элементу $x \in M$ сам этот элемент x, то получим *единичное* отображение $Id_M : M \to M$ которое, конечно, будет биекцией.

Композицией отображений $f : M \to N$ и $g : N \to U$ называется отображение $g \circ f : M \to U$ такое, что $g \circ f(x) = g(f(x))$ для всех $x \in M$. Заметим, что композиция подчиняется закону ассоциативности: если кроме f и g имеется еще отображение $h : U \to T$, то

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Действительно, применяя левую и правую часть этого соотношения к элементу $m \in M$, получаем в обоих случаях $h(g(f(x)))$. Заметим также, что *композиция биекций будет снова биекцией* (см. следующую задачу).

Задача 1. Доказать, что композиция отображений "на" (взаимно-однозначных отображений) будет также отображением "на" (взаимно-однозначным отображением).

Задача 2. Доказать, что если $g \circ f = g' \circ f$ и f – отображение "на", то $g = g'$. Симметрично, если $g \circ f = g \circ f'$ и g – взаимно-однозначное отображение, то $f = f'$.

Теорема 2. *Отображение $f : M \to N$ является биекцией в том и только том случае, когда существует отображение $f^{-1} : N \to M$, называемое обратным, такое, что $f \circ f^{-1} = Id_N$ и $f^{-1} \circ f = Id_M$.*

Доказательство. Пусть f – биекция. Определим $g : N \to M$ так, что, если элемент $n \in N$ произволен, то $m = g(n)$ – тот единственный элемент, для которого $f(m) = n$. Легко проверить, что $f \circ g = Id_N$ и $g \circ f = Id_M$, т.е. $g = f^{-1}$.

Наоборот, пусть $f \circ g = Id_N$ и $g \circ f = Id_M$ для некоторого отображения $g : N \to M$. Если $f(m) = f(m')$, то $m = g(f(m)) = g(f(m')) = m'$ и взаимная однозначность следует. Далее, если $n \in N$ – произвольный элемент, то $m := g(n)$ тот элемент из N, для которого $f(m) = n$. Это доказывает, что f – отображение "на". □

1.4 Алгебраические системы

1.4.1 Бинарные операции.

*Операцией (*более точно: *бинарной операцией)* на множестве называется правило, в силу которого любым двум элементам $a, b \in M$ ставится в соответствие третий элемент $a * b$ ($*$ - знак операции; вместо него могут использоваться другие символы , например $+$, или $\cdot$, или $\circ$). Итак, бинарная операция на множестве M – это отображение $M^2 \to M$. Здесь $M^2 = M \times M$ – *декартов квадрат.* Кроме бинарных операций, существуют и *унарные операции* на множестве M - это просто отображения $M \to M$, а также *0-арные операции,* – отображение $\{\emptyset\} \to M$. 0-арные операция это не что иное как выделение конкретного элемента в множестве M. На одном и том же множестве могут рассматриваться несколько операций, каким-либо образом связанных между собой. Например, на множестве целых чисел $\mathbb{Z}$ можно рассматривать операции сложения, умножения, вычитания и т. д. Мы говорим, что подмножество $N \subseteq M$ *замкнуто* относительно операции $*$, если для любых элементов $a, b \in N$ результат $a * b$ также принадлежит N. Аналогично определяется замкнутость относительно унарной опера-ции.

Операция $*$ на M называется *ассоциативной*, если

$$a * (b * c) = (a * b) * c$$

для любых элементов $a, b, c \in M$ и называется *коммутативной*, если

$$a * b = b * a.$$

для любых элементов $a, b \in M$. Элемент $e \in M$ называется *нейтральным* относительно операции $*$ или *единичным*, если

$$a * e = e * a = a$$

для всякого $a \in M$ (если операция $*$ - умножение, то $e = 1$ называют *единицей*; а если $*$ - сложение, то e называют *нулем* и обозначают 0).

Например, сложение - ассоциативная и коммутативная операция на множестве действительных чисел; она имеет нулевой элемент - 0. Умножение на этом же множестве $\mathbb{R}$ также будет ассоциативным и коммутативным и будет обладать нейтральным элементом - единицей. Умножение матриц ассоциативная, но не коммутативная операция. В алгебре и приложениях приходится иметь дело с весьма важными операциями, не являющимися ни ассоциативными, ни коммутативными. Таковой будет операция *коммутирования* матриц: $[A, B] = AB - BA$ (см. главу 2).

Непустое множество M с заданной на нём ассоциативной операцией $*$ называется *полугруппой*. Если, кроме того, существует единичный элемент, то M называется *моноидом*. Полугруппой будет, например, множество всех слов в заданном алфавите; операцией при этом служит приписывание к одному слову другого. Если добавить еще и *пустое слово* e (слово, не содержащее ни одной буквы), то получим моноид, который называется *свободным*. Если алфавит - одна буква x, то этот свободный моноид состоит из слов $e, x, x^2 = xx, x^3 = xxx, \ldots$.

Теорема 1. *Единица в моноиде единственна.*

Доказательство. Пусть e и f - две единицы. Тогда $ef = e$ так как f единица, и $ef = f$ так как e единица. Отсюда получаем: $e = f$ $\square$

Пусть $(M, *, e)$ – моноид. Элемент $b \in M$ называется *обратным* к элементу $a \in M$, если $a*b = b*a = e$. В этом случае пишут $b = a^{-1}$ и называют a *обратимым* элементом. Если операция $*$ – сложение, то вместо a^{-1} пишут $-a$ и называют $-a$ *противоположным* элементом. Например, в $(\mathbb{Z}, +, 0)$ любой элемент имеет противоположный; а в $(\mathbb{Z}, \cdot, 1)$ только элементы ± 1 обратимы.

Теорема 2. *Пусть $(M, \cdot, e)$-моноид. Тогда*

а) *обратный элемент, если он существует, единственен;*

б) *e обратим и $e^{-1} = e$;*

в) *обратный элемент a^{-1} обратим и $(a^{-1})^{-1} = a$;*

г) *если элементы $a, b \in M$ - обратимы, то произведение ab также обратимо и $(ab)^{-1} = b^{-1}a^{-1}$.*

Доказательство. а). Предположим, что b_1, b_2 - обратные элементы к элементу $a \in M$. Тогда $b_1 = b_1e = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2$, где использовано определение нейтрального элемента, ассоциативность и определение обратного элемента. Утверждения б) и в) – тривиальности. Докажем г). Имеем:

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = e.$$

Аналогично доказывается, что в обратном порядке произведение также равно единице e. Остается учесть определение обратного элемента. □

1.4.2 Конструкции над алгебраическими системами

Алгебраической системой называют непустое множество с семейством операций и отношений, заданным на нём. Мы уже рассматривали примеры алгебраических систем: полугруппы, моноиды, частично упорядоченные множества, множества с эквивалентностью. Вот пример более богатой алгебраической системы: $(\mathbb{R}, +, \cdot, 0, 1, \leq)$. Здесь "$+$" и "$\cdot$" – бинарные операции; 0 и 1 – выделенные элементы, которые можно рассматривать как 0-арные операции; кроме того, имеется отношение линейного порядка. Рассмотрим теперь три основных способа построения алгебраических систем из уже имеющихся.

Подсистемы. Пусть M - алгебраическая система и N - непустое подмножество множества M. Скажем, что N является *подсистемой* алгебраической системы M, если N замкнута относительно всех операций (бинарных, унарных, 0-арных и т. д.), а также для любого отношения $\mathcal{R}$ в системе M, на подмножестве N определяется *сужение* $\mathcal{R}_N$ этого отношения:

$$\textit{если} \ \ a, b \in N, \ \textit{то} \quad a\mathcal{R}_N b \Leftrightarrow a\mathcal{R}b.$$

Например, чётные целые числа $2\mathbb{Z}$, – подсистема системы $M = (\mathbb{Z}, +, \cdot, 0, \leq\ )$, но не является подсистемой системы $(\mathbb{Z}, \cdot, 1)$. Нечетные числа $1 + 2\mathbb{Z}$ будут подсистемой в $(\mathbb{Z}, \cdot, 1)$, но уже не являются подсистемой в $(\mathbb{Z}, +)$ и тем более не являются таковой в M.

Если алгебраическая система имеет какое-либо специальное название (например: моноид, группа, кольцо, поле и т. п.), то подсистема такой алгебраической системы называется соответственно подмоноидом, подгруппой, подкольцом, подполем и т. п.

Декартовы произведения. Пусть M и N – алгебраические системы с одинаковым набором операций и без отношений. Тогда декартово произведение множеств $M \times N$ можно превратить в алгебраическую систему с тем же набором операций выполняющихся покомпонентно:

$$(m, n) * (m', n') = (m * m', n * n'), \quad (m, n)^u = (m^u, n^u).$$

Конструкцию декартова произведения можно многократно повторять; аналогично *покомпонентно* определяются операции на произведении n алгебраических систем.

Фактор-системы. Пусть M алгебраическая система, содержащая лишь операции. Предположим, что " $\sim$ " - отношение эквивалентности на M, *согласованное с операциями* на M в том смысле, что, если $m_1 \sim m_1'$ и $m_2 \sim m_2'$ для некоторых элементов из M, то $m_1 * m_2 \sim m_1' * m_2'$ для любой бинарной операции $*$ и $(m_1)^u \sim (m_1')^u$ для любой унарной операции $()^u$. В этом случае *множество* $M/\sim$ *классов эквивалентности* превращается в алгебраическую систему с теми же операциями:

$$[m_1] * [m_2] = [m_1 * m_2] \quad \text{и} \quad [m]^u = [m^u].$$

Корректность определения операций над классами эквивалентности, т.е. независимость результата от представителей классов вытекает как раз из согласованности отношения эквивалентности и операций. Известная всем с детства алгебраическая система {чет, нечет} с операциями чет + чет = чет, чет+нечет=нечет и т. д. является фактически факторизацией системы $(\mathbb{Z}, +, 0)$ по отношению эквивалентности: $z_1 \sim z_2$ тогда и только тогда , когда остатки от деления целых чисел z_1 и z_2 на 2 совпадают. Если заменить в последней фразе число 2 на число 7, т. е. рассматривать остатки от деления на 7, то получается также эквивалентность, факторизация по которой используется нами буквально каждый день, - это система дней недели {пн., вт., ср., чт., пт., сб., вс} с унарными операциями "следующий/предыдущий день недели", которым в $\mathbb{Z}$ соответствуют унарные операции "прибавления/вычитания" единицы.

1.4.3 Морфизмы

Обсудим теперь, как в точности понимать фразу "является фактически" в последнем абзаце предыдущего параграфа. Пусть M и N алгебраические системы с одним и тем же набором операций и отношений. Отображение $f : M \to N$ назовем *морфизмом*, если для любых элементов $a, b \in M$ имеют место следующие соотношения:

$$f(a * b) = f(a) * f(b) \tag{1.2}$$

для любой бинарной операции $*$, и,

$$\textit{если} \quad a\mathcal{R}b, \quad \textit{то} \quad f(a)\mathcal{R}f(b) \tag{1.3}$$

для любого отношения $\mathcal{R}$. Соотношения, аналогичные (1.2), должны иметь место для всех операций, не обязательно бинарных. Например, для унарных операций это выглядит так: $f(a^u) = (f(u))^u$. Морфизм f называется *изоморфизмом*, а системы M и N называются *изоморфными*, если f биекция; причем $a\mathcal{R}b \Leftrightarrow f(a)\mathcal{R}f(b)$ для любого отношения $\mathcal{R}$ этой алгебраической системы и для любых элементов $a, b \in M$. Изоморфные алгебраические системы неотличимы друг от друга с точки зрения алгебры; иными словами все алгебраические свойства одной системы верны во второй алгебраической системе и наоборот. На этом факте основано доказательство неизоморфности алгебраических систем: если найдено алгебраическое свойство одной системы, не имеющее место во второй, то такие системы заведомо не изоморфны.

Заметим, что изоморфизм – отношение эквивалентности на классе всех алгебраических систем с фиксированным набором операций и отношений. Это следует из того, что композиция морфизмов есть морфизм, и обратное отображение к изоморфизму будет также изоморфизмом.

Задача 1. Доказать сформулированные выше утверждения.

1.5 Группы

1.5.1 Определение группы.

Определение 1. *Группой* называется множество G с бинарной операцией "$*$", для которой выполняются следующие три аксиомы:

Г1. Операция "$*$" ассоциативна.

Г2. Существует нейтральный элемент $e \in G$ такой, что $e * g = g * e = g$ для любого элемента $g \in G$.

Г3. Для любого элемента $g \in G$ найдется элемент $g' \in G$ такой, что $g * g' = g' * g = e$.

Если операция $*$ – умножение, то нейтральный элемент e называют единичным и часто обозначают как 1 или 1_G; элемент g' из аксиомы Г3 называют обратным и обозначают g^{-1} (единственность его доказана в теореме 2, §1.4.1). Очень часто знак операции умножения опускают. Если же операция $*$ – сложение, то нейтральный элемент e называют *нулем* и обозначают 0, а элемент g' называют *противоположным к g элементом* и обозначают $-g$. Определение группы можно переформулировать совсем кратко: – моноид, в котором все элементы обратимы. В группе $(G, \cdot)$ разрешимы уравнения $ax = b$ и $xa = b$; первое имеет единственное решение $x = a^{-1}b$, а второе – $x = ba^{-1}$. Если операция в группе G сложение, то решением уравнения $x + a = b$ будет *разность* $x = b - a$, по определению равная $b + (-a)$.

Группа G называется *абелевой*, если операция "$\cdot$" коммутативна. Знак сложения в качестве операции употребляется лишь для абелевых групп.

Примеры: 1) Группа целых чисел по сложению $(\mathbb{Z}, +, 0)$ и группа действительных чисел по сложению $(\mathbb{R}, +, 0)$ – абелевы группы.

2) $\{e\}$ - *единичная группа*, т. е. группа, состоящая только из одного элемента – единицы с очевидным правилом умножения $ee = e$.

3) *Группа знаков* $\{\pm 1\}$ состоит из двух элементов 1 и -1; операция - умножение.

4) Пусть D – тело в пространстве или фигура на плоскости. Рассмотрим множество $SE(D)$ всех движений пространства (плоскости), оставляющих тело D на месте. Операция на $SE(D)$ - композиция, т. е. последовательное выполнение движений. Тогда $SE(D)$ - группа, называемая *группой симметрий* тела (или фигуры) D.

С точки зрения алгебраических систем, группа – множество с тремя операциями: бинарная операция умножения "$\cdot$", унарная операция $^{-1}$ взятия обратного и 0-арная операция выделения единичного элемента e. Поэтому подмножество S группы G называется *подгруппой*, если $e \in S$, и для любых элементов $a, b \in S$ произведение ab, так же, как и элемент a^{-1}, принадлежит S. Всегда имеется по крайней мере две подгруппы - *единичная* и сама группа G. Остальные подгруппы называются *собственными*.

Пусть $(G, \cdot, ^{-1}, e)$ – группа, $a \in G$. Определим *целые степени* элемента a:

$$a^0 = e, \quad a^n = a \cdot a \cdot \ldots \cdot a \ (n \text{ раз}) \ , \ a^{-n} = (a^{-1})^n \quad (n \in \mathbb{N}).$$

Пользуясь индукцией, легко установить следующий факт.

Теорема 1. *Для любых целых чисел z_1, z_2 имеют место равенства:*

$$a^{z_1} \cdot a^{z_2} = a^{z_1+z_2}, \quad (a^{z_1})^{z_2} = a^{z_1 z_2}.$$

Множество всех степеней элемента a образует подгруппу группы G, обозначаемую $\langle a \rangle$ и называемую циклической подгруппой, порожденной элементом a $\square$

Проанализируем $\langle a \rangle$ подробнее.

Случай 1. Не существует натурального числа n такого, что $a^n = e$. В этом случае $a^{z_1} \neq a^{z_2}$, коль скоро $z_1 \neq z_2$, т. е. все элементы

$$\ldots, a^{-2}, a^{-1}, e, \ a, \ a^2, \ a^3, \ldots$$

попарно различны. В этом случае говорят, что $\langle a \rangle$ – *бесконечная циклическая группа*, и a называют *элементом бесконечного порядка*: $\mathrm{ord}(a) = \infty$.

Случай 2. Найдется натуральное число $n \in \mathbb{N}$ такое, что $a^n = e$. Пусть n – наименьшее натуральное число с таким свойством. Тогда элементы $e, \ a, \ a^2, \ldots, \ a^{n-1}$ попарно различны, и

$$\langle a \rangle = \{e, \ a, \ a^2, \ldots, \ a^{n-1}\}.$$

Этот факт следует из того, что если $z \in \mathbb{Z}$ и $z = nq + r$, где $0 \leq r \leq n-1$, то $a^z = a^r$. В этом случае говорят, что *порядок элемента a* равен n (обозначение: $\mathrm{ord}(a) = n$) и *порядок подгруппы* $\langle a \rangle$ также равен n.

Количество элементов в группе G называется *порядком группы* G и обозначается $|G|$.

Обратимся к примерам. Рассмотрим и фиксируем на плоскости какой-либо правильный треугольник Δ. Все движения плоскости, оставляющие этот треугольник на месте, образуют группу симметрий $SE(\Delta)$ относительно операции композиции, – последовательного выполнения движений. В этой группе 6 элементов: повороты на $0, 120$ и 240 градусов (обозначим их Id, r_{120}, r_{240} соответственно) и симметрии относительно медиан (обозначим их s_a, s_b, s_c). Эта группа не абелева, например $r_{120}s_a \neq s_a r_{120}$, ибо первое произведение переводит вершину A в B, а второе - в C . Подмножество H из трех поворотов - подгруппа группы $SE(\Delta)$; при этом $r_{240} = r_{120}^2$, $r_{120}^3 = Id$, и тем самым элемент r_{120} и подгруппа H имеют порядок 3.

Задача 1. Две симметрии относительно двух медиан правильного треугольника порождают группу $SE(\Delta)$.

Задача 2. Описать группу симметрий квадрата, правильного шестиугольника.

Задача 3*. Описать группу симметрий тетраэдра, куба.

Группа G называется *циклической*, если она порождается одним элементом, т. е. состоит из степеней одного элемента. Например, единица порождает группу целых чисел по сложению.

Задача 4. Найти все порождающие элементы группы целых чисел по сложению. Порождают ли элементы 3 и 7 группу $(\mathbb{Z}, +, 0)$?

1.5.2 Группа подстановок.

Обозначим через S_n множество всех биекций $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. В качестве операции на множестве S_n рассмотрим композицию. Эта операция ассоциативна, обладает единичным элементом Id и каждая биекция имеет обратную биекцию (см. § 1.3.3). Следовательно, S_n группа, называемая *группой подстановок на n символах.* Подстановка $\tau \in S_n$ записывается в виде

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \tag{1.4}$$

или более коротко: $\tau = (i_1, i_2, i_3, \dots, i_n)$. Здесь $i_1, i_2, i_3, \dots, i_n$ - попарно различные натуральные числа от 1 до n; причём запись (1.4) означает, что $\tau(j) = i_j$. Всего $n!$ таких подстановок, т. е. порядок группы S_n равен $n!$.

Подстановка, переставляющая лишь два числа i и j, а остальные числа оставляющая на месте, называется *транспозицией* и обозначается (ij). Всего в группе S_n $n(n-1)/2$ транспозиций.

Теорема 2. *Множество всех транспозиций порождает группу S_n.*

Доказательство. Пусть τ – произвольная подстановка. Применяя транспозицию, т.е. умножая τ слева на некоторую транспозицию t_1, элемент 1 поставим на первое место. Далее то же самое проделаем с элементом 2 и т. д. пока последний элемент n не будет поставлен на свое n-ое место. Тем самым мы имеем набор транспозиций $t_1, t_2, \dots, t_m$ таких, что $t_m t_{m-1} \dots t_1 \tau = e$ (e – единичная подстановка). Отсюда $\tau = t_1^{-1} t_2^{-1} \dots t_m^{-1}$, и остается заметить, что $t^{-1} = t$ для любой транспозиции t. □

1.5.3 Знак подстановки.

Мы хотим приписать каждой подстановке $\tau = (i_1, i_2, \dots, i_n)$ знак $\operatorname{sgn}\tau \in \{\pm 1\}$. Назовем *инверсией подстановки* τ пару натуральных чисел k, l таких, что $1 \le k < l \le n$, но $i_k > i_l$. Скажем, что подстановка τ *четная* и будем писать $\operatorname{sgn}\tau = 1$, если количество всех инверсий подстановки τ четно. В случае, если число всех инверсий нечетно, подстановку τ назовем *нечетной* и будем писать $\operatorname{sgn}\tau = -1$. Для дальнейшего понадобится

Лемма 1. *При умножении подстановки τ на транспозицию $t = (jk)$ четность подстановки меняется.*

Доказательство леммы проводим индукцией по числу $|k-j|$. Основание индукции – случай, когда $t = (j\,j+1)$. Пусть
$\tau = (i_1, i_2, \dots, i_n)$.
Нетрудно подсчитать, что $\tau t = (i_1, \dots, i_{j+1}, i_j, \dots, i_n)$. Если пара $j, j+1$ составляла инверсию в подстановке τ (т.е. $i_j > i_{j+1}$), то в подстановке τt эта пара уже инверсию не составит. Наоборот, если $i_j < i_{j+1}$, то пара $j, j+1$ - инверсия в τt, но не в τ. Что касается остальных пар, то совершенно очевидно, что пара j', k' ($j' < k'$ и либо $j' \ne j$, либо $k' \ne j+1$) образует инверсию в τ тогда и только тогда , когда она образует инверсию в τt.

Предположим теперь, что для транспозиций t таких, что $|k-j| < N$ утверждение леммы доказано и сейчас $|k-j| = N > 1$. Так как $(jk) = (kj)$, то можно считать, что $j < k$. Нетрудно проверить, что $(j,k) = (j\,j+1)(j+1\,k)(j\,j+1)$. Тогда $\tau t = ((\tau(j\,j+1))(j+1\,k))(j\,j+1)$ и, следовательно, по предположению индукции и доказанному выше получаем, что четность подстановки τ меняется три раза; откуда $\operatorname{sgn}(\tau t) = -\operatorname{sgn}\tau$ $\square$

Теорема 3. *Любую подстановку τ можно разложить в произведение транспозиций: $\tau = t_1 t_2 \dots t_k$. Подстановка τ при этом будет четной тогда и только тогда , когда число k четно.*

Доказательство. Первое утверждение доказано в теореме 2. Далее надо учесть равенство $\operatorname{sgn}(e) = 1$ (e - единичная подстановка) и применить лемму 1 к произведению
1
$(\dots(e \cdot t_1)t_2)\dots)t_k = \tau.$ $\square$

Следствие 1. *Для подстановки τ в условии теоремы 3 имеет место равенство* $\operatorname{sgn}\tau = (-1)^k$.

Следствие 2. *Пусть $n > 1$. Отображение $\operatorname{sgn} : S_n \to \{\pm 1\}$ – морфизм группы S_n на группу $\{\pm 1\}$. Ядро этого морфизма, - множество всех четных подстановок, - называется знакопеременной группой и обозначается A_n. Порядок группы A_n равен $n!/2$.*

Доказательство. Пусть подстановки τ и ρ раскладываются в произведение k и l транспозиций соответственно. Тогда произведение $\tau\rho$ разложимо в произведение $k+l$ транспозиций и $\operatorname{sgn}\tau\rho = (-1)^{k+l} = (-1)^k(-)^l = \operatorname{sgn}\tau \cdot \operatorname{sgn}\rho$. Доказано, что sgn – морфизм. Так как $\operatorname{sgn} e = 1$ и $\operatorname{sgn}(12) = -1$, то sgn – отображением "на".

Пусть t – какая-либо транспозиция. Тогда tA_n – множество всех нечетных подстановок, и $S_n = A_n \cup tA_n$ – разбиение. Число элементов в множестве tA_n тоже самое, что и в A_n, так как отображение $\tau \to t\tau$ задает биекцию A_n на tA_n. Отсюда следует, что число элементов в A_n равно половине числа элементов в S_n, т. е. $n!/2$. □

1.6 Кольца, поля

1.6.1 Кольца

Определение 1. Алгебраическая система $(K, +, \cdot)$ с двумя бинарными операциями, умножением и сложением, называется *кольцом*, если

K1. $(K, +)$ – абелева группа;

K2. $(K, \cdot)$ – полугруппа;

K3. операция умножения дистрибутивна относительно сложения, т.е. $a(b+c) = ab+ac$ и $(b+c)a = ba+ca$ для любых элементов $a, b, c \in K$.

Если, к тому же, существует единица 1 в K , т. е. $1a = a1 = a$ для любых $a \in K$, то K называется *кольцом с единицей.* Если $ab = ba$ для любых $a, b \in K$, то K называется *коммутативным кольцом.*

Множество действительных чисел относительно операций сложения и умножения будет коммутативным кольцом с единицей, множество рациональных чисел и множество целых чисел будут подкольцами в $\mathbb{R}$. Также будет коммутативным кольцом с единицей множество всех функций $\mathcal{F}(M) = \{f : M \to \mathbb{R}\}$ относительно операций сложения и умножения функций. В кольце $\mathcal{F}[a, b]$ всех функций, заданных на отрезке $[a, b]$, имеются подкольца непрерывных функций $C[a, b]$ и непрерывно дифференцируемых функций $C^1[a, b]$. В свою очередь, это кольцо содержит подкольцо многочленов $\mathbb{R}[x]$.

Определение кольца классов вычетов. Пусть n – натуральное число. Множество целых чисел разбивается на подмножества

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup \ldots \cup (n - 1 + n\mathbb{Z}).$$

Числа $0, 1, 2, \ldots, n-1$ – все возможные остатки при делении на n. Если $m \in \mathbb{Z}$ и $m = nq + r$, то $m + n\mathbb{Z} = r + n\mathbb{Z}$. Обозначим это множество $\overline{m}$. Итак, *кольцо классов вычетов по модулю n* – это множество $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ со следующими правилами сложения и умножения:

$$\overline{a} + \overline{b} = \overline{a + b}; \quad \overline{a}\overline{b} = \overline{ab}$$

для любых $a, b \in \mathbb{Z}$. Доказательство следующей теоремы опускаем, оно состоит из рутинной проверки аксиом.

Теорема 1. $\mathbb{Z}_n$ *– коммутативное кольцо с нулем* $\overline{0}$ *и единицей* $\overline{1}$.

Вычислим $\overline{2^{100}}$ в кольце $\mathbb{Z}_7$. Имеем: $\overline{2^3} = \overline{1}$; отсюда $\overline{2^{100}} = \overline{2^{99}} \cdot \overline{2} = \overline{2}$, т.е. число 2^{100} дает в остатке 2 при делении на 7.

Элемент k кольца K называется *делителем* 0, если $kb = 0$, либо $bk = 0$ для некоторого элемента $b \in K$, отличного от 0. Элемент k называется *нильпотентным*, если $k^n = 0$ для некоторого натурального n. Элемент $u \in K$ называется *обратимым*, если u обратим в моноиде $(K, \cdot, 1)$, т. е., если существует элемент $d \in K$ такой, что $ud = du = 1$.

Задача 1. Нильпотентный элемент является делителем 0 и делитель 0 не может быть обратимым элементом.

Предложение 1. *Обратимые элементы кольца образуют группу.*

Доказательство. Утверждение является следствием теоремы 2, §1.4. □

1.6.2 Поля

Определение 2. Ненулевое коммутативное кольцо с единицей называется *полем*, если любой его ненулевой элемент обратим.

Чаще всего используемые поля в математике и приложениях – поля рациональных, действительных и комплексных чисел. Полем является также множество всех рациональных функций $\mathbb{R}(x)$. Алгебраическая система {чет., нечет.} – поле из двух элементов. Обобщим этот пример.

Теорема 2. *Кольцо* $\mathbb{Z}_n$ *будет полем в том и только том случае, когда* n *простое число.*

Доказательство. Если $n = k \cdot m$ для натуральных чисел k и m меньших чем n, то $\overline{k} \cdot \overline{m} = \overline{0}$, причем элементы $\overline{k}$ и $\overline{m}$ ненулевые. Следовательно, $\mathbb{Z}_n$ не является полем. Наоборот, если n – простое число, и $\overline{m} \in \mathbb{Z}_n$ – ненулевой элемент, то натуральное число m взаимно просто с n; тем самым найдутся целые числа a, b с условием $ma + nb = 1$ (здесь мы пользуемся свойством НОД двух чисел – возможности его представления в виде линейной комбинации, доказательство которого см. в главе "Комплексные числа и многочлены", [Д]). Тогда $\overline{ma} = \overline{1}$, и поэтому элемент $\overline{m}$ обратим в кольце $\mathbb{Z}_n$. Следовательно, доказано, что $\mathbb{Z}_n$ – поле. □

Подмножество T поля P называется *подполем*, а P называется *расширением поля* T, если $1_P \in T$ и для любых элементов $a, b \in T$ элементы $a+b, a \cdot b, -a$ и a^{-1} (если $a \neq 0$) также принадлежат T. Проблема расширения полей связана с необходимостью решать уравнения, не разрешимые в исходном поле. Например, уравнение $x^2 = 2$ не имеет решения в поле $\mathbb{Q}$, но в расширении $\mathbb{R}$ и даже в расширении $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \sqrt{2}\mathbb{Q}$ уже имеет решение. Мы знаем, что уравнение $x^2+1=0$ не имеет решения в поле действительных чисел. Это значит, что, если корень квадратный из -1 и существует, то он принадлежит какому-то расширению поля $\mathbb{R}$. Задача построения такого расширения поля $\mathbb{R}$, содержащего $\sqrt{-1}$, решается в следующем параграфе.

1.7 Поле комплексных чисел

1.7.1 Конструкция.

Комплексным числом называется выражение вида $z = x + iy$, где x и y - действительные числа, а i - новое число, называемое *мнимой единицей.* Мнимую единицу иногда записывают в виде $i = \sqrt{-1}$, имея в виду то, что $i^2 = -1$, как мы потом увидим. Число x называется *действительной частью* комплексного числа z и обозначается $Re\, z$, а y называется *мнимой частью* комплексного числа z и обозначается $Im\, z$. Комплексное число z полностью определяется своей действительной и мнимой частью, т. е. будем считать, что $x + iy = x' + iy'$ тогда и только тогда , когда $x = x'$ и $y = y'$ одновременно. Комплексные числа вида $x + i0$ обозначаем просто как x и называем действительными, комплексные числа вида $0 + iy$ обозначаем iy и называем *чисто мнимыми.* Комплексное число z изображается вектором на декартовой плоскости, идущим из начала координат в точку с координатами (x, y). Множество всех комплексных чисел будем обозначать $\mathbb{C}$ и называть *комплексной плоскостью.* (см. рис. 1 далее).

Определим операции сложения и умножения: пусть $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ – произвольные комплексные числа. Полагаем:

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

Мы видим, что комплексные числа складываются как векторы и, поэтому $(\mathbb{C}, +)$ – абелева группа. Более того имеет место следующая теорема.

Теорема 1. *Множество комплексных чисел образует поле, в котором нулевой элемент* – $0 = 0+i0$*; единичный элемент* – $1 = 1+i0$*; противоположным комплексным числом к числу* $z = x+iy$ *будет* $-z = (-x)+i(-y)$*, и обратным комплексным числом к ненулевому числу* z *будет* $z^{-1} = \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2}$.

Доказательство. Как уже было сказано, $(\mathbb{C}, +)$ - абелева группа. Ассоциативность и коммутативность произведения, а также дистрибутивность проверяются непосредственно. Далее, $(x+iy)(1+i0) = (x \cdot 1 - y \cdot 0) + i(x \cdot 0 + y \cdot 1) = x + iy$, откуда следует нейтральность элемента $1 + i0$ относительно умножения. Установим справедливость последнего утверждения. Пусть $z = x + iy$ – ненулевое комплексное число. Тогда либо $x \neq 0$, либо $y \neq 0$, и поэтому величина $x^2 + y^2$ также не равна 0. Имеем:

$$(x + iy)(\frac{x}{x^2 + y^2} + i\frac{-y}{x^2 + y^2}) =$$
$$= \left(\frac{x^2}{x^2 + y^2} - \frac{y(-y)}{x^2 + y^2}\right) + i\left(\frac{x(-y)}{x^2 + y^2} + \frac{yx}{x^2 + y^2}\right) = 1 + 0i$$

□

Заметим, что отображение $\mathbb{R} \to \mathbb{C}$, переводящее действительное число x в комплексное число $x + i0$, *сохраняет операции сложения и умножения* в следующем смысле:

$$(x_1 + i0) + (x_2 + i0) = (x_1 + x_2) + i0; \qquad (x_1 + i0)(x_2 + i0) = x_1x_2 + i0.$$

Эти равенства верны для любых действительных чисел x_1,x_2. Именно это свойство даёт нам право отождествлять действительное число x с комплексным числом $x + i0$, что далее мы и будем делать. Более того, будем отождествлять *чисто мнимое число* iy с комплексным числом $0 + iy$.

Следствие 1. *Комплексное число i – корень уравнения $z^2 + 1 = 0$.*

Доказательство. Действительно,

$$i^2 = (0 + 1i)(0 + 1i) = (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 1 \cdot 0)i = -1 + 0i = -1$$

□

Отображение $\mathbb{C} \to \mathbb{C}$, сопоставляющее комплексному числу $z = x + iy$ *сопряженное комплексное число* $\overline{z} = x - iy$, называется *операцией сопряжения*. Геометрический смысл этой операции – отражение относительно действительной оси (см. рис. 1)

Рис. 1. Поле комплексных чисел

Свойства операции сопряжения. *Для любых комплексных чисел $z = x + iy, z_1, z_2$ справедливы следующие равенства:*

а) $\overline{z} = z \;\Leftrightarrow\; z \in \mathbb{R}$*;*

б) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ *и* $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$*;*

в) $\overline{\overline{z}} = z$*;*

г) $z\overline{z} = x^2 + y^2$*.*

Задача 1. Доказать свойства а)-г). Доказать, что сопряжение – изоморфизм поля $\mathbb{C}$ на себя, оставляющий поле действительных чисел неподвижным.

1.7.2 Показательная форма записи комплексных чисел

Пусть $z = x+iy$ - ненулевое комплексное число, представленное вектором на комплексной плоскости. Угол φ, на который надо повернуть действительную ось до совмещения с вектором z, называется *аргументом комплексного числа* z и обозначается $\arg z$. Аргумент нуля неопределен. Можно считать областью изменения аргумента все действительные числа, тогда аргумент определен неоднозначно, с точностью до целого кратного 2π. Если ограничить область изменения аргумента полуинтервалом $(0, 2\pi]$, то получается однозначность, но теряется непрерывность изменения аргумента.

Квадратный корень величины $x^2 + y^2$ называется *модулем* комплексного числа z и обозначается $|z|$. Геометрически модуль комплексного числа - это длина вектора, изображающего комплексное число z. Отметим привычные свойства модуля. В начале заметим, что если $z = x + 0\mathbf{i}$, то $|z| = \sqrt{x^2} = |x|$ – "обычный" модуль.

Свойства модуля. *Для любых комплексных чисел* z*,* z_1*,* z_2 *верно:*

а) $|z_1 z_2| = |z_1||z_2|$*;*

б) $|z_1/z_2| = |z_1|/|z_2|$*;*

в) *(неравенство треугольника)* $|z_1 + z_2| \le |z_1| + |z_2|$*;*

г) $z\overline{z} = |z|^2$*;*

д) $|z| = 0$ *тогда и только тогда ,когда* $z = 0$*.*

Итак, для ненулевого комплексного числа $z = x + iy$ обозначим через r и φ модуль и аргумент соответственно (см. рис. 1). Тогда

$$\begin{cases} x = r\cos\varphi \\ y = r\sin\varphi \end{cases} \qquad \text{и} \quad z = r(\cos\varphi + i\sin\varphi)$$

– *тригонометрическая форма комплексного числа* z. Удобно обозначать комплексное число $\cos\varphi + i\sin\varphi$ как $e^{i\varphi}$. Тогда получаем *показательную форму записи:* $z = re^{i\varphi}$. Более того, имеет смысл определить *комплексную экспоненту* e^z (или $\exp(z)$) как комплексное число $e^x(\cos y + i\sin y)$. Заметим, что, если $z = x$ - действительное число, то $e^z = e^x$, где справа стоит привычная действительная экспонента. Естественность определения и обозначения комплексной экспоненты подтверждают свойства а)-в) из следующего списка.

Свойства комплексной экспоненты. *Для любых комплексных чисел z,z_1,z_2, любых действительных чисел φ, φ_1, φ_2 и для любого целого числа m имеют место равенства:*

а) $e^{z_1+z_2} = e^{z_1}e^{z_2}$, *в частности* $e^{i(\varphi_1+\varphi_2)} = e^{i\varphi_1}e^{i\varphi_2}$, *т. е. при умножении аргументы комплексных чисел складываются;*

б) $e^{z_1-z_2} = e^{z_1}/e^{z_2}$, *в частности* $e^{i(\varphi_1-\varphi_2)} = e^{i\varphi_1}/e^{i\varphi_2}$*;*

в) $(e^z)^m = e^{mz}$*;*

г) $e^{-z} = \frac{1}{e^z}$*;*

д) $|e^{i\varphi}| = 1$, *т. е. комплексное число $e^{i\varphi}$ лежит на единичной окружности;*

е) $e^{i(\varphi+2\pi)} = e^{i\varphi}$, *т. е. комплекснозначная функция $e^{i\varphi}$ действительного аргумента φ является периодической функцией с периодом 2π.*

Доказательство. Несмотря на обилие утверждений, проверки требует только утверждение а). Имеем:

$$\begin{gathered} e^{i\varphi_1}e^{i\varphi_2} = (\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) = \\ = (\cos\varphi_1\cos\varphi - \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2) = \\ = \cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2) = e^{i(\varphi_1+\varphi_2)}. \end{gathered}$$

Отсюда вытекает равенство $e^{z_1+z_2} = e^{z_1}e^{z_2}$. Равенство б) верно в силу $e^{z_2}\cdot e^{z_1-z_2} = e^{z_2+z_1-z_2} = e^{z_1}$, где применено а).

Свойства в) и г) являются прямыми следствиями доказанного равенства, а свойства д) и е) - следствия основного тригонометрического тождества и периодичности функций $\cos x$ и $\sin x$. □

Следствие (формула Муавра). *Для любых $\varphi \in \mathbb{R}$ и $n \in \mathbb{Z}$ верно равенство*

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi.$$

Доказательство. Имеем:

$$(\cos\varphi + i\sin\varphi)^n = (e^{i\varphi})^n = e^{in\varphi} = \cos n\varphi + i\sin n\varphi$$

□

1.7.3 Решение квадратных уравнений над $\mathbb{C}$.

Лемма 1. *Для любого комплексного числа* $D = re^{i\varphi}$ $(r, \varphi \in \mathbb{R}; r > 0)$ *числа* $\pm\sqrt{r}e^{i\varphi/2}$ *являются корнями уравнения* $z^2 = D$.

Доказательство. Используя свойства комплексной экспоненты убеждаемся, что указанные комплексные числа, обозначим их z_1, z_2, удовлетворяют соотношению $z_1^2 = z_2^2 = D$. Далее, $z^2 - D = (z - z_1)(z + z_1)$. Отсюда следует, что $z_{1,2}$ – все корни уравнения $z^2 = D$. □

Пусть дано квадратное уравнение

$$az^2 + bz + c = 0 \quad (a, b, c \in \mathbb{C}\,;\ a \neq 0) \tag{1.5}$$

Величина $D = b^2 - 4ac$ называется *дискриминантом уравнения* (1.5). Выделением полного квадрата приведем уравнение (1.5) к равносильному уравнению

$$\left(z + \frac{b}{2a}\right)^2 = \frac{D}{4a^2} \tag{1.6}$$

Обозначим через $\pm\sqrt{D}$ - комплексные квадратные корни из числа D. Тогда решением уравнения (1.6), а значит и равносильного ему уравнения (1.5) будут два комплексных числа

$$z_{1,2} = \frac{-b \pm \sqrt{D}}{2a}.$$

Мы видим, что любое квадратное уравнение разрешимо над полем комплексных чисел. Справедливо намного более общее утверждение

Основная теорема алгебры комплексных чисел. *Любой многочлен, не равный константе, имеет корень над полем комплексных чисел.*

Доказательство этой теоремы отложим до главы "Комплексные числа и многочлены" (см. также [B], глава 3, §3).

Глава 2

Системы линейных уравнений, матрицы, определители

В этой главе через K обозначается некоторое поле. Если речь идет о геометрической интерпретации, то подразумевается $K = \mathbb{R}$ – поле действительных чисел. Эта глава и последующая глава о линейных пространствах занимают центральное положение в данном пособии. Очень часто при изложении алгебраические вычисления чередуются с геометрической и физической интерпретацией.

2.1 Системы линейных уравнений малых порядков

Определение системы линейных уравнений и сопутствующих понятий будут даны в следующем параграфе. Здесь же мы рассмотрим линейное уравнение с одной и двумя неизвестными и систему двух линейных уравнений с двумя неизвестными.

2.1.1 Одно уравнение с одним неизвестным

Прежде всего, что означает слово "линейный"? Функция $y(x) = kx$ линейная ($k \in K$ – фиксированный элемент). Под этим подразумевается, что для любых элементов x_1, x_2 и λ имеют место следующие соотношения

(Л1) $y(x_1 + x_2) = y(x_1) + y(x_2)$;

(Л2) $y(\lambda x) = \lambda y(x)$

Задача 1. Докажите, что если функция $y(x)$ обладает свойствами (Л1) и (Л2), то она имеет вид $y(x) = kx$ для подходящего $k \in K$.

Задача 2. Какие из следующих функций над $\mathbb{R}$ линейны: а) $y = |x|$,
б) $y = x/\pi$, в) $y = e^x$, г) $y = 0$?

Общий вид линейного уравнения с одним неизвестным x следующий:

$$ax = b \tag{2.1}$$

Здесь a и b какие-то элементы поля K, называемые *коэффициентами.* Мы ищем все решения уравнения (2.1), т. е. такие элементы поля K, при подстановке которых вместо x, получается слева в (2.1) то же число, что и справа. Сформулируем ответ.

Случай 1: $a \neq 0$. Тогда

$$ax = b \Leftrightarrow a^{-1}(ax) = a^{-1}b \Leftrightarrow (a^{-1}a)x = a^{-1}b \Leftrightarrow 1 \cdot x = a^{-1}b \Leftrightarrow x = a^{-1}b \tag{2.2}$$

Итак, решение в этом случае существует, единственно и задается формулой $x = b/a$. В цепочке эквивалентностей (2.2) мы воспользовались существованием обратного элемента a^{-1}, ассоциативностью произведения, свойством единичного элемента. Позже, решая системы n уравнений с n неизвестными, мы обнаружим поразительную аналогию с выводом решения этого простейшего уравнения (см. §2.8). Обсуждается такое уравнение в общем случае в § 1.5, после определения группы.

Случай 2: $a = 0$, но $b \neq 0$. Тогда решений нет или как мы будем говорить *множество решений пусто.*

Случай 3: $a = b = 0$. Тогда множество решений - всё поле K.

Подведем итог: *решений у уравнения (2.1) может не быть* ($a = 0, b \neq 0$)*, может быть одно решение* ($a \neq 0$) *и может быть множество решений, заполняющих всё поле* K ($a = b = 0$)*.*

2.2 Одно уравнение с двумя неизвестными

Одно уравнение с двумя неизвестными x и y имеет вид:

$$ax + by = c \tag{2.3}$$

В случае $K = \mathbb{R}$ решения уравнения (2.3) можно интерпретировать точками на плоскости с декартовой системой координат Oxy.

Если $a = b = 0$, а $c \neq 0$, то решений нет. Если $a = b = c = 0$, то решения заполняют всю "плоскость" K^2.

Рассмотрим оставшийся случай, когда один из коэффициентов a или b не равен 0. Тогда, в случае $K = \mathbb{R}$, множество решений уравнения (2.3) образует прямую на плоскости. Действительно, если $b \neq 0$, то уравнение (2.3) эквивалентно известной функциональной зависимости $y = -\frac{a}{b}x - \frac{c}{b}$, графиком которой является прямая. Если же $b = 0$, то $a \neq 0$, и уравнение (2.3) эквивалентно следующему уравнению: $x = -\frac{c}{a}$ – прямая параллельная оси Oy. В общем случае можно дать аналогичный ответ: если $b \neq 0$, то $\left\{(x, -\frac{a}{b}x - \frac{c}{b}) \mid x \in K\right\}$ – множество всех решений. Здесь x "свободно" пробегает поле K. Если же $b = 0$, то $\{(-\frac{c}{a}, y) \mid y \in K\}$ – множество решений и здесь уже y – свободная неизвестная.

2.2.1 Система 2×2

Перейдем теперь к линейной системе двух уравнений с двумя неизвестными x и y. Общий вид её следующий:

$$\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{cases} \tag{2.4}$$

Фигурная скобка слева в (2.4) заменяет союз "и". Нам надо найти все пары чисел (x, y), при подстановке которых в первое **и** во второе уравнение системы (2.4) получаются верные числовые равенства.

Решим систему (2.4) методом исключения одного неизвестного, скажем y. Для этого первое уравнение умножим на b_2, второе – на b_1, и вычтем из полученного первого уравнения получившееся второе уравнение:

$$(a_1b_2 - a_2b_1)x = c_1b_2 - c_2b_1 \tag{2.5}$$

Уравнение (2.5) является следствием системы (2.4). Это значит, что равенство (2.5) верно, коль скоро пара (x, y) – решение системы (2.4). Если внимательно присмотреться к коэффициентам уравнения (2.5), то можно заметить, что как первый, так и второй, составлены по одному и тому же правилу.

Число $a_1b_2 - a_2b_1$ назовем *определителем* 2×2 и будем записывать так:

$$a_1b_2 - a_2b_1 = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}. \tag{2.6}$$

Определитель (2.6) называют также *определителем системы* (2.4). Будем обозначать этот определитель прописной греческой буквой Δ (дельта). Заметим, что правая часть уравнения (2.5) также является определителем. Обозначим его следующим образом:

$$\Delta_x = c_1b_2 - c_2b_1 = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}.$$

Аналогично, обозначим

$$\Delta_y = c_2a_1 - c_1a_2 = \begin{vmatrix} a_1 & a_2 \\ c_2 & c_2 \end{vmatrix}.$$

При исключении неизвестной y из системы (2.4) мы приходим к уравнению $\Delta \cdot y = \Delta_y$. Уравнение (2.5) и аналогичное ему уравнение $\Delta y = \Delta_y$ мы уже знаем как решать (см. §2.1.1).

Случай 1: $\Delta \neq 0$. Тогда уравнение (2.5) и уравнение $\Delta \cdot y = \Delta_y$ имеют единственное решение

$$x = \frac{\Delta_x}{\Delta}, \quad y = \frac{\Delta_y}{\Delta}. \tag{2.7}$$

Оказывается, что (2.7) – единственное решение системы (2.4). Эта есть **правило Крамара** для системы 2×2. В общем случае правило Крамара доказано в §2.7. Мы сформулировали правило Крамара, но доказали лишь единственность решения (2.7), а сам факт, что (2.7) - решение системы (2.4) пока не доказан. Установить это можно прямой проверкой:

$$a_1x + b_1y = a_1\frac{\Delta_x}{\Delta} + b_1\frac{\Delta_y}{\Delta} = \frac{1}{\Delta}(a_1(c_1b_2 - c_2b_1) + b_1(c_2a_1 - c_1a_2)) =$$
$$= \frac{1}{\Delta}(a_1c_1b_2 - b_1c_1a_2) = \frac{1}{\Delta}(a_1b_2 - b_1a_2)c_1 = c_1.$$

Аналогично проверяется, что пара чисел $(\frac{\Delta_x}{\Delta}, \frac{\Delta_y}{\Delta})$ является решением и второго уравнения системы (2.4).

Случай 2: $\Delta = 0$, но либо $\Delta_x \neq 0$, либо $\Delta_y \neq 0$. Тогда либо уравнение (2.5) (если $\Delta_x \neq 0$), либо аналогичное ему уравнение $\Delta \cdot y = \Delta_y$ (если $\Delta_y \neq 0$) не имеет решения. Отсюда немедленно вытекает, что система (2.4) также не имеет решений.

Случай 3: $\Delta = \Delta_x = \Delta_y = 0$. Конечно, в этом случае уравнение (2.5) и уравнение $\Delta y = \Delta_y$ имеют решением любое число. Но это не значит, что любая пара чисел является решением системы (2.4).

Задача 3. Приведите пример, подтверждающий последнее высказывание.

Если $a_1 = b_1 = 0$ и $c_1 \neq 0$, то первое уравнение, а, значит, и вся система (2.4) решений не имеет. Если же $a_1 = b_1 = c_1 = 0$, то первое уравнение можно отбросить. Под этим понимается, что при отбрасывании нулевого уравнения, получается система, эквивалентная исходной. После отбрасывания нулевого уравнения остаемся с одним уравнением с двумя неизвестными (см. §2.2). По этой причине полагаем далее, что либо a_1 либо b_1 не равен 0, а также либо a_2 либо b_2 не равен 0.

Перепишем равенства $\Delta = 0$ и $\Delta_x = 0$ в виде пропорций: $\frac{a_2}{a_1} = \frac{b_2}{b_1}$ и $\frac{b_2}{b_1} = \frac{c_2}{c_1}$. Так как либо $a_1 \neq 0$, либо $b_1 \neq 0$, то общее отношение $\lambda = \frac{a_2}{a_1} = \frac{b_2}{b_1} = \frac{c_2}{c_1}$ определено, тем самым число λ таково, что $a_2 = \lambda a_1, b_2 = \lambda b_1$ и $c_2 = \lambda c_1$. А это означает, что, если мы ко второму уравнению системы (2.4) прибавим первое уравнение, предварительно умноженное на $-\lambda$, то придем к системе вида

$$\begin{cases} a_1x + b_1y = c_1; \\ 0 \cdot x + 0 \cdot y = 0 \end{cases}. \tag{2.8}$$

Система (2.4) может быть получена из системы (2.8) *обратным преобразованием*: надо ко второму уравнению системы (2.8) прибавить первое, умноженное на $\frac{1}{\lambda}$. Это значит, что системы (2.4) и (2.8) имеют одно и тоже множество решений, или как мы будем говорить, они *эквивалентны.* Система (2.8) эквивалентна уравнению $a_1x+b_1y=c_1$.

Мы полностью решили систему 2×2. Подведем итог. В случае отличия от нуля определителя системы, – $\Delta\neq0$, решение единственно. Если же $\Delta=0$, то решений может не быть вовсе, либо может быть бесконечное множество решений, заполняющих "прямую" на плоскости K^2. В исключительном, но также возможном случае, равенства нулю всех коэффициентов, множество решений заполняет всю "плоскость" K^2.

Мы не случайно в последнем абзаце прибегнули к геометрии. Если есть возможность какой-либо математический объект истолковать геометрически, то этой возможностью надо обязательно воспользоваться. То, что такая возможность есть для системы 2×2 показывает следующая таблица (в этой таблице предполагается, что оба коэффициента a_1, b_1 также как и a_2, b_2 не могут быть одновременно равны 0, а также $K=\mathbb{R}$).

Аналитический язык	*Геометрический язык*
пара чисел (x,y)	точка $P(x,y)$ на плоскости Oxy
уравнение $a_1x+b_1y=c_1$	прямая на плоскости Oxy
Решение системы (2.4)	Поиск пересечения двух прямых – $\ell_1: a_1x+b_1y=c_1$ и $\ell_2: a_2x+b_2y=c_2$
Решение системы (2.4) единственно ($\Leftrightarrow\Delta\neq0$)	Прямые ℓ_1 и ℓ_2 пересекаются в одной точке
Система (2.4) решений не имеет ($\Delta=0$, но $\Delta_y\neq0$ либо $\Delta x\neq0$)	Прямые ℓ_1 и ℓ_2 параллельны
Система (2.4) имеет бесконечное множество решений	Прямые ℓ_1 и ℓ_2 совпадают.

2.3 Метод Гаусса решения систем линейных уравнений.

Система m линейных уравнений с n неизвестными $x_1,x_2,\dots,x_n$ имеет вид:

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n & =b_1\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n & =b_2\\ \dots\dots\dots\dots\dots\dots\dots\dots & \dots\\ a_{m1}x_1+a_{m2}x_2+\ldots+a_{mn}x_n & =b_m\end{cases} \tag{2.9}$$

Здесь $a_{ij}\in K$ – *коэффициент* системы, стоящий в i-ом уравнении при j-ой неизвестной. Числа $b_1,b_2,\dots,b_m$ называют *правой частью.* Если все они равны 0, то систему называют *однородной. Решением* системы (2.9) называется строка n чисел при подстановке которой в (2.9) вместо $x_1,x_2,\dots,x_n$ получается верное числовое равенство в каждом из уравнений. Система (2.9) называется *совместной*, если она имеет хотя бы одно решение и называется *несовместной* в противном случае. Совместная система называется *определенной*, если она имеет в точности одно решение и называется *неопределенной*, если имеет более одного решения. Две системы линейных уравнений называются *эквивалентными*, если их множества решений совпадают.

Решать систему (2.9) мы будем *методом последовательного исключения неизвестных.* Этот метод также называется иначе *методом Гаусса.* Для этого шаг за шагом будем преобразовывать систему, все время переходя к эквивалентной, но более просто устроенной. Сначала обозначим набор возможных шагов.

Элементарными преобразованиями системы линейных уравнений называются:

(1 тип) прибавление к одному уравнению другого, умноженного на какое-либо число;

(2 тип) перестановка двух уравнений;

(3 тип) умножение какого-либо уравнения системы на ненулевое число;

(4 тип) присоединение или отбрасывание нулевого уравнения.

Любое элементарное преобразование обратимо, то есть существует элементарное преобразование, применение которого к полученной системе, возвращает ее в исходное состояние. Действительно, для элементарного преобразования первого типа (к i-тому уравнению прибавили j-ое, умноженное на λ) обратным преобразованием будет вычитание из i-го уравнения j-го, умноженного на λ. Это равносильно прибавлению к i-му уравнению j-го, умноженного на $-\lambda$. Для перестановки уравнений обратным преобразованием будет сама эта перестановка. Для умножения на ненулевое число k обратным преобразованием будет умножение на число k^{-1}. Для присоединения (отбрасывания) нулевого уравнения обратным будет отбрасывание (присоединение) этого же уравнения.

При элементарном преобразовании получается система, эквивалентная исходной. Во-первых, при таком преобразовании получается *следствие системы*, т. е. множество решений новой системы содержит множество решений исходной системы. Далее можно воспользоваться обратимостью элементарных преобразований и получить, что исходная система – следствие новой системы. Следовательно, исходная и новая системы эквивалентны.

Процесс элементарных преобразований имеет конечную цель – ступенчатый вид системы. Система (2.9) имеет *ступенчатый вид*, если первое ненулевое слагаемое каждого последующего уравнения стоит правее, чем первое ненулевое слагаемое предыдущего уравнения.

Теорема 1. *Любую систему линейных уравнений элементарными преобразованиями 1-го и 2-го типов можно привести к ступенчатому виду.*

Доказательство. - индукция по количеству уравнений. При этом заметим, что любая "система" с одним уравнением имеет ступенчатый вид. Это база индукции. Предположим, что утверждение доказано для систем, содержащих менее чем n уравнений и теперь дана система из n уравнений.

Можно считать, что один из коэффициентов $a_{11}, a_{21}, \ldots, a_{m1}$ стоящих в первом столбце не равен 0. Иначе переходим к следующему столбцу и так далее пока не наткнемся на столбец, имеющий хотя бы один отличный от нуля коэффициент. Если такового не окажется, то есть все $a_{ij} = 0$ и все $b_j = 0$, то доказывать нечего - система уже имеет ступенчатый вид. Итак, пусть $a_{1j} \neq 0$ для некоторого j. Совершив, если нужно (т. е. если $a_{11} = 0$), элементарное преобразование 3 типа – перестановка первого и j-го уравнения, добьемся того, что на месте $(1,1)$ будет стоять не равный нулю коэффициент. Переобозначим коэффициенты так, что именно $a_{11} \neq 0$. Тогда, прибавляя ко второму уравнению первое, умноженное на $-\frac{a_{21}}{a_{11}}$, "занулим" коэффициент, стоящий на месте $(2,1)$. Аналогичными преобразованиями занулим коэффициенты, стоящие на местах $(3,1), \ldots, (m,1)$. Получим следующую систему:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n & = b_1 \\ \quad a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n & = b'_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots \\ \quad a'_{m2}x_2 + a'_{m3}x_3 + \ldots + a'_{mn}x_n & = b'_m \end{cases} \tag{2.10}$$

Применим предположение индукции к подсистеме системы (2.10), полученной из (2.10) вычеркиванием первого уравнения и приведем эту подсистему к ступенчатому виду. Тогда и вся система (2.10) примет ступенчатый вид. □

Задача 1. Найти константу C и натуральное число k такие, чтобы можно было утверждать, что любую систему $n \times n$ можно привести к ступенчатому виду пользуясь $\leq Cn^k$ элементарными преобразованиями.

Задача 2. Составить алгоритм приведения системы к ступенчатому виду с дополнительным условием: ненулевой коэффициент a_{ij} в столбце надо выбирать наибольшим по абсолютной величине. Такой способ важен с точки зрения уменьшения погрешности в вычислениях и называется *методом последовательного исключения неизвестных с выбором главного элемента.*

Исследование системы по ступенчатому виду. Предположим, что система линейных уравнений приведена к ступенчатому виду:

$$\begin{cases} a_{11}x_1 + a_kx_2 + \ldots + a_{1n}x_n & = b_1 \\ \quad a_{2k}x_k + \ldots + a_{2n}x_n & = b_2 \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots \\ \qquad a_{mp}x_p + \ldots & = b_m \end{cases} \tag{2.11}$$

Здесь $x_1, x_k, \ldots, x_p$ – неизвестные, стоящие в углах ступенчатого вида. Их мы будем называть *главными*. Остальные неизвестные (их может и не быть) называются *сво-*

бодными. По определению ступенчатого вида имеем: $1 < k < \ldots < p$. Вообще-то в ступенчатом виде могут присутствовать нулевые уравнения, то есть уравнения вида $0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = 0$. Но их можно отбросить, пользуясь элементарным преобразованием четвертого типа. Обсудим сначала случай, когда система не имеет решения.

Если в процессе приведения к ступенчатому виду или в самом ступенчатом виде встретилось уравнение вида

$$0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = b, \tag{2.12}$$

где $b \neq 0$, то это уравнение не имеет решения, а, значит, и исходная система несовместна.

Считаем далее, что нулевых уравнений в ступенчатом виде, а также уравнений вида (2.11) нет. Число ненулевых уравнений может быть меньше или равно числу неизвестных (то есть $m \leq n$), но не может превосходить n. В самом деле, каждая ступенька имеет ширину ≥ 1, следовательно общая ширина ступенек $\geq m$, а с другой стороны общая ширина ступенек вместе с последней, m-ой не может превосходить n. Отсюда и получаем неравенство $m \leq n$.

Завершает решение системы *обратный процесс.* Это серия элементарных преобразований системы (2.11), позволяющая записать главные неизвестные через свободные в виде *линейной комбинации.* Сначала выражают x_p через все последующие неизвестные, пользуясь последним уравнением:

$$x_p = b_m/a_{mp} - a_{mp+1}/a_{mp}x_{p+1} - \ldots - a_{mn}/a_{mp}x_n$$

(если $p = n$, то это выражение имеет вид: $x_n = b_n/a_{nn}$). Далее, применяя элементарные преобразования 1 типа, зануляют все коэффициенты в (2.11), стоящие над коэффициентом a_{mp} точно также как мы это делали в "прямом" процессе приведения системы к ступенчатому виду (см. доказательство теоремы 1). Затем из получившегося предпоследнего уравнения выражают предпоследнее главное неизвестное через оставшиеся свободные неизвестные и так далее, пока не доберемся до первого главного неизвестного и не выразим его через свободные неизвестные.

Проиллюстрируем эту процедуру обратного процесса на примере системы 3×3 уже приведенной к ступенчатому виду, в котором отсутствуют свободные неизвестные ($a_1 \neq 0$, $b_2 \neq 0$, $c_3 \neq 0$):

$$\begin{cases} a_1x + b_y + c_1z & = d_1 \\ b_2y + c_2z & = d_2 \\ c_3z & = d_3 \end{cases} \Leftrightarrow \begin{cases} a_1x + b_1y & = d_1 - d_3c_1/c_3 \\ b_2y & = d_2 - d_3c_2/c_3 \\ z & = d_3/c_3 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a_1 x &= d_1 - d_3 c_1/c_3 - d_2 b_1/b_2 - d_3 c_2 b_1/(c_3 b_2) \\ y &= d_2/b_2 - d_3 c_2/(c_3 b_2) \\ z &= d_3/c_3 \end{cases}$$

Ответ:

$$\begin{cases} x &= d_1/a_1 - d_3 c_1/(c_3 a_1) - d_2 b_1/(b_2 a_1) - d_3 c_2 b_1/(c_3 b_2 a_1) \\ y &= d_2/b_2 - d_3 c_2/(c_3 b_2) \\ z &= d_3/c_3 \end{cases}$$

Итак, мы видим, что

> *если в ступенчатом виде все неизвестные главные ($m = n$), то система определена. Если же имеются свободные неизвестные, то общее решение получается обратным процессом, выражающим главные неизвестные через свободные.*

При этом свободные неизвестные играют роль параметров, "свободно" и независимо друг от друга пробегающих множество K. В этом случае система неопределена, более того, она имеет бесконечное множество решений, если поле K бесконечно. Исследование системы по ступенчатому виду, как и изложение метода Гаусса закончено.

Задача 3. Определите понятие *размерности* множества решений. Обоснуйте это определение, рассматривая все возможные случаи множества решений системы 3×3.

Задача 4. Рассмотрим в пространстве $Oxyz$ плоскость γ, проходящую через точки $A(1,0,0), B(0,1,0)$ и $C(0,0,1)$. Приведите пример системы 2×3 с множеством решений, заполняющих плоскость γ.

Задача 5. Может ли система линейных уравнений иметь ровно 7 решений? Рассмотреть случаи конечных полей и бесконечных полей отдельно.

Рассмотрим теперь важный частный случай однородной системы. Такая система заведомо совместна, поскольку строка из нулей - $(0, 0, \ldots, 0)$ является её решением. Критерий существования ненулевого решения дает следующая

Теорема 2. *Однородная система имеет ненулевое решение, т.е. является неопределенной в том и только том случае, когда после приведения к ступенчатому виду число ненулевых уравнений меньше, чем число неизвестных. В частности это так, если изначальная однородная система имела число уравнений меньше, чем число неизвестных.*

2.4 Матрицы

Матричная алгебра – один из мощных инструментов всей математики. С таблицами чисел приходилось встречаться каждому (оценки группы студентов по различным предметам, зависимость стоимости нескольких видов продукции от времени и т. д.).

Это и есть матрицы. Заметим, что, работая с программой Excel, мы фактически имеем дело с таблицей в электронном варианте и пользуемся часто терминологией матричного исчисления. Монография [БЛ] посвящена целиком такому исчислению.

2.4.1 Определение матрицы

Всякий, кто хотя бы один раз решал систему линейных уравнений, мог заметить, что в процессе решения сами переменные $x_1, x_2, \ldots, x_n$, а также знаки сложения и равенства в уравнениях системы можно не писать, а лишь подразумевать. То, что остается от системы после выбрасывания всех этих символов называется *расширенной матрицей системы* (2.9), а сами коэффициенты a_{ij} без столбца $b_1, b_2, \ldots, b_n$ составляют *матрицу* системы (2.9) размера $m \times n$. Итак, *матрицей размера* $m \times n$ или $m \times n$-*матрицей* над полем K называется прямоугольная таблица вида

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{pmatrix}, \tag{2.13}$$

где $a_{ij} \in K$. Строго говоря, $m \times n$-матрица, это отображение декартова произведения $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$ в поле K, и a_{ij} – значение этого отображения от пары (i, j). Матрицы будем обозначать прописными латинскими буквами – A, B, C и т. д. Более компактная запись матрицы (2.13) следующая: $A = (a_{ij})_{m \times n}$. Здесь индекс i пробегает от 1 до m, а j изменяется от 1 до n независимо от i. Очень часто ссылку "$m \times n$" на размер матрицы A будем опускать, записывая ее короче: $A = (a_{ij})$. Две *матрицы равны*, если, во-первых, совпадают их размеры, а во-вторых на одинаковых местах стоят равные друг другу элементы.

Задача 1. Записать $n \times n$-матрицу у которой а) $a_{ij} = (-1)^{i+j}$; б) $a_{ij} = \min\{i; j\}$; в) $a_{ij} = \max\{i; j\}$.

Задача 2. Сколько матриц размера $m \times n$ можно составить из k попарно различных чисел, которые можно выбирать в качестве коэффициентов a_{ij}.

Места, на которых располагаются коэффициенты матрицы, нумеруются парой индексов - (i, j) так, что a_{ij} - это (i, j)-*й коэффициент матрицы* A, а

$$(a_{i1}, a_{i2}, \ldots, a_{in}); \qquad \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

называются i-*й строкой* и j-*м столбцом* той же матрицы. Может случиться так, что матрица A содержит ровно одну строку (один столбец). Тогда такая матрица называется *строкой* (*столбцом*), а число n (число m) её (его) длиной. Крайний случай, –

матрица размера 1×1. Тогда ее единственный коэффициент в круглые скобки можно не заключать, и такую матрицу можно отождествлять с элементом поля K. Множество всех матриц над полем K будем обозначать $\mathcal{M}at\,(K)$. Аналогично, множество всех матриц, у которых коэффициенты, скажем, целые числа, обозначается $\mathcal{M}at\,(\mathbb{Z})$. Множество матриц фиксированного размера $m \times n$ обозначается $\mathcal{M}at_{\,m\times n}(K)$. Следовательно,

$$\mathcal{M}at\,(K) = \bigcup_{m,n=1}^{\infty} \mathcal{M}at_{\,m\times n}(K).$$

2.4.2 Сложение матриц и умножение на число

Множество $\mathcal{M}at\,(K)$ образует крайне важную и полезную во многих отношениях алгебраическую систему относительно операций сложения, умножения и транспонирования. К изучению этой системы мы и переходим.

Определение 1. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ – две $m \times n$ - матрицы, а $r \in K$.

Суммой матриц A и B называется $m \times n$ - матрица $A + B$, (i, j)-ый коэффициент которой равен $a_{ij} + b_{ij}$.

Произведение матрицы A на элемент $r \in K$ определяется также покомпонентно: $Ar = rA = (ra_{ij})$. Иными словами Ar так же, как и rA, – матрицы того же размера $m \times n$, и на (i, j)-м месте у них стоит коэффициент ra_{ij}.

Не случайно в определении 1 мы написали два произведения Ar и rA. В данном случае они совпадают; однако произведение двух матриц, как мы увидим позже, зависит от порядка сомножителей. Заметим также, что сложение матриц разных размеров не определяется.

Отметим фундаментальные свойства только что определенных операций сложения и произведения на число.

Ассоциативность сложения: выполняется равенство $A + (B + C) = A + (B + C)$ для любых трех матриц A, B, C одинакового размера.

Коммутативность сложения: $A + B = B + A$ для любых $A, B \in \mathcal{M}at_{\,m\times n}(K)$.

Нулевая матрица: Это матрица, у которой на всех местах стоят нули. Обозначается нулевая матрица также как и число ноль - 0. Нулевая матрица является *нейтральным элементом* по отношению к сложению, то есть $A + 0 = 0 + A = A$ для любой матрицы A. (Подразумевается, что матрицы имеют одинаковый размер).

Противоположная матрица к данной матрице A: Так называется матрица $-A = (-a_{ij}) = (-1) \cdot A$, очевидно имеющая тот же размер, что и исходная матрица A. Имеет место тождество: $A + (-A) = 0$.

Ассоциативность умножения на числа: $(rs)A = r(sA)$ для любых $r, s \in K$ и $A \in \mathcal{M}at\,(K)$. Аналогично: $A(sr) \equiv (As)r$.

Дистрибутивность: $r(A+B) \equiv rA + rB$ и $(r+s)A \equiv rA + sA$

Следствие. *Множество матриц $\mathcal{M}at_{m\times n}(K)$ образует абелеву группу относительно сложения.*

Задача 3. Доказать перечисленные выше свойства матриц.
(Указание: – опираться на соответствующие свойства сложения и умножения элементов поля).

Задача 4. Написать общую формулу решения (решений) уравнения $rA + sX = C$. Здесь A, C - данные матрицы размера $m \times n$; $r, s \in K$ - данные элементы поля K, а $X \in \mathcal{M}at_{m\times n}(K)$ - переменная.

Как и в любой абелевой группе, комбинацию $A + (-B)$ записываем короче как $A - B$ и называем *разностью матриц A и B*.

Задача 5. Коммутативна (ассоциативна) ли операция вычитания
$(A, B \longrightarrow A - B)$? Имеется ли у нее нейтральный элемент (правый нейтральный элемент)?

2.4.3 Транспонирование матриц

Так называется операция над $m \times n$-матрицей A, превращающая ее в $m \times n$- матрицу $A^\top$, у которой (i, j)-ый коэффициент равен (j, i)-ому коэффициенту матрицы A. Иными словами

$$A^\top = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{m1} \\ a_{12} & a_{22} & a_{32} & \dots & a_{m2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{mn} \end{pmatrix}.$$

Операция транспонирования $(A \to A^\top)$ – *унарная операция* в отличии от *бинарных* операций сложения и вычитания.

Задача 6. Составьте программу, реализующую операцию транспонирования матриц. Что происходит со столбцом (строкой) при транспонировании?

Свойства операции транспонирования следующие:

$$(A+B)^\top = A^\top + B^\top; \quad (rA)^\top = rA^\top; \quad \left(A^\top\right)^\top = A \tag{2.14}$$

для любых $A, B \in \mathcal{M}at_{m\times n}(K)$ и $r \in K$.

Задача 7. Доказать свойства (2.14).

Матрица, у которой число строк и столбцов совпадают, называется *квадратной*. Элементы $a_{11}, a_{22}, a_{33}, \ldots$ называются *главной диагональю* матрицы (2.13). Операцию транспонирования квадратной матрицы можно представлять себе как "отражение" коэффициентов матрицы относительно главной диагонали.

Задача 8. Матрица A с условием $A^\top = A$ называется *симметричной*, а с условием $A^\top = -A$, - *кососимметричной*. Докажите, что симметричные и кососимметричные матрицы квадратны, и что любую матрицу можно записать в виде суммы симметричной и кососимметричной матриц.

Задача 9. Множество $\mathcal{M}at_{n\times n}(\mathbb{R})$ является пространством размерности n^2. Какова размерность подпространства всех симметричных (кососимметричных) $n \times n$-матриц? (размерность понимать как число независимых друг от друга параметров, требующих-ся для задания общего элемента; см. также §3.3).

2.4.4 Произведение матриц

Для мотивировки определения этой операции обратимся к одной физической задаче. Допустим, что в физическом пространстве имеется материальная точка, которую под действием некоторой силы мы переместили по оси OX на a_x единиц, по оси OY на a_y единиц и по оси OZ на a_z единиц. Сила воздействия на материальную точку также должна быть охарактеризована не только абсолютной величиной, но и направлением. Один из способов сделать это - указать проекции силы на те же оси OX, OY и OZ. Пусть эти проекции будут F_x, F_y, F_z. Тогда работа силы (F_x, F_y, F_z) при перемещении материальной точки на (a_x, a_y, a_z) равна

$$W = F_x a_x + F_y a_y + F_z a_z = (F_x, F_y, F_z) \begin{pmatrix} a_x \\ a_y \\ a_z \end{pmatrix}$$

Правая часть в этом соотношении - произведение строки длины 3 на столбец длины 3. Общее определение аналогично:

$$(a_1, a_2, \ldots, a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$$

– *произведение строки длины n на столбец длины n.*

Пусть теперь у нас кроме $m \times n$ - матрицы $A = (a_{ij})$ имеется еще $n \times k$ - матрица $B = (b_{ij})$, у которой число строк $(= n)$ совпадает с числом столбцов матрицы A. Тогда *произведение* AB - это матрица $D = (d_{ij})$ размера $m \times k$, (i, j)-ый коэффициент которой равен призведению i-ой строки матрицы A на j-ый столбец матрицы B:

$$d_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj} = (a_{i1} + \ldots + a_{in}) \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}.$$

Первое основное свойство произведения - *ассоциативность*: для любых матриц A, B, C размеров $m \times n$, $n \times k$, $k \times l$ соответственно имеет место равенство:

$$A(BC) = (AB)C. \tag{2.15}$$

Доказательство. Во-первых, из определения произведения матриц следует, что произведение BC и AB, также как и произведение в правой и левой части (2.15), определены и результатом последнего является матрица размера $m \times l$. Обозначим через $D = (d_{ij})$ $m \times k$-матрицу AB, а через $F = (f_{ij})$ – $m \times l$-матрицу $(AB)C$. Тогда

$$f_{ij} = \sum_{\alpha=1}^{\alpha=k} d_{i\alpha}c_{\alpha j} = \sum_{\alpha=1}^{\alpha=k}(\sum_{\beta=1}^{\beta=n} a_{i\beta}b_{\beta\alpha})c_{\alpha j} = \sum_{\substack{1\le\beta\le n\\ 1\le\alpha\le k}} a_{i\beta}b_{\beta\alpha}c_{\alpha j}$$

Обозначим теперь через $M = (m_{ij})$ $n \times l$-матрицу BC, а через $Q = (q_{ij})$ – $m \times l$-матрицу $A(BC)$. Тогда

$$g_{ij} = \sum_{\beta=1}^{\beta=n} a_{i\beta}m_{\beta j} = \sum_{\beta=1}^{\beta=n} a_{i\beta}\sum_{\alpha=1}^{\alpha=k} b_{\alpha\beta}c_{\alpha j} = \sum_{\substack{1\le\alpha\le k\\ 1\le\beta\le n}} a_{i\beta}b_{\beta\alpha}c_{\alpha j}$$

Мы видим, что $f_{ij} = g_{ij}$ для любых возможных пар (i, j). Значит, $F = Q$, то есть равенство $A(BC) = (AB)C$ доказано. □

Второе фундаментальное свойство произведения матриц - *дистрибутивность по отношению к сложению*: для любой $m \times n$- матрицы A и любых матриц B, C размера $n \times k$ имеет место равенство

$$A(B + C) = AB + AC.$$

Если же матрица A имеет размер $k \times m$, а B и C как и выше, то

$$(B + C)A = BA + CA.$$

Задача 10. Доказать дистрибутивность произведения матриц.

Обладает ли произведение матриц свойством коммутативности? Прежде всего может случиться так, что произведение AB определено, а BA нет. Тогда заведомо равенство $AB = BA$ не имеет места. Далее, пример

$$(a_1, a_2)\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = a_1b_1 + a_2b_2; \quad \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \cdot (a_1a_2) = \begin{pmatrix} b_1a_1 & b_1a_2 \\ b_2a_1 & b_2a_2 \end{pmatrix}$$

показывает, что размеры матриц AB и BA могут не совпадать между собой по размерности; тогда снова $AB \neq BA$. Но может быть $AB = BA$, если оба произведения существуют и размер матриц AB, BA один и тот же? Это не так, как показывает пример

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

Множество $\mathcal{M}at_{n\times n}(K)$ всех $n \times n$-матриц образует кольцо, т. е. оно замкнуто относительно произведения и сложения матриц, а также выполнены свойства сложения, перечисленные выше и свойства произведения - ассоциативность и дистрибутивность. *Кольцо целых чисел* $\mathbb{Z}$ известно фактически уже школьнику начальных классов. От кольца $n \times n$- матриц его отличает одно фундаментальное свойство - коммутативность. Но свойство $1 \cdot z = z \cdot 1 = z$ нейтрального элемента, - единицы, может быть обобщено на кольцо $\mathcal{M}at_{n\times n}(K)$. Квадратную $n\times n$- матрицу E_n назовем *единичной*, если у ней на главной диагонали стоят единицы, а остальные элементы - нули.

> *Единичная матрица - нейтральный элемент по отношению к произведению матриц, то есть $E_mA = AE_n = A$ для любой матрицы $A \in \mathcal{M}at_{m\times n}(K)$.*

Докажем это свойство, записав (i, j) - коэффициент единичной матрицы как δ_{ij}. По определению

$$\delta_{ij} = \begin{cases} 1, & \text{если} \quad i = j; \\ 0, & \text{если} \quad i \neq j. \end{cases}$$

Таким образом определенная величина называется *символом Кронекера.*

Обозначим (i, j)-ый элемент матрицы E_mA через c_{ij}. Тогда

$$c_{ij} = \delta_{i1}a_{1j} + \delta_{i2}a_{2j} + \ldots + \delta_{im}a_{mj} = 0 \cdot a_{1j} + \ldots + 1 \cdot a_{ij} + \ldots + 0 \cdot a_{mj} = a_{ij}$$

Отсюда вытекает равенство $E_mA = A$. Равенство $AE_n = A$ доказывается аналогично.

Матрица $A = (a_{ij}) \in \mathcal{M}at_{n\times n}(\mathbb{R})$ называется *верхнетреугольной*, если ниже главной диагонали матрицы A стоят нули. Аналогично, A - *нижнетреугольная матрица*, если выше главной диагонали матрицы A стоят нули. Матрица A *треугольная*, если она либо верхнетреугольная, либо нижнетреугольная. Примеры верхнетреуголных матриц доставляют матрицы систем линейных уравнений, приведенных к ступенчатому виду. Матрица называется *диагональной*, если все элементы стоящие вне главной диагонали равны 0. Общий вид и обозначение диагональной $n \times n$-матрицы такое:

$$\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Задача 11. Доказать, что множество верхнетреугольных (нижнетреугольных, диагональных) $n \times n$- матриц замкнуто относительно сложения и умножения и тем самым составляет подкольцо кольца $\mathcal{M}at_{n\times n}(K)$.

Как соотносится операция транспонирования с операцией произведения матриц? Оказывается

> *для любых матриц A и B, произведение которых определено, имеет место равенство*
>
> $$(AB)^\top = B^\top A^\top$$
>
> *В частности, произведение $B^\top A^\top$ в этом случае также определено.*

Задача 12. Доказать сформулированное выше свойство.

Квадратная матрица A называется *нильпотентной*, если $A^n = 0$ для некоторого натурального n. Ясно, что нулевая матрица нильпотентна и n можно взять равным единице. Наличие других нильпотентных матриц предлагается доказать:

Задача 13. Всякая *строго верхнетреугольная $n \times n$- матрица*

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 0 & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

нильпотентна. Более точно, $A^n = 0$. Аналогичный результат имеет место для *строго нижнетреугольных* матриц.

2.5 Определители

Вернемся снова к правилу Крамара, позволившему так просто и изящно выразить решение системы 2×2 (см. §1.1). На этот раз будем решать систему 3×3:

$$\begin{cases} a_1x + b_1y + c_1z = d_1; \\ a_2x + b_2y + c_2z = d_2; \\ a_2x + b_2y + c_2z = d_2. \end{cases} \tag{2.16}$$

Обозначим:

$$\Delta_{11} = \begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix}; \quad \Delta_{21} = \begin{vmatrix} b_1 & c_1 \\ b_3 & c_3 \end{vmatrix}; \quad \Delta_{31} = \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}.$$

Умножим первое уравнение системы (2.16) на Δ_{11}, второе – на $-\Delta_{21}$, а третье – на Δ_{31} и результаты сложим. Получим:

$$(a_1\Delta_{11} - a_2\Delta_{21} + a_3\Delta_{31})x + (b_1\Delta_{11} - b_2\Delta_{21} + b_3\Delta_{31})y +$$
$$+(c_1\Delta_{11} - c_2\Delta_{21} + c_3\Delta_{31})z = (d_1\Delta_{11} - d_2\Delta_{21} + d_3\Delta_{31}).$$

Нетрудно вычислить и доказать, что $b_1\Delta_{11} - b_2\Delta_{21} + b_3\Delta_{31} = 0$ и $c_1\Delta_{11} - c_2\Delta_{21} + c_3\Delta_{31} = 0$. С учётом этого остаётся

$$(a_1\Delta_{11} - a_2\Delta_{21} + a_3\Delta_{31})x = (d_1\Delta_{11} - d_2\Delta_{21} + d_3\Delta_{31}) \tag{2.17}$$

Обозначим:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 \begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix} - b_1 \begin{vmatrix} b_1 & c_1 \\ b_3 & c_3 \end{vmatrix} + c_1 \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix} =$$
$$= a_1b_2c_3 + a_3b_2c_2 + a_2b_3c_1 - a_1b_3c_2 - a_2b_1c_3 + a_3b_2c_1. \tag{2.18}$$

и назовем эту конструкцию *определителем* 3×3. Конечно, шесть произведений в (2.18) запомнить нелегко. Существует правило, точнее диаграмма, облегчающая это запоминание:

В каждом из произведений в правой части (2.18) расставьте сомножители по кружочкам этой диаграммы и её смысл станет ясен.

Итак, применяя определение определителя 3×3, мы можем переписать (2.17) в виде

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} x = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}. \tag{2.19}$$

Совершенно аналогично можно получить два других следствия системы (2.19):

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} y = \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}, \quad \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} z = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}. \tag{2.20}$$

Обозначим через

$$\Delta = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix},$$

– *определитель системы* (2.16) и

$$\Delta_x = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}, \quad \Delta_y = \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}, \quad \Delta_z = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}.$$

Предположим, что $\Delta \neq 0$. Тогда решение системы (2.16) может быть только такое:

$$x = \frac{\Delta_x}{\Delta}, \quad y = \frac{\Delta_y}{\Delta}, \quad z = \frac{\Delta_z}{\Delta}. \tag{2.21}$$

(см. (2.19) и (2.20)). Тот факт, что (2.21) – действительно решение системы (2.16), доказывается прямой проверкой. Это есть правило Крамара для систем 3×3. После этого естественно предположить, что существует аналогичное правило и аналогичные *формулы Крамара* для квадратных систем любого порядка. Для того, что бы подтвердить это (и для многих других целей) нам нужно понятие определителя произвольной квадратной матрицы. Каким образом определить эту важнейшую характеристику квадратной матрицы? Для ответа на этот вопрос ещё раз перепишем определитель 3×3 для матрицы (a_{ij}):

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - \tag{2.22}$$

$$-a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

Мы специально написали все шесть произведений так чтобы первый индекс шел в возрастающем порядке: 1,2,3. Тогда вторые индексы образуют перестановку, – элемент группы S_3. При этом все шесть перестановок из S_3 задействованы в (2.22), и чётным перестановкам соответствует знак плюс перед произведением, а нечётным – знак минус. Такая же закономерность прослеживается и для определителей 2×2:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Это приводит нас к следующему определению. Пусть $A = (a_{ij})$ – $n \times n$-матрица. *Определителем* матрицы A называется элемент поля K, который вычисляется по следующему правилу

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}. \tag{2.23}$$

Пусть $F(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$ – функция строк длины n ($\mathbf{x}_i \in K^n$). Функция F называется *полилинейной*, если для любых элементов $\lambda, \mu \in K$ и любого индекса i имеет место равенство

$$F(\dots \lambda\mathbf{x}_i' + \mu\mathbf{x}_i'' \dots) = \lambda F(\dots \mathbf{x}_i' \dots) + \mu F(\dots \mathbf{x}_i'' \dots)$$

(точками обозначены аргументы с номерами $\neq i$).

Задача 1. Доказать, что линейность функции $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ одной строки $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ равносильна следующему: найдутся такие числа $B_1, B_2, \ldots, B_n$, что $f(\mathbf{x}) = B_1 x_1 + B_2 x_2 + \ldots + B_n x_n$.

Функция F называется *кососимметричной*, если при перестановке двух аргументов ее значение меняет знак:

$$F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots) = -F(\ldots \mathbf{x}_j \ldots \mathbf{x}_i \ldots) \qquad (2.24)$$

Если в поле K двойка не равна нулю, то из кососимметричности сразу следует равенство $F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots) = 0$ в случае $\mathbf{x}_i = \mathbf{x}_j$. Если же в поле K двойка равна нулю (например, $K = \mathbb{Z}_2$) , то определение кососимметричности следует подправить: полилинейная функция называется кососимметричной, если она равна 0 в случае совпадения каких-либо двух аргументов.

Из второго определения следует кососимметричность в смысле первого определения. Действительно, из равенств

$$0 = F(\ldots \mathbf{x}_i + \mathbf{x}_j \ldots \mathbf{x}_i + \mathbf{x}_j \ldots) =$$
$$= F(\ldots \mathbf{x}_i \ldots \mathbf{x}_i \ldots) + F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots) + F(\ldots \mathbf{x}_j \ldots \mathbf{x}_i \ldots) +$$
$$+ F(\ldots \mathbf{x}_j \ldots \mathbf{x}_j \ldots) = F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots) + F(\ldots \mathbf{x}_j \ldots \mathbf{x}_i \ldots)$$

сразу вытекает (2.24).

Теорема 1. *Определитель – полилинейная и кососимметричная функция строк матрицы.*

Доказательство. Докажем линейность для первой строки матрицы:

$$\begin{vmatrix} \lambda a'_{11} + \mu a''_{11} & \lambda a'_{12} + \mu a''_{12} & \ldots & \lambda a'_{1n} + \mu a''_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; (\lambda a'_{1\sigma(1)} + \mu a''_{1\sigma(1)}) a_{2\sigma(2)} \ldots a_{n\sigma(n)} =$$

$$= \lambda \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a'_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} + \mu \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a''_{1\sigma(1)}) a_{2\sigma(2)} \ldots a_{n\sigma(n)} =$$

$$= \lambda \begin{vmatrix} a'_{11} & a'_{12} & \ldots & a'_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \mu \begin{vmatrix} a''_{11} & a''_{12} & \ldots & a''_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

Далее, пусть в матрице $A = (a_{ij})$ мы переставили t-ую и s-ую строку и получили матрицу $B = (b_{ij})$. В этой матрице

$$b_{ij} = \begin{cases} a_{ij}, & \text{если } i \neq t, i \neq s; \\ a_{sj}, & \text{если } i = t; \\ a_{tj}, & \text{если } i = s. \end{cases}$$

Обозначим через τ транспозицию (ts). Без ограничения общности можно считать, что $t < s$. Тогда

$$\det B = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; b_{1\sigma(1)} \dots b_{t\sigma(t)} \dots b_{s\sigma(s)} \dots b_{n\sigma(n)} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma\tau) \; b_{1\sigma\tau(1)} \dots b_{t\sigma\tau(t)} \dots b_{s\sigma\tau(s)} \dots b_{n\sigma\tau(n)} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \operatorname{sgn} \tau \; b_{1\sigma(1)} \dots b_{t\sigma(s)} \dots b_{s\sigma(t)} \dots b_{n\sigma(n)} =$$

$$= - \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a_{1\sigma(1)} \dots a_{s\sigma(s)} \dots a_{t\sigma(t)} \dots a_{n\sigma(n)} = - \det A,$$

что и требовалось доказать. Здесь учтено, что при умножении на транспозицию четность подстановки меняется (см. § 1.5.3, лемма 1). □

Теорема 2. *Определитель треугольной матрицы равен произведению элементов на главной диагонали. В частности,* $\det E = 1$.

Доказательство. Пусть $A = (a_{ij})$ – верхнетреугольная $n{\times}n$-матрица. Тогда $a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} = 0$, если хотя бы для одного i имеет место неравенство $\sigma(i) < i$. Рассмотрим оставшийся случай: для любого i выполнено неравенство $\sigma(i) \geq i$. Тогда $\sigma(n) = n$; далее $\sigma(n-1) = n-1$ и т.д. вплоть до $\sigma(1) = 1$. Итак, в оставшемся случае имеется только одна подстановка – единичная. Тогда $\det A = a_{11} a_{22} \dots a_{nn}$. В точности такая же формула имеет место и для нижнетреугольной матрицы. Доказательство аналогично. □

Теорема 3 (единственности). *Любая полилинейная и кососимметричная функция* $\mathcal{D} : \mathcal{M}at_{n\times n}(K) \to K$ *пропорциональна определителю, а именно* $\mathcal{D}(A) = \mathcal{D}(E) \det A$ *для любой квадратной матрицы A. Если, кроме того,* $\mathcal{D}(E) = 1$, *то* $\mathcal{D}(A) = \det A$ *для любой матрицы A.*

Доказательство. Рассмотрим $n \times n$-матрицы e_{ij}, у которых на месте (i, j) стоит 1, а на остальных местах стоят нули. Тогда произвольная $n \times n$-матрица $A = (a_{ij})$ может быть записана так: $A = \sum_{1 \leq i,j \leq n} a_{ij} e_{ij}$. Пользуясь полилинейностью, получаем равенство

$$\mathcal{D}(A) = \sum_{1 \leq j_1, \dots, j_n \leq n} a_{1j_1} \dots a_{nj_n} \mathcal{D}(e_{1j_1} + \ldots + e_{nj_n}).$$

Но $\mathcal{D}(e_{1j_1} + \ldots + e_{nj_n}) = 0$, если найдутся индексы $i \neq i'$ такие, что $j_i = j_{i'}$ (см. свойство после определения кососимметричности). Если же индексы $j_1, j_2, \ldots, j_n$ все различны, то

$$\mathcal{D}(e_{1j_1} + \ldots e_{nj_n}) = \operatorname{sgn}(j_1, j_2, \ldots, j_n)\mathcal{D}(e_{11} + \ldots + e_{nn}) = \\ = \operatorname{sgn}(j_1, j_2, \ldots, j_n)\mathcal{D}(E),$$

как следует из кососимметричности. Обозначив подстановку $(j_1, j_2, \ldots, j_n)$ через σ, мы приходим к равенству

$$\mathcal{D}(A) = \mathcal{D}(E) \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a_{1\sigma(1)} \ldots a_{n\sigma(n)} = \mathcal{D}(E) \det A.$$

Отсюда и следует утверждение теоремы. □

Отметим теперь некоторые свойства определителей

Свойство 1. *Определитель матрицы равен определителю транспонированной матрицы.*

Доказательство. Действительно, $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$ для любой подстановки σ, как следует из теоремы о том, что четность подстановки определяется четностью числа транспозиций, в которые она раскладывается (см. § 1.5.3). Пусть матрица $B = (b_{ij})$ получается из $n \times n$-матрицы A транспонированием. Тогда

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} = \\ = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \; a_{\sigma^{-1}(1)1} a_{\sigma^{-1}(2)2} \ldots a_{\sigma^{-1}(n)n} = \\ = \sum_{\mu \in S_n} \operatorname{sgn} \mu \; a_{\mu(1)1} a_{\mu(2)2} \ldots a_{\mu(n)n} = \sum_{\mu \in S_n} \operatorname{sgn} \mu \; b_{1\mu(1)} b_{2\mu(2)} \ldots b_{n\mu(n)} = \det B$$

□

В силу равенства $\det A = \det A^{\top}$ все свойства, доказанные для строк, автоматически переносятся на столбцы и наоборот. В частности

Свойство 2. *Определитель – полилинейная и кососимметричная функция столбцов матрицы.*

Свойство 3. *Определитель равен нулю, если какие-либо две строки (два столбца) совпадают.*

Это свойство мы отмечали ранее в более общем случае для полилинейной функции. Следующее свойство также следствие полилинейности.

Свойство 4. *Определитель с нулевой строкой (столбцом) равен нулю.*

Свойство 5. *Определитель не изменится, если над строками (столбцами) совершить элементарное преобразование первого типа, т.е. к одной строке прибавить другую, умноженную на какое-либо число.*

Доказательство. Это утверждение – следствие полилинейности и свойства 3:

$$F(\ldots \mathbf{x}_i + \lambda \mathbf{x}_j \ldots \mathbf{x}_j \ldots) = F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots) + \lambda F(\ldots \mathbf{x}_j \ldots \mathbf{x}_j \ldots) =$$

$$= F(\ldots \mathbf{x}_i \ldots \mathbf{x}_j \ldots)$$

Здесь F – любая полилинейная и кососимметричная функция строк. □

Прежде чем формулировать следующее свойство, приведем определение минора матрицы. *(i, j)-ым минором матрицы A* называется определитель матрицы, получающейся из A вычеркиванием i-ой строки и j-го столбца. Обозначается этот минор – M_{ij}. *Алгебраическим дополнением (i, j)-го элемента матрицы A* называется величина $A_{ij} = (-1)^{i+j} M_{ij}$.

Свойство 6. *Разложение определителя по j-му столбцу и i-ой строке*:

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj};$$

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}.$$

Доказательство. Функция $\mathcal{D}(A) = a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj}$ полилинейна и кососимметрична. Кроме того, легко вычислить, что $\mathcal{D}(E) = 1$. Остается применить теорему единственности. □

Имеют место также *ложные разложения по r-ой строке и r-ому столбцу*; если $r \neq i$ и $r \neq j$, то

$$0 = a_{r1}A_{i1} + a_{r2}A_{i2} + \ldots + a_{rn}A_{in},$$
$$0 = a_{1r}A_{1j} + a_{2r}A_{2j} + \ldots + a_{nr}A_{nj}.$$

Действительно, правая часть здесь совпадает с определителем матрицы, у которой две строки (два столбца) совпадают.

2.6 Вычисление определителей некоторых матриц

2.6.1 Определитель произведения матриц

Квадратная матрица A называется *невырожденной*, если $\det A \neq 0$, и называется *вырожденной* в противном случае.

Теорема 1. *Определитель произведения матриц равен произведению определителей:* $\det(AB) = \det A \det B$ *(для любых $n \times n$-матриц A и B).*

Доказательство. Фиксируем матрицу B. Тогда функция $\mathcal{D}(A) = \det AB$ полилинейна и кососимметрична. Это легко следует из определения умножения матриц. По теореме единственности получаем: $\det AB = \mathcal{D}(A) = \det A \cdot \mathcal{D}(E) = \det A \cdot \det B$ □

Следствие. *Произведение вырожденной матрицы на любую квадратную матрицу того же размера снова будет вырожденной матрицей. Произведение невырожденных матриц является невырожденной матрицей.*

Теорема 2 (определитель с углом нулей) *Пусть A, B - квадратные матрицы (не обязательно одинакового размера). Тогда*

$$\begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = \det A \cdot \det B \tag{2.25}$$

для любой матрицы C подходящего размера. Аналогично,

$$\begin{vmatrix} A & 0 \\ D & B \end{vmatrix} = \det A \cdot \det B \tag{2.26}$$

для любой матрицы D подходящего размера.

Доказательство. Левая часть в (2.25) – полилинейная функция столбцов матрицы A и строк матрицы B. Следовательно, по теореме единственности,

$$\begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = \det A \cdot \det B \begin{vmatrix} E & C \\ 0 & E \end{vmatrix} = \det A \cdot \det B.$$

□

2.6.2 Определитель Вандермонда

Для любых $x_1, \ldots, x_n$ имеет место равенство:

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i) \tag{2.27}$$

В правой части здесь стоит произведение вида

$$(x_2 - x_1)(x_3 - x_1) \ldots (x_n - x_1) \cdot (x_3 - x_2) \ldots (x_n - x_2) \ldots (x_n - x_{n-1})$$

(всего $\frac{n(n-1)}{2}$ сомножителей.)

Доказательство. Вычтем из каждого последующего столбца предыдущий, умноженный на x_1, а далее разложим по получившейся первой строке – (1,0,0. . . ,0). Приходим к определителю $(n-1) \times (n-1)$:

$$\begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \dots & x_2^{n-2}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \dots & x_3^{n-2}(x_3 - x_1) \\ \dots & \dots & \dots & \dots \\ x_n - x_1 & x_n(x_n - x_1) & \dots & x_n^{n-2}(x_n - x_1) \end{vmatrix}$$

Далее вынесем из строк множители $(x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1)$ и сведем задачу к вычислению такого же определителя меньшего размера. Применение индукции заканчивает доказательство. □

2.7 Правило Крамара

Пусть

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = b_2 \\ \dots\dots\dots\dots\dots & \dots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n & = b_n \end{cases} \tag{2.28}$$

– система n линейных уравнений с n неизвестными.

Теорема 1 (правило Крамара). *Система (2.28) определена тогда и только тогда, когда матрица A невырождена. В этом случае решение находится по формулам:*

$$x_1 = \frac{\det A_1}{\det A}, \quad x_2 = \frac{\det A_2}{\det A}, \dots, x_n = \frac{\det A_n}{\det A}, \tag{2.29}$$

где A_i - матрица, полученная из матрицы A заменой i-го столбца на столбец свободных членов
$(b_1, b_2, \dots, b_n)^\top$.

Доказательство. Заметим, что при элементарных преобразованиях системы 1-3 типов свойство невырожденности (вырожденности) матрицы системы сохраняется. Следовательно, если $\det A \neq 0$, то в ступенчатом виде на главной диагонали должны стоять ненулевые элементы (см. теорему об определителе треугольной матрицы), т. е. система (2.28) будет определенной. Наоборот, если система (2.28) определена, то все неизвестные – главные, следовательно матрица ступенчатого вида невырождена, и поэтому $\det A \neq 0$. Остается проверить формулу (2.29) в случае $\det A \neq 0$.

Фиксируем натуральное число k, $1 \leq k \leq n$. Умножим i-ое уравнение системы (2.28) на A_{ik} – алгебраическое дополнение элемента a_{ik} матрицы A, и результаты просуммируем по $i = 1, 2, \dots, n$. Тогда в силу свойства "ложного разложения" по столбцу матрицы A будем иметь $\sum_{i=1}^n a_{ij}A_{ik} = 0$ для всякого j, $j \neq k$, а $\sum_{i=1}^n a_{ik}A_{ik} = \det A$. Тем самым результат после суммирования будет следующий:

$$\det A \cdot x_k = \sum_{i=1}^n b_{ik}A_{ik} = \det A_k$$

(Последнее равенство верно в силу разложения $\det A_k$ по k-ому столбцу). Отсюда находим $x_k = \det A_k / \det A$ и тем самым доказательство правила Крамара завершено. □

Следствие доказательства. *Если* $\det A = 0$, *но* $\det A_k \neq 0$ *для какого-либо* k, *то система (2.28) несовместна.*

Теорема 2. *Пусть (2.28) – однородная система, т. е.* $b_1 = b_2 = \ldots = b_n = 0$. *Эта система имеет ненулевое решение тогда и только тогда, когда* $\det A = 0$.

Доказательство. Так как однородная система всегда совместна, то остается две возможности - эта система либо определена (т. е. имеет только нулевое решение), либо неопределена (т. е. имеет ненулевое решение). Остается применить правило Крамара. □

2.8 Обратная матрица

2.8.1 Определение и вычисление обратной матрицы

Обратимость элемента в моноиде разобрана в §1.4.1, см. там же теорему 3. В применении к матрицам это выглядит так: $n \times n$-матрица D называется *обратной* к $n \times n$-матрице A, если $AD = DA = E$.

Обратная матрица единственна, если она существует и в этом случае она обозначается как A^{-1}. Обозначение в виде дроби не применяется, так как умножение матриц некоммутативно. Следующие свойства доказаны ранее в более общей ситуации (см. §1.4, теорема 3).

1. *Если матрица* A *обратима, то* A^{-1} *также обратима и* $(A^{-1})^{-1} = A$.

2. *Если матрицы* A *и* B *обратимы, то матрица* AB *также обратима и* $(AB)^{-1} = B^{-1}A^{-1}$.

Теорема 1. *Обратная матрица к* $n \times n$*-матрице* A *существует тогда и только тогда, когда матрица* A *невырождена. В этом случае*

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix}, \tag{2.30}$$

где A_{ij}, *как и ранее, алгебраическое дополнение к* (i, j)*-тому элементу матрицы* A.

Доказательство. Если матрица A вырождена, то и AB вырождена (§2.6.1, следствие теоремы 1), поэтому произведение не может быть равно единичной матрице.

Предположим теперь, что $\det A \neq 0$. Тогда правая часть в (2.30) определена и можно убедиться непосредственной проверкой, что ее произведение на матрицу A дает единичную матрицу; при этом используются свойства разложения и ложного разложения определителя матрицы по столбцу (строке). □

Предложение 1. *Имеет место равенство* $\det A^{-1} = 1/\det A$ *для любой невырожденной матрицы* A.

Действительно, применение теоремы об определителе произведения матриц к $A \cdot A^{-1} = E$ дает равенство $\det A \det A^{-1} = 1$, откуда и следует нужное равенство.

Обозначим через $\mathrm{GL}(n, K)$ множество невырожденных $n \times n$-матриц. Из выше доказанного следует, что это множество – группа относительно умножения. Ее называют *общей линейной группой*. Более того, отображение $\det : \mathrm{GL}(n, K) \to K \setminus \{0\}$ – морфизм общей линейной группы в группу ненулевых элементов поля K (относительно умножения).

Задача 1. Доказать сформулированные выше утверждения.

2.8.2 Матричный метод решения линейных систем

Рассмотрим систему n уравнений с n неизвестными (2.28), §2.7. Обозначим через $A = (a_{ij})$ матрицу этой системы, $B = (b_1, b_2, \dots, b_n)^\top$ – столбец свободных членов и через $X = (x_1, x_2, \dots, x_n)^\top$ обозначим столбец неизвестных. Тогда эта система может быть записана в *матричном виде*:

$$AX = B \tag{2.31}$$

Умножив слева это соотношение на A^{-1}, приходим к следующему результату:

Теорема 2. *Если A невырожденная матрица, то система (2.31) определена, и ее решение находится по формуле $X = A^{-1}B$.*

Эта теорема показывает, что принципиально уравнение (2.31) и метод его решения ничем не отличается от уравнения вида $ax = b$ (см. §2.1.1).

Задача 1. Решить матричное уравнение $AXB = C$ относительно неизвестной матрицы X. Здесь A и B – квадратные невырожденные матрицы.

Задача 2*. Доказать, что матрица $E - AB$ обратима тогда и только тогда, когда обратима матрица $E - BA$.

Задача 3. Пусть A – нильпотентная матрица. Доказать, что матрица $E - A$ обратима и указать обратную для нее матрицу.

Глава 3

Линейные пространства

Теория линейных пространств – ядро линейной алгебры. В ней очень тесно переплетается геометрический и алгебраический язык. В частности, это проявляется в том, что элементы линейного пространства называются иногда векторами. С геометрических векторов и начинается изложение.

3.1 Геометрические вектора

3.1.1 Основные определения

Вектором называется направленный отрезок, т. е. отрезок AB, одна крайняя точка которого (скажем A) объявлена *началом*, а другая *концом* . Такой вектор обозначается как $\overrightarrow{AB}$. *Длиной* или *модулем* вектора $\overrightarrow{AB}$ называется длина отрезка AB; она обозначается как $|\overrightarrow{AB}|$. Примерами векторных величин является скорость, ускорение, сила, перемещение. Если $A = B$, то вектор $\overrightarrow{AB}$ называется *нулевым* и обозначается $\mathbf{0}$. *Два вектора $\overrightarrow{AB}$ и $\overrightarrow{A'B'}$ называются равными*, если их длины равны и они *сонаправлены*, т. е. лежат на одной прямой или на параллельных прямых и "смотрят" в одну сторону. Простое геометрическое построение убеждает нас, что для любого вектора $\mathbf{a}$ и любой точки A существует единственная точка B такая, что $\mathbf{a} = \overrightarrow{AB}$. Этот вектор $\overrightarrow{AB}$ называется *реализацией* вектора $\mathbf{a}$ в точке A.

Пусть начало A и конец B вектора заданы координатами: $A(x_1, y_1, z_1)$, $B(x_2, y_2, z_2)$. Тогда упорядоченная тройка

$$X = x_2 - x_1, \qquad Y = y_2 - y_1, \qquad Z = z_2 - z_1 \tag{3.1}$$

называется *координатами* вектора $\overrightarrow{AB}$.

Имеет место **критерий равенства векторов**: *два вектора равны тогда и только тогда, когда равны их x-овые, y-овые и z-овые координаты.*

Длина вектора $\mathbf{a}(X, Y, Z)$ выражается через его координаты следующим образом

$$|\mathbf{a}| = \sqrt{X^2 + Y^2 + Z^2}.$$

Пусть α, β, γ - углы, которые образует ненулевой вектор $\mathbf{a}$ с осями OX, OY, OZ соответственно. Тогда $\cos\alpha$, $\cos\beta$, $\cos\gamma$ назовем *направляющими косинусами* вектора $\mathbf{a}$. Вектор, сонаправленный с вектором $\mathbf{a}$, и имеющий единичную длину, назовем *ортом* и обозначим $\mathbf{a}^o$. Нетрудно видеть, что, если $\mathbf{a}$ – ненулевой вектор с координатами (X, Y, Z), то координаты орта $\mathbf{a}^o$ имеют вид

$$\left(\frac{X}{|\mathbf{a}|}, \frac{Y}{|\mathbf{a}|}, \frac{Z}{|\mathbf{a}|}\right),$$

причем они совпадают с направляющими косинусами вектора $\mathbf{a}$:

$$\cos\alpha = \frac{X}{|\mathbf{a}|}, \quad \cos\beta = \frac{Y}{|\mathbf{a}|}, \quad \cos\gamma = \frac{Z}{|\mathbf{a}|}.$$

Зная длину и направляющие косинусы, можно найти координаты вектора по формулам

$$X = |\mathbf{a}|\cos\alpha, \quad Y = |\mathbf{a}|\cos\beta, \quad Z = |\mathbf{a}|\cos\gamma. \tag{3.2}$$

3.1.2 Арифметические операции над векторами

Пусть имеются два вектора $\mathbf{a}$ и $\mathbf{b}$. Реализуем $\mathbf{a}$ в точке A: $\mathbf{a} = \overrightarrow{AB}$, а вектор $\mathbf{b}$ реализуем в точке B – конце вектора $\mathbf{a}$: $\mathbf{b} = \overrightarrow{BC}$. Тогда вектор $\overrightarrow{AC}$ назовем суммой векторов $\mathbf{a}$ и $\mathbf{b}$ (см. рис. 1, а)).

Это определение корректно, т. е. результат суммы двух векторов не зависит от изначально выбранной точки A. Из определения суммы векторов вытекает **равенство Шаля**:

$$\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}.$$

Существует другое определение операции суммы двух векторов – *правило параллелограмма*, но оно "работает" только для ненулевых и не коллинеарных векторов. При этом семейство векторов называется *коллинеарным*, если все вектора этого семейства лежат либо на одной прямой, либо на параллельных прямых. Пусть имеются два неколлинеарных вектора $\mathbf{a}$ и $\mathbf{b}$. Реализуем их в одной точке A, так что $\mathbf{a} = \overrightarrow{AB}$ и $\mathbf{b} = \overrightarrow{AD}$. Достроим $\triangle ABD$ до параллелограмма $ABCD$. Тогда $\mathbf{a} + \mathbf{b} = \overrightarrow{AC}$ (см. рис. 1, б)). Результат сложения не зависит от выбора точки A.

Умножить вектор $\mathbf{a} = \overrightarrow{AB}$ *на число* $\lambda \in \mathbb{R}$, – значит на прямой ℓ , проходящей через точки A и B, построить точку D такую, что $|AD| = |\lambda||AB|$, причем, если $\lambda > 0$, то точка D должна лежать по ту же сторону от A, что и точка B; если же $\lambda < 0$, то точку D следует выбирать на прямой ℓ по другую сторону от A чем B. Если $\lambda = 0$, то полагаем $\lambda\mathbf{a} = \mathbf{0}$ – нулевой вектор (см. рис. 1, в)).

Рис. 1. Арифметические операции над векторами

Множество всех векторов в пространстве, обозначим его $\mathcal{V}(\mathbb{E}^3)$, относительно определенных выше операций сложения и умножения обладает следующими свойствами

ЛП1. $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$ (коммутативность);

ЛП2. $\mathbf{a}+(\mathbf{b}+\mathbf{c})=(\mathbf{a}+\mathbf{b})+\mathbf{c}$ (ассоциативность);

ЛП3. $\mathbf{0}+\mathbf{a}=\mathbf{a}$ (существование нуля для операции сложения);

ЛП4. для любого вектора $\mathbf{a}$ существует *противоположный* вектор $-\mathbf{a}$ такой, что $\mathbf{a}+(-\mathbf{a})=\mathbf{0}$;

ЛП5. $(\lambda\mu)\mathbf{a}=\lambda(\mu\mathbf{a})$ (ассоциативность умножения);

ЛП6. $(\lambda+\mu)\mathbf{a}=\lambda\mathbf{a}+\mu\mathbf{a}$ и $\lambda(\mathbf{a}+\mathbf{b})=\lambda\mathbf{a}+\lambda\mathbf{b}$ (дистрибутивность);

ЛП7. $1\cdot\mathbf{a}=\mathbf{a}$ (унитарность).

Эти равенства верны для любых векторов $\mathbf{a},\mathbf{b},\mathbf{c}\in\mathcal{V}(\mathbb{E}^3)$ и любых действительных чисел λ и μ. Доказательство этого факта весьма длинная и скучная, хотя и элементарная проверка. Например, докажем ассоциативность сложения. Реализуем вектор $\mathbf{a}$ в точке A: $\mathbf{a}=\overrightarrow{AB}$, вектор $\mathbf{b}$ реализуем в точке B: $\mathbf{b}=\overrightarrow{BC}$, а вектор $\mathbf{c}$ реализуем в точке C: $\mathbf{c}=\overrightarrow{CD}$. Тогда

$$\mathbf{a}+(\mathbf{b}+\mathbf{c})=\overrightarrow{AB}+(\overrightarrow{BC}+\overrightarrow{CD})=\overrightarrow{AB}+\overrightarrow{BD}=\overrightarrow{AD},$$

$$(\mathbf{a}+\mathbf{b})+\mathbf{c}=(\overrightarrow{AB}+\overrightarrow{BC})+\overrightarrow{CD}=\overrightarrow{AC}+\overrightarrow{CD}=\overrightarrow{AD}.$$

Здесь четыре раза мы применили равенство Шаля. Правые части равны, значит равенство $\mathbf{a}+(\mathbf{b}+\mathbf{c})=(\mathbf{a}+\mathbf{b})+\mathbf{c}$ доказано.

Свойство ЛП1 следует из правила параллелограмма сложения двух векторов. Свойство ЛП4 доказывается так: если $\mathbf{a}=\overrightarrow{AB}$, то $-\mathbf{a}=\overrightarrow{BA}$. Действительно, $\overrightarrow{AB}+\overrightarrow{BA}=\overrightarrow{AA}=\mathbf{0}$, где ещё раз применено равенство Шаля. Для того, чтобы доказать ЛП5 заметим сначала, что модули левой и правой частей совпадают с $|\lambda|\,|\mu|\,|\mathbf{a}|$. Ясно также, что векторы $(\lambda\mu)\mathbf{a}$ и $\lambda(\mu\mathbf{a})$ лежат на одной прямой и имеют общее начало. Остается убедиться, что они сонаправлены. Это достигается с помощью перебора следующих случаев 1) $\lambda>0$, $\mu>0$, 2) $\lambda>0$, $\mu<0$, 3) $\lambda<0$, $\mu>0$, 4) $\lambda<0$, $\mu<0$, 5) либо $\lambda=0$, либо $\mu=0$. В случаях 1) и 4) вектора $(\lambda\mu)\mathbf{a}$ и $\lambda(\mu\mathbf{a})$ сонаправлены с $\mathbf{a}$, а поэтому сонаправлены между собой; в случаях 2) и 3) эти вектора сонаправлены с $-\mathbf{a}$, а поэтому также сонаправлены между собой. В случае 5) эти вектора нулевые.

Свойства ЛП3 и ЛП7 – тривиальности.

Задача 1. Доказать свойство ЛП6 (дистрибутивность).

Из свойств ЛП1-ЛП4 следует, что множество $\mathcal{V}(\mathbb{E}^3)$ образует абелеву группу относительно сложения.

В координатах арифметические операции над векторами выражаются следующим образом. Пусть вектора $\mathbf{a}$ и $\mathbf{b}$ имеют координаты (X_1, Y_1, Z_1) и (X_2, Y_2, Z_2) соответственно. Тогда координаты векторов $\mathbf{a}+\mathbf{b}$ и $\lambda\mathbf{a}$ будут $(X_1 + X_2, Y_1 + Y_2, Z_1 + Z_2)$ и $(\lambda X_1, \lambda Y_1, \lambda Z_1)$ соответственно.

Вектора единичной длины, направленные по осям OX, OY, OZ обозначают обычно - $\mathbf{i}, \mathbf{j}, \mathbf{k}$ и эту упорядоченную тройку векторов называются *стандартным базисом* (см. рис. 2, а)). Легко видеть, что любой вектор $\mathbf{a}$ с координатами (X, Y, Z) можно *разложить по базисным векторам*: $\mathbf{a} = X\mathbf{i} + Y\mathbf{j} + Z\mathbf{k}$. Через $\mathcal{V}(\mathbb{E}^2)$ будем обозначать пространство векторов на евклидовой плоскости $\mathbb{E}^2$. Стандартный базис на плоскости состоит из двух векторов $\mathbf{i}$ и $\mathbf{j}$. Разложение вектора $\mathbf{a}(X, Y)$ по стандартному базису показано на рис. 2, б).

Рис. 2. Стандартный базис геометрических векторов

3.2 Определение линейного пространства

Свойства векторов ЛП1-ЛП7, отмеченные в предыдущем параграфе, характерные также и для чисел любой природы – рациональных, действительных, комплексных, для матриц фиксированного размера $m \times n$, для функций $\mathcal{F}(X)$ на множестве X, если определить сложение функций $f, g \in \mathcal{F}(X)$ и умножение функции на число $\lambda \in \mathbb{R}$ следующим образом:

$$(f+g)(x) = f(x) + g(x); \quad (\lambda \cdot f)(x) = \lambda f(x) \qquad (x \in X). \tag{3.3}$$

С точки зрения универсальности и широты охвата удобнее эти свойства положить в основу теории, а далее теоремы, понятия и формулы этой теории применять для всех перечисленных выше объектов. Теория, о которой мы говорим, называется *линейные пространства.* Вот ее основное

Определение 1. Множество L с операцией сложения и операциями умножения на элементы поля K называется *линейным пространством (над полем K)*, если выполнены следующие аксиомы:

LS1. $(L, +)$ – абелева группа, т. е. имеет место коммутативность и ассоциативность операции сложения, существует нулевой элемент $\mathbf{0} \in L$, и для каждого элемента $\mathbf{a} \in L$ найдется противоположный элемент $-\mathbf{a}$ такой, что $\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$.

LS2. *(ассоциативность умножения)* $(\lambda\mu)\mathbf{a} = \lambda(\mu\mathbf{a})$;

LS3. *(дистрибутивность)* $(\lambda + \mu)\mathbf{a} = \lambda\mathbf{a} + \mu\mathbf{a}$ и $\lambda(\mathbf{a} + \mathbf{b}) = \lambda\mathbf{a} + \lambda\mathbf{b}$;

LS4. *(унитарность)* $1_K \cdot \mathbf{a} = \mathbf{a}$.

Эти равенства верны для любых элементов $\mathbf{a}, \mathbf{b}, \mathbf{c} \in L$ и любых $\lambda, \mu \in K$.

Теперь нетрудно проверить, что семейство функций на множестве действительно является линейным пространством над полем $\mathbb{R}$ относительно операций (3.3). Также является линейным пространством в смысле определения 1 множество матриц $\mathcal{M}at_{n\times m}(K)$.

Задача 1. Реализовать $\mathcal{M}at_{n\times m}(K)$ как пространство функций $\mathcal{F}(X, K)$ со значениями в поле K (на каком множестве X?)

Задача 2. Нужна ли аксиома LS4? Привести пример множества с операциями сложения и умножения на числа, для которого выполняются все аксиомы линейного пространства, кроме последней.

Действительные числа сами по себе образуют линейное пространство. Именно из этого факта вытекает утверждение о том, что $\mathcal{F}(X)$ будет линейным пространством. Множество, состоящее из одного нуля, с очевидными правилами сложения и умножения на числа образует *нулевое линейное пространство* (обозначается: 0).

Линейное пространство строк K^n $(= \mathcal{M}at_{1\times n}(K))$ *и столбцов* ${}^nK$ $(= \mathcal{M}at_{n\times 1}(K))$ будут играть особую универсальную роль. Как мы увидим, к нему сводятся все n-мерные линейные пространства.

Из аксиом LS1-LS3 следует, что $0 \cdot \mathbf{a} = \mathbf{0}$. Действительно, $0 \cdot \mathbf{a} = (0+0) \cdot \mathbf{a} = 0 \cdot \mathbf{a} + 0 \cdot \mathbf{a}$, откуда и вытекает равенство $0 \cdot \mathbf{a} = \mathbf{0}$. Докажем теперь, что для любого элемента $\mathbf{a} \in L$ имеет место совпадение: $-\mathbf{a} = (-1) \cdot \mathbf{a}$. Для доказательства потребуется и последняя аксиома:

$$\mathbf{a} + (-1)\mathbf{a} = 1 \cdot \mathbf{a} + (-1)\mathbf{a} = (1 + (-1)) \cdot \mathbf{a} = 0 \cdot \mathbf{a} = \mathbf{0} \Rightarrow (-1)\mathbf{a} = -\mathbf{a}.$$

Отметим также ещё одно простое следствие аксиом LS1-LS4: $\lambda \cdot \mathbf{0} = \mathbf{0}$ для любых $\lambda \in K$. В самом деле

$$\lambda \cdot \mathbf{0} = \lambda(0 \cdot \mathbf{0}) = (\lambda \cdot 0)\mathbf{0} = 0 \cdot \mathbf{0} = \mathbf{0},$$

что завершает доказательство.

Подмножество H линейного пространства L называется *подпространством*, если $\mathbf{0} \in H$, и H замкнуто относительно операций сложения и умножения на элементы поля K:

$$a, b \in H, \lambda \in K \Rightarrow a + b \in H; \quad \lambda a \in H.$$

Всякое подпространство само по себе будет линейным пространством. Ясно также, что всё пространство L и подмножество состоящее из одного нуля, будут подпространствами в L; остальные подпространства называют *собственными*.

Задача 3. Отождествим $\mathbb{R}^2$ с множеством точек на плоскости, а $\mathbb{R}^3$ с множеством точек в пространстве. Доказать, что собственные подпространства в $\mathbb{R}^2$ исчерпываются прямыми, проходящими через начало координат, в случае $\mathbb{R}^3$ добавляются еще плоскости, проходящие через начало координат.

Рассмотрим следующую цепочку подпространств пространства функций на отрезке

$$\mathbb{R}[x] \subset C^1[a, b] \subset C[a, b] \subset \mathcal{R}[a, b] \subset \mathcal{F}[a, b]$$

Здесь $\mathcal{R}[a, b]$ все функции, для которых существует интеграл Римана $\int_a^b f(x)\,dx$; $C[a, b]$ – все непрерывные на отрезке $[a, b]$ функции, $C^1[a, b]$ – функции, имеющие непрерывную производную, $\mathbb{R}[x]$ – пространство всех многочленов. Факт, что перечисленные выше множества являются подпространствами следует из известных свойств типа: сумма непрерывных функций суть непрерывная функция и т. д.

Задача 4*. Доказать, что все включения в указанной выше цепочке действительно строгие.

Задача 5. Доказать, что следующие множества – подпространства.

- Все решения однородной системы линейных уравнений в пространстве строк.
- Все матрицы с нулевым следом в пространстве $n \times n$-матриц.
- Сходящиеся последовательности в пространстве всех последовательностей. Пространство всех последовательностей это не что иное как пространство $\mathcal{F}(\mathbb{N})$.
- Последовательности с нулевым пределом в пространстве последовательностей.
- Множество функций на отрезке $[a, b]$, имеющих нулевое значение интеграла.
- Функции из $C^1[a, b]$ имеющие нулевое значение и нулевое значение производной на фиксированных подмножествах отрезка $[a, b]$.

Пусть $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ – элементы линейного пространства L, а $\lambda_1, \lambda_2, \ldots, \lambda_n$ – элементы поля K. Выражение $\lambda_1\mathbf{a}_1 + \cdots + \lambda_n\mathbf{a}_n$ называется *линейной комбинацией* элементов $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$. Эта линейная комбинация называется *нетривиальной*, если хотя бы один из λ_i-ых отличен от нуля. В противном случае эта линейная комбинация называет-ся *тривиальной*; ее значение равно $\mathbf{0}$. Скажем, что элемент $\mathbf{b} \in L$ разложим по элементам $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$, если $\mathbf{b}$ равен какой-либо линейной комбинации этих элементов.

Множество всех линейных комбинаций образует подпространство линейного пространства L, обозначим его $K\mathbf{a}_1 + K\mathbf{a}_2 + \ldots + K\mathbf{a}_n$. Если это подпространство совпадает со всем пространством, т. е. любой элемент из L представим в виде линейной комбинации $\mathbf{a}_i$-х, то назовем систему элементов $\{\mathbf{a}_i\}$ *полной*; иными словами в этой ситуации будем говорить, что L *порождено элементами* $\{\mathbf{a}_i\}$.

Представление элемента $\mathbf{b} \in L$ в виде линейной комбинации элементов $\{\mathbf{a}_i\}$ может быть не единственным (приведите пример!). Легко видеть, что следующие два условия относительно системы векторов $\{\mathbf{a}_i\}$ $(i \in I)$ эквивалентны:

а) *любой элемент* $\mathbf{b} \in K\mathbf{a}_1 + K\mathbf{a}_2 + \ldots + K\mathbf{a}_n$ *имеет единственное разложение в виде линейной комбинации* $\mathbf{a}_i$*-х.*

б) *если* $\lambda_1\mathbf{a}_1 + \lambda_2\mathbf{a}_2 + \cdots + \lambda_n\mathbf{a}_n = \mathbf{0}$*, то* $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$.

Если выполнены эти эквивалентные условия, то элементы $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ называются *линейно независимыми.* В противном случае элементы $\mathbf{a}_1$, $\mathbf{a}_2, \dots, \mathbf{a}_n$ называются *линейно зависимыми*, т. е. элементы линейно зависимы тогда, когда существует нетривиальная линейная комбинация этих элементов, равная нулю.

Определение линейной зависимости и независимости применимо и к бесконечному семейству элементов линейного пространства. А именно, такое семейство будет линейно зависимым, если найдется конечное линейно зависимое подсемейство и будет линейно независимым, если любое конечное подсемейство линейно независимо.

Задача 6. Два геометрических вектора $\mathbf{a}, \mathbf{b} \in \mathcal{V}(\mathbb{E}^3)$ линейно зависимы тогда и только тогда, когда они коллинеарны. Аналогично три вектора линейно зависимы в том и только том случае, когда они компланарны (т. е. лежат на одной плоскости или на параллельных плоскостях).

Предложение 1.

- *Семейство элементов линейного пространства, содержащее нулевой элемент,-зависимо.*
- *Подсемейство линейно независимого семейства само линейно независимо.*
- *Надсемейство линейно зависимого семейства само линейно зависимо.*
- *Если каждый из элементов* $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m$ *линейно выражается через семейство элементов* $\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_n$ *и* $m > n$*, то элементы* $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m$ *линейно зависимы.*

Доказательство. Равенство $1 \cdot \mathbf{0} + 0\mathbf{a}_2 + \ldots + 0\mathbf{a}_m = \mathbf{0}$ является нетривиальной линейной зависимостью. Отсюда следует первое утверждение. Второе утверждение очевидно. Третье эквивалентно второму. Докажем последнее утверждение.

Пусть $\mathbf{a}_i = a_{1i}\mathbf{f}_1 + \ldots + a_{ni}\mathbf{f}_n$ – разложение элемента $\mathbf{a}_i$ по семейству $\{\mathbf{f}_j\}$ $(i = 1, 2, \ldots m)$. Однородная система линейных уравнений

$$\lambda_1 a_{j1} + \lambda_2 a_{j2} + \ldots + \lambda_m a_{jm} = 0 \qquad (j = 1, 2, \ldots, n)$$

имеет ненулевое решение $\lambda_1^*, \ldots, \lambda_m^*$, так как число уравнений n меньше чем число неизвестных m (см. §2.3, теорема 2). Тогда

$$\lambda_1^*\mathbf{a}_1 + \ldots + \lambda_m^*\mathbf{a}_m = (\sum_{i=1}^m \lambda_i^* a_{1i})\mathbf{f}_1 + \ldots + (\sum_{i=1}^m \lambda_i^* a_{ni})\mathbf{f}_n = 0 \cdot \mathbf{f}_1 + \ldots + 0 \cdot \mathbf{f}_n = \mathbf{0},$$

что и требовалось доказать. □

Задача 7. Доказать линейную независимость семейств

- $\{1, x, x^2, \ldots\}$ в пространстве многочленов $\mathbb{R}[x]$
- $e^{k_1 x}, e^{k_2 x}, \ldots e^{k_n x}$ в пространстве функций $\mathcal{F}(\mathbb{R})$ при условии, что все k_i-е попарно различны.
- $\{1, \sin x, \cos x, \sin 2x, \cos 2x, \ldots\}$ в $C[0, 2\pi]$
- семейство матриц $\{E_{ij}\}$ у которых на (i, j)-ом месте стоит 1, а на остальных местах нули в пространстве $\mathcal{M}at_{n\times m}(K)$.
- Матрицы 3×3, у которых на 8 местах стоит 1, а на остальном 0 в пространстве $\mathcal{M}at_{3\times 3}(K)$.

Задача 8. а)Найти линейную зависимость семейств функций

$$\left\{1, \cos 2x, \sin^2 x\right\}, \quad \left\{\sin 3x, \sin^3 x, \sin x\right\}, \quad \left\{e^x, e^{x+2}\right\}$$

б) Найти линейную зависимость семейства всех 2×2-матриц, у которых на двух местах единицы, а на остальных местах – нули.

3.3 Базис.

Определение 1. Упорядоченное семейство элементов линейного пространства L называется *базисом*, если через него единственным образом может быть выражен любой другой элемент в виде линейной комбинации. Коэффициенты такого выражения называются *координатами* элемента в данном базисе.

Определение базиса можно переформулировать так: упорядоченное семейство элементов линейного пространства L называется базисом, если это семейство полно и линейно независимо.

Стандартный базис в пространтве строк K^n состоит из следующих элементов:

$$\mathbf{e}_1 = (1, 0, 0, \ldots, 0),\ \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_n = (0, 0, 0, \ldots, 1)$$

Тот факт, что $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ – базис, следует из разложения

$$(x_1, x_2, \ldots, x_n) = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \ldots + x_n\mathbf{e}_n \tag{3.4}$$

Действительно, если $x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \ldots + x_n\mathbf{e}_n = \mathbf{0}$, то $x_1 = x_2 = \ldots = x_n = 0$, как сразу следует из (3.4). Доказана линейная независимость семейства $\{\mathbf{e}_i\}$. Из соотношения (3.4) вытекает и полнота этого семейства.

Заметим, что, если $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n$ – базис, то и семейство $\mathbf{f}_2, \mathbf{f}_1, \ldots, \mathbf{f}_n$, полученное перестановкой первых двух элементов, также будет базисом. Но это будет уже другой базис! Например, строка $(3, -2) \in \mathbb{R}^2$ имеет координаты 3,-2 в стандартном базисе, а в базисе $\mathbf{f_1} = \mathbf{e}_2$, $\mathbf{f_2} = \mathbf{e}_1$ имеет координаты -2,3.

Предложение 1. *Семейство* $\mathcal{F} = (\mathbf{f_i})$ *– базис пространства* L *тогда и только тогда, когда выполнено одно из условий*

1. *семейство* $(\mathbf{f_i})$ *полное и любое собственное подсемейство не является таковым;*

2. *семейство* $(\mathbf{f_i})$ *линейно независимое и любое собственное надсемейство не является таковым.*

Доказательство. $\mathcal{F}$ – базис $\Rightarrow 1$. Семейство $\mathcal{F}$ полно по определению базиса. Пусть семейство $\mathcal{F}'$ получено из $\mathcal{F}$ удалением некоторых элементов и в том числе элемента $\mathbf{f}_1$. Предположим, что семейство $\mathcal{F}'$ полно. Тогда $\mathbf{f}_1$ выражается через $\mathcal{F}'$ в виде линейной комбинации: $\mathbf{f}_1 = \lambda_2\mathbf{f}_2 + \ldots + \lambda_n\mathbf{f}_n$. Из этого следует соотношение $\mathbf{f}_1 - \lambda_2\mathbf{f}_2 - \ldots - \lambda_n\mathbf{f}_n = 0$, являющееся линейной зависимостью элементов семейства $\mathcal{F}$. Это противоречит тому, что $\mathcal{F}$ – базис. Противоречие показывает, что семейство $\mathcal{F}'$ не полно.

$1 \Rightarrow \mathcal{F}$ – базис. Надо доказать только линейную независимость системы $\mathcal{F}$. Предположим противное: существует нетривиальная линейная зависимость $\lambda_1\mathbf{f}_1 + \lambda_2\mathbf{f}_2 + \ldots + \lambda_n\mathbf{f}_n = 0$, где, скажем $\lambda_1 \neq 0$. Тогда $\mathbf{f}_1 = -\frac{\lambda_2}{\lambda_1}\mathbf{f}_2 - \ldots - \frac{\lambda_n}{\lambda_1}\mathbf{f}_n$. Обозначим через $\mathcal{F}'$ систему элементов, полученную из $\mathcal{F}$ удалением $\mathbf{f}_1$. Если $\mathbf{a} = \mu_1\mathbf{f}_1 + \ldots + \mu_n\mathbf{f}_n$ – выражение какого-либо элемента $\mathbf{a} \in L$ в виде линейной комбинации элементов из $\mathcal{F}$, то $\mathbf{a} = (\mu_1 - \frac{\lambda_2}{\lambda_1})\mathbf{f}_2 + \ldots + (\mu_n - \frac{\lambda_n}{\lambda_1})\mathbf{f}_n$ – разложение $\mathbf{a}$ по системе $\mathcal{F}'$. Следовательно, система $\mathcal{F}'$ полна. Это противоречие с условием. Противоречие показывает, что $\mathcal{F}$ – линейно независимая система.

$\mathcal{F}$ – базис $\Rightarrow 2$. $\mathcal{F}$ линейно независима по определению базиса. Если $\mathbf{a} = \lambda_1\mathbf{f}_1 + \ldots + \lambda_n\mathbf{f}_n$ – разложение какого-либо элемента $\mathbf{a} \in L$ по системе $\mathcal{F}$, то $\lambda_1\mathbf{f}_1 + \ldots + \lambda_n\mathbf{f}_n +$

$(-1)\mathbf{a} = 0$ – нетривиальная линейная зависимость. Это значит, что система, полученная из $\mathcal{F}$ добавлением элемента $\mathbf{a}$ уже будет линейно зависимой.

<u>$2 \Rightarrow \mathcal{F}$ – базис</u>. Надо доказать лишь полноту системы $\mathcal{F}$. Выберем произвольный элемент $\mathbf{a} \in L$. Так как система, полученная из $\mathcal{F}$ добавлением $\mathbf{a}$, не будет линейно независимой, то имеет место равенство

$$\mu\mathbf{a} + \lambda_1\mathbf{f}_1 + \ldots + \lambda_n\mathbf{f}_n + (-1)\mathbf{a} = 0, \tag{3.5}$$

где не все из коэффициентов $\mu, \lambda_1, \lambda_2, \ldots, \lambda_n$ равны 0. Если $\mu = 0$, то (3.5) превращается в нетривиальную линейную зависимость элементов из $\mathcal{F}$; это противоречит условию. Значит $\mu \neq 0$ и

$$\mathbf{a} = -\frac{\lambda_1}{\mu}\mathbf{f}_1 - \ldots - \frac{\lambda_n}{\mu}\mathbf{f}_n.$$

Полнота системы $\mathcal{F}$ доказана. □

Задача 1. Доказать, многочлены $1, x, x^2, x^3, \ldots$ образуют базис в пространстве $\mathbb{R}[x]$, а многочлены $1, x, x^2, x^3, \ldots, x^n$ образуют базис в пространстве $\mathcal{P}_n$ всех многочленов степени не выше, чем n.

Как видно из утверждения задачи 1 базис может содержать и бесконечное число элементов. Линейное пространство называют *бесконечномерным* и записывают $\dim L = \infty$, если никакая конечная система его элементов не является полной. Пространство L называется *конечномерным*, если существует конечная и одновременно полная система элементов. В этом случае существует базис, состоящий из конечного числа элементов, который можно получить выбрасывая из полной системы "лишние" элементы, пока не получим полную систему, удовлетворяющую первому условию предложения 1.

Теорема 1 (о размерности). *Пусть пространство L конечномерно. Тогда любой базис пространства L содержит одно и тоже количество векторов. (Это число называется* РАЗМЕРНОСТЬЮ *пространства L и обозначается $\dim L$). Любое линейно независимое семейство в количестве $\dim L$ элементов будет базисом пространства L, а также, если n элементов порождают пространство L, и $n = \dim L$, то эти элементы образуют базис.*

Доказательство. 1. Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис, а $\mathcal{E} = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m)$ – линейно независимая система элементов из L. Если $m > n$, то система $\mathcal{E}$ линейно зависима согласно предложению 1, §3.2. Это противоречие показывает, что $m \leq n$.

2. Предположим теперь, что $\mathcal{E}$ базис, а $\mathcal{F}$ – полная система. Если $m > n$, то так же, как и выше, приходим к противоречию. Следовательно, $m \leq n$.

3. Если $\mathcal{F}$ и $\mathcal{E}$ – два базиса, то $m \leq n$ согласно пункту 1 этого доказательства. Меняя местами $\mathcal{F}$ и $\mathcal{E}$, получаем неравенство $n \leq m$. Следовательно, $m = n$.

4. Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис, а $\mathcal{E} = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ – линейно независимая система. Если есть собственная надсистема системы $\mathcal{E}$, которая также линейно независима, то это будет противоречить первому пункту этого доказательства. Значит любое собственное надсемейство семейства $\mathcal{E}$ уже не будет линейно независимым. Применяя предложение 1, видим, что $\mathcal{E}$ – базис.

5. Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – полное семейство элементов пространства L, а $\mathcal{E} = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ – базис. Если какая-либо собственная подсистема системы $\mathcal{F}$ также полна, то это противоречит пункту 2 настоящего доказательства. Значит снова можно применить предложение 1, п. 1 и получить из этого, что $\mathcal{F}$ – базис. □

Следствие. *Размерность собственного подпространства конечномерного линейного пространства меньше, чем размерность всего пространства.*

Доказательство. Пусть H – подпространство пространства L, $\dim L = n$ и $H \neq L$. Согласно теореме 1 в H не может быть линейно независимого семейства более, чем из n элементов. Пусть $\mathcal{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$ – линейно независимые элементы из H с наибольшим возможным m. Тогда $\mathcal{B}$ – базис пространства H в силу предложения 1. Если $m = n$, то $\mathcal{B}$ будет также и базисом в L. Тогда $H = \sum \mathbf{b}_i K = L$ – противоречие с неравенством $H \neq L$. Итак, $\dim H = m < n = \dim L$, что и требовалось доказать. □

Задача 2*. Доказать, что пространство $\mathcal{F}[0,1]$ не имеет счетного базиса, т. е. базиса, элементы которого можно занумеровать натуральными числами.

Пусть $b_1, b_2, \ldots, b_n$ - координаты элемента $\mathbf{b}$ относительно базиса $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$, т. е.

$$\mathbf{b} = b_1\mathbf{f}_1 + b_2\mathbf{f}_2 + \ldots + b_n\mathbf{f}_n. \tag{3.6}$$

Предположим,что $\mathcal{F}' = (\mathbf{f}'_1, \ldots, \mathbf{f}'_n)$ - другой (*новый*) базис пространства L. Разложим каждый из элементов $\mathbf{f}'_i$ по базису $\mathcal{F}$:

$$\begin{cases} \mathbf{f}'_1 & = c_{11}\mathbf{f}_1 + \ldots + c_{n1}\mathbf{f}_n \\ \ldots & \ldots\ldots\ldots \\ \mathbf{f}'_n & = c_{1n}\mathbf{f}_1 + \ldots + c_{nn}\mathbf{f}_n \end{cases}$$

Матрица $C = (c_{ij})$ называется *матрицей перехода* от старого базиса к новому базису. Имеем:

$$(\mathbf{f}'_1, \ldots, \mathbf{f}'_n) = (\mathbf{f}_1, \ldots, \mathbf{f}_n)C \tag{3.7}$$

Пусть

$$\mathbf{b} = b'_1\mathbf{f}'_1 + b'_2\mathbf{f}'_2 + \ldots + b'_n\mathbf{f}'_n = (\mathbf{f}'_1, \mathbf{f}'_2, \ldots, \mathbf{f}'_n)\begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{pmatrix}$$

– разложение элемента $\mathbf{b}$ по новому базису. Подставляя сюда выражение для строки $(\mathbf{f}'_1, \mathbf{f}'_2, \ldots, \mathbf{f}'_n)$ из (3.7) и сравнивая с разложением (3.6), получим формулу перехода от новых координат к старым:

$$\begin{pmatrix} b_1 \\ . \\ . \\ . \\ b_n \end{pmatrix} = C \begin{pmatrix} b'_1 \\ . \\ . \\ . \\ b'_n \end{pmatrix}. \tag{3.8}$$

Матрица C заведомо невырождена, так как нашлись бы коэффициенты $b'_1, \ldots, b'_n$, не все равные 0, такие, что левая часть в (3.8) равна нулевому столбцу (применили теорему 2, §2.7). В этом случае элемент $\mathbf{b} = \sum_{i=1}^{n} b'_i \mathbf{f}'_i$

не равен 0, ибо семейство $\{\mathbf{f}'_i\}$ линейно независимо. С другой стороны, $\mathbf{b} = \sum_{i=1}^{n} b_i \mathbf{f}_i = \mathbf{0}$. Это противоречие показывает, что C – невырожденная матрица и, следовательно, она обратима. Умножая (3.8) слева на C^{-1}, получим формулу перехода от старых координат к новым:

$$\begin{pmatrix} b'_1 \\ . \\ . \\ . \\ b'_n \end{pmatrix} = C^{-1} \begin{pmatrix} b_1 \\ . \\ . \\ . \\ b_n \end{pmatrix}. \tag{3.9}$$

Теорема 2 (о базисе). *Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис пространства L. Семейство элементов*

$$\mathbf{b}_i = b_{1i}\mathbf{f}_1 + \ldots + b_{ni}\mathbf{f}_n \quad (1 \le i \le n)$$

образует базис в L тогда и только тогда, когда $\det(b_{ij}) \neq 0$.

Доказательство. Обозначим $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$, а через B - обозначим матрицу (b_{ij}). Далее X – произвольный столбец длины n.

$$\begin{gathered} \mathcal{B} \text{ - базис} \\ \Updownarrow \\ \mathcal{B} \text{ - линейно независимое семейство} \\ \Updownarrow \\ \mathcal{B}X = 0 \Rightarrow X = 0 \\ \Updownarrow \\ \mathcal{F}BX = 0 \Rightarrow X = 0 \\ \Updownarrow \\ BX = 0 \Rightarrow X = 0 \\ \Updownarrow \\ \det B \neq 0 \text{ (см. теорема 2, § 2.7)} \end{gathered}$$

$\square$

Следствие. *Строки* $\mathbf{b}_i = (b_{1i}, \dots b_{ni}) \in K^n$ *($1 \le i \le n$) образуют базис тогда и только тогда, когда* $\det(b_{ij}) \neq 0$.

3.4 Евклидовы пространства

Всюду в этом параграфе линейные пространства рассматриваются над полем действительных чисел.

3.4.1 Скалярное произведение геометрических векторов

Одна из важнейших физических величин, работа, в простейшем случае вычисляется по формуле $A = F \cdot a$, где F величина действующей силы, сонаправленнной с перемещением, а a – величина перемещения. Если же вектор силы $\mathbf{F}$ направлен под углом к вектору перемещения, то следует разложить силу на две составляющие $\mathbf{F} = \mathbf{F}_a + \mathbf{N}$, где вектор $\mathbf{F}_a$ коллинеарен $\mathbf{a}$, а вектор $\mathbf{N}$ ортогонален $\mathbf{a}$. Ортогональная составляющая работу не производит, и поэтому

$$A = \begin{cases} |\mathbf{F}_a||\mathbf{a}|, & \text{если } \mathbf{F}_a \text{ и } \mathbf{a} \text{ сонаправлены,} \\ -|\mathbf{F}_a||\mathbf{a}|, & \text{если } \mathbf{F}_a \text{ и } \mathbf{a} \text{ направлены в противоположные стороны.} \end{cases}$$

Нетрудно видеть, что это равенство может быть записано одной формулой $A = |\mathbf{F}||\mathbf{a}|\cos(\widehat{\mathbf{F}, \mathbf{a}})$, где $\widehat{\mathbf{F}, \mathbf{a}}$ – угол между векторами $\mathbf{F}$ и $\mathbf{a}$ (см. рис. 1).

Рис. 1. Работа силы.

Определение 1. *Скалярным произведением* геометрических векторов $\mathbf{a}$ и $\mathbf{b}$ называется произведение длин этих векторов на косинус угла между ними:

$$\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}||\mathbf{b}|\cos(\widehat{\mathbf{a}, \mathbf{b}})$$

Если один из векторов нулевой, то и скалярное произведение равно 0.

Это произведение называется скалярным, поскольку двум векторам сопоставляется число – скалярная величина.

Напомним свойства скалярного произведения. Сразу из определения следует **симметричность**: скалярное произведение не зависит от порядка сомножителей.

$$\mathbf{ab} = \mathbf{ba}.$$

Скалярным квадратом называется скалярное произведение вектора на самого себя: $\mathbf{a}^2 = \mathbf{a} \cdot \mathbf{a}$. Имеет место **положительная определенность и невырожденность** скалярного произведения:

$$\mathbf{a}^2 \geq 0 \quad \text{и} \quad \mathbf{a}^2 = 0 \Leftrightarrow \mathbf{a} = \mathbf{0}.$$

В частности, длина вектора выражается через скалярное произведение следующим образом:

$$|\mathbf{a}| = \sqrt{\mathbf{a}^2} \tag{3.10}$$

Угол между ненулевыми векторами также выражается через скалярное произведение, ибо

$$\cos(\widehat{\mathbf{a}, \mathbf{b}}) = \frac{\mathbf{a} \cdot \mathbf{b}}{|\mathbf{a}||\mathbf{b}|} \qquad (\mathbf{a} \neq \mathbf{0}, \mathbf{b} \neq \mathbf{0}) \tag{3.11}$$

В формулах (3.10) и (3.11) заключается геометрический смысл скалярного произведения, оно задает евклидову геометрию в пространстве.

Если векторы ортогональны, т. е. лежат на перпендикулярных прямых, то скалярное произведение равно нулю. Очевидно верно и обратное утверждение. Таким образом, мы получаем **критерий ортогональности:**

$$\mathbf{a} \perp \mathbf{b} \Leftrightarrow \mathbf{a} \cdot \mathbf{b} = 0$$

В частности, имеет место **ортонормированность стандартного базиса**:

$$\mathbf{ij} = \mathbf{jk} = \mathbf{ki} = 0; \qquad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = 1. \tag{3.12}$$

Для доказательства следующего свойства реализуем вектора $\mathbf{a}, \mathbf{b}, \mathbf{c}$ в одной точке O, и прямую ℓ, на которой лежит вектор $\mathbf{a}$, превратим в ось Ox, выбрав положительное направление по вектору $\mathbf{a}$. Будем обозначать X_b, X_c, X_{b+c} координаты векторов $\mathbf{b}, \mathbf{c}, \mathbf{b} + \mathbf{c}$ на оси Ox. Тогда

$$\mathbf{a}(\mathbf{b} + \mathbf{c}) = |\mathbf{a}||\mathbf{b} + \mathbf{c}| \cos(\mathbf{b} + \mathbf{c}, x) = |\mathbf{a}| X_{\mathbf{b}+\mathbf{c}} =$$
$$= |\mathbf{a}|(X_b + X_c) = |\mathbf{a}| X_b + |\mathbf{a}| X_c = |\mathbf{a}||\mathbf{b}| \cos(\mathbf{b}, x) + |\mathbf{a}||\mathbf{c}| \cos(\mathbf{c}, x) = \mathbf{ab} + \mathbf{ac}$$

мы применили формулу (3.2) – координата вектора по оси Ох равна произведению длины этого вектора на направляющий косинус, а также применили правило покоординатного сложения векторов. Итак, мы доказали **билинейность**:

$$\mathbf{a}(\mathbf{b} + \mathbf{c}) = \mathbf{ab} + \mathbf{ac}; \;\; (\mathbf{a} + \mathbf{b})\mathbf{c} = \mathbf{ac} + \mathbf{bc}; \;\; \mathbf{a}(\lambda \mathbf{b}) = (\lambda \mathbf{a})\mathbf{b} = \lambda(\mathbf{ab}).$$

Действительно, равенство $(\mathbf{a}+\mathbf{b})\mathbf{c} = \mathbf{ac}+\mathbf{bc}$ верно в силу симметричности скалярного произведения, а равенство $\mathbf{a}(\lambda\mathbf{b}) = \lambda\mathbf{ab}$ доказывается, как и выше:

$$\mathbf{a}(\lambda\mathbf{b}) = |\mathbf{a}|X_{\lambda\mathbf{b}} = |\mathbf{a}|\lambda X_b = \lambda|\mathbf{a}||\mathbf{b}|\cos(\widehat{\mathbf{a},\mathbf{b}}) = \lambda\mathbf{ab}$$

Теорема 1 (вычисление скалярного произведения в координатах). *Если* $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$ *и* $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$*, то*

$$\mathbf{a}\cdot\mathbf{b} = X_1X_2 + Y_1Y_2 + Z_1Z_2 \tag{3.13}$$

Доказательство. Применяем билинейность и учитываем (3.12). □

Следствие. *Если вектора* $\mathbf{a}$ *и* $\mathbf{b}$ *ненулевые, то*

$$\cos(\widehat{\mathbf{a},\mathbf{b}}) = \frac{X_1X_2 + Y_1Y_2 + Z_1Z_2}{\sqrt{X_1^2+Y_1^2+Z_1^2}\sqrt{X_2^2+Y_2^2+Z_2^2}} \tag{3.14}$$

В частности, вектора $\mathbf{a}$ *и* $\mathbf{b}$ *ортогональны тогда и только тогда, когда* $X_1X_2 + Y_1Y_2 + Z_1Z_2 = 0$.

3.4.2 Скалярное произведение в вещественных линейных пространствах

Мы уже отмечали выше, что скалярное произведение задает как длины, так и углы в пространстве. Именно этот факт и положен в основу построения геометрии Евклида в многомерных пространствах.

Определение 1. Пусть L - линейное пространство над полем действительных чисел. Отображение $L\times L\to\mathbb{R}$ (любым двум элементам $\mathbf{a},\mathbf{b}\in L$ ставится в соответствие число $\mathbf{a}\cdot\mathbf{b}$) называется *скалярным произведением*, если оно удовлетворяет следующим свойствам

СК1 (билинейность)

$$(\mathbf{a}_1+\mathbf{a}_2)\mathbf{b} = \mathbf{a}_1\mathbf{b}+\mathbf{a}_2\mathbf{b};\quad \mathbf{a}(\mathbf{b}_1+\mathbf{b}_2) = \mathbf{ab}_1+\mathbf{ab}_2;$$

$$\lambda(\mathbf{ab}) = (\lambda\mathbf{a})\mathbf{b} = \mathbf{a}(\lambda\mathbf{b}).$$

СК2 (симметричность) $\mathbf{ab} = \mathbf{ba}$

СК3 (положительная определенность)

$$\mathbf{a}^2 = \mathbf{aa} \geq 0$$

СК4 (невырожденность)

$$\mathbf{a}^2 = 0 \Longleftrightarrow \mathbf{a} = \mathbf{0}.$$

для любых $\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{b}, \mathbf{b}_1, \mathbf{b}_2 \in L$ и $\lambda \in \mathbb{R}$.

Иногда приходится обозначать скалярное произведение по другому. Например, в функциональном анализе скалярное произведение между двумя функциями обозначают $(f(x), g(x))$; обозначение $f(x) \cdot g(x)$ зарезервировано за операцией произведения функций. Ясно, что *умножение скалярного произведения на положительное число дает снова скалярное произведение.* Далее:

$$\mathbf{0} \cdot \mathbf{b} = (\mathbf{0} + \mathbf{0})\mathbf{b} = \mathbf{0}\mathbf{b} + \mathbf{0}\mathbf{b},$$

откуда следует равенство $\mathbf{0}\mathbf{b} = 0$ для любого элемента $\mathbf{b} \in L$.

Примеры скалярных произведений

1. *Стандартное скалярное произведение в пространстве строк* $\mathbb{R}^n$ определяется так:

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n. \tag{3.15}$$

Тот факт, что правило (3.15) задает скалярное произведение, проверяется непосредственно.

2. В пространстве непрерывных функций $C[a, b]$ формула $(f(x), g(x)) = \int_a^b f(x) g(x)\, dx$ задает скалярное произведение. В данном случае проверка последней аксиомы является наиболее сложной задачей. Оставляем это читателю.

Для любых двух элементов $\mathbf{a}$ и $\mathbf{b}$ пространства со скалярным произведением имеет место **неравенство Коши-Буняковского-Римана-Шварца**:

$$(\mathbf{ab})^2 \le \mathbf{a}^2 \mathbf{b}^2 \tag{3.16}$$

При этом равенство в (3.16) имеет место тогда и только тогда, когда элементы $\mathbf{a}$ *и* $\mathbf{b}$ *линейно зависимы.*

Докажем неравенство (3.16). Если $\mathbf{a} = \mathbf{0}$, то вектора $\mathbf{a}$ и $\mathbf{b}$ линейно зависимы и равенство (3.16) очевидно. Предположим теперь, что $\mathbf{a}$ – ненулевой элемент. Рассмотрим квадратный трехчлен

$$f(t) = (t\mathbf{a} + \mathbf{b})^2 = t^2 \mathbf{a}^2 + 2t\mathbf{ab} + \mathbf{b}^2.$$

Согласно СК3 имеем неравенство $f(t) \ge 0$ для всех чисел t. Тогда дискриминант этого квадратного трехчлена меньше либо равен нулю. Отсюда $4(\mathbf{ab})^2 - 4\mathbf{a}^2\mathbf{b}^2 \le 0$, и неравенство Коши-Буняковского следует.

Предположим теперь, что в (3.16) имеет место равенство. Тогда найдется число t такое, что $f(t) = 0$. В силу невырожденности скалярного произведения, получаем: $t\mathbf{a} + \mathbf{b} = \mathbf{0}$. Тем самым элементы $\mathbf{a}$ и $\mathbf{b}$ зависимы в этом случае. Наоборот, если эти вектора линейно зависимы, то $\mathbf{b}$ выражается через $\mathbf{a}$, т. е. $\mathbf{b} = s\mathbf{a}$ для некоторого

$s \in \mathbb{R}$. Отсюда $f(-s) = 0$, значит и дискриминант равен 0. Это влечет равенство в (3.16).

Величину $|\mathbf{a}| = \sqrt{\mathbf{a}^2}$ называют *нормой* или *длиной* элемента $\mathbf{a} \in L$. *Углом* $\widehat{\mathbf{a}, \mathbf{b}}$ между ненулевыми элементами $\mathbf{a}, \mathbf{b}$ пространства L со скалярным произведением назовем число $\varphi \in [0, \pi]$ такое, что

$$\cos\varphi = \frac{\mathbf{ab}}{|\mathbf{a}||\mathbf{b}|} \tag{3.17}$$

Это определение корректно, т. е. число φ существует и единственно, так как абсолютная величина дроби $\frac{\mathbf{ab}}{|\mathbf{a}||\mathbf{b}|}$ меньше единицы, что следует из неравенства Коши-Буняковского.

Два элемента пространства со скалярным произведением называются *ортогональными*, если либо один из них нулевой, либо угол между ними равен $\frac{\pi}{2}$. Обозначаем ортогональность так: $\mathbf{a} \perp \mathbf{b}$. Из формулы (3.17) вытекает **критерий ортогональности**:

- *Элементы* $\mathbf{a}, \mathbf{b} \in L$ *ортогональны тогда и только тогда, когда* $\mathbf{ab} = 0$.

Основные свойства длины и угла

А. $|\mathbf{a}| \geq 0$ *и* $|\mathbf{a}| = 0$ *тогда и только тогда, когда* $\mathbf{a} = \mathbf{0}$.

Б. $|\lambda\mathbf{a}| = |\lambda||\mathbf{a}|$ *для любых* $\lambda \in \mathbb{R}$ *и* $\mathbf{a} \in L$.

В. *(неравенство треугольника)* $|\mathbf{a} + \mathbf{b}| \leq |\mathbf{a}| + |\mathbf{b}|$. *Более общо:* $|\sum_{i=1}^{n} \mathbf{a}_i| \leq \sum_{i=1}^{n} \|\mathbf{a}_i|$

Г. *Для любых двух векторов имеет место равенство* $\widehat{\mathbf{a}, \mathbf{b}} = \widehat{\mathbf{b}, \mathbf{a}}$.

Д. *Равенство* $\widehat{\mathbf{a}, \mathbf{b}} = 0$ *выполняется в том и только том случае, когда* $\mathbf{b} = \lambda\mathbf{a}$ *для некоторого положительного* λ*;* $\widehat{\mathbf{a}, \mathbf{b}} = \pi$ *в том и только том случае, когда* $\mathbf{b} = \lambda\mathbf{a}$ *для некоторого* $\lambda < 0$.

Е. *Для любых трех ненулевых векторов имеет место неравенство*

$$\widehat{\mathbf{a}, \mathbf{c}} \leq \widehat{\mathbf{a}, \mathbf{b}} + \widehat{\mathbf{b}, \mathbf{c}}$$

Если здесь имеет место равенство, то будем говорить, что вектор $\mathbf{b}$ лежит между векторами $\mathbf{a}$ и $\mathbf{c}$.

Задача 1. Доказать свойства А, Б, В, Г, Д, Е.

Определение 2. Базис $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ евклидова пространства L называется *ортогональным*, если $\mathbf{f}_i \perp \mathbf{f}_j$ для всех пар (i, j) с $i \neq j$. Если, кроме того, длины всех элементов $\mathbf{f}_i$ равны единице, то базис $\mathcal{F}$ называется *ортонормированным*.

Следующее предложение может быть проверено непосредственно.

Предложение 1. *Стандартный базис пространства строк ортонормирован относительно стандартного скалярного произведения.*

Определение 3. Конечномерное линейное пространство со скалярным произведением называется *евклидовым пространством.*

Заметим, что если ненулевые вектора $\mathbf{f}_1, \ldots, \mathbf{f}_n$ пространства L со скалярным произведением попарно ортогональны, то они линейно независимы. В самом деле, из линейной зависимости $\lambda_1\mathbf{f}_1 + \ldots + \lambda_n\mathbf{f}_n = \mathbf{0}$, после умножения на $\mathbf{f}_1$, вытекает равенство $\lambda_1\mathbf{f}_1^2 = 0$, ибо $\mathbf{f}_1\mathbf{f}_i = 0$ при $i \neq 1$. Отсюда следует, что $\lambda_1 = 0$. Аналогично доказывается, что $\lambda_2 = \ldots = \lambda_n = 0$. Если дополнительно предположить, что $\dim L = n$, то вектора $\mathbf{f}_1, \ldots, \mathbf{f}_n$ образуют базис евклидова пространства L, а их орты - $\mathbf{f}_1^o, \ldots, \mathbf{f}_n^o$ будут ортонормированным базисом. Для доказательства этого утверждения достаточно применить теорему 1 о размерности §3.3.

Теорема 2 (о разложении вектора по ортонормированному базису). *Пусть* $\mathbf{f}_1, \ldots, \mathbf{f}_n$ *– ортонормированный базис евклидова пространства, и* $\mathbf{b}$ *– какой-либо элемент этого пространства. Тогда*

$$\mathbf{b} = (\mathbf{b}\mathbf{f}_1)\mathbf{f}_1 + \ldots + (\mathbf{b}\mathbf{f}_n)\mathbf{f}_n,$$

т. е. i*-ая координата разложения элемента* $\mathbf{b}$ *по этому базису равна скалярному произведению* $\mathbf{b}\mathbf{f}_i$*.*

Доказательство. Пусть $\mathbf{b} = x_1\mathbf{f}_1 + \ldots + x_n\mathbf{f}_n$ – разложение элемента $\mathbf{b}$ по базису $(\mathbf{f}_i)$. Умножая это разложение скалярно на $\mathbf{f}_k$, получим

$$\mathbf{b}\mathbf{f}_k = x_1 \cdot 0 + \ldots + x_k \cdot 1 + \ldots + x_n \cdot 0 = x_k,$$

что и требовалось доказать. □

Задача 2. Проверить, что функции $\frac{1}{2}$, $\sin x$, $\cos x$, $\sin 2x$, $\cos 2x$,…, $\sin nx$, $\cos nx$,.. образуют ортонормированную систему относительно скалярного произведения $\frac{1}{\pi}\int_{-\pi}^{\pi} f(x)g(x)\,dx$.

3.4.3 Ортогональные дополнения

Пусть H - подпространство пространства L со скалярным произведением. Тогда множество

$$H^\perp = \{\mathbf{v} \in L \,|\, \mathbf{v}\mathbf{w} = 0 \text{ для любых } \mathbf{w} \in H\}$$

назовем *ортогональным дополнением подпространства* H*.*

Ясно, что $\mathbf{0}^\perp = L$ и $L^\perp = \mathbf{0}$. Но может быть равенство $H^\perp = \mathbf{0}$ и для собственного подпространства H пространства L. Например, рассмотрим пространство непрерывных функций $L = C[-\pi, \pi]$ со скалярным произведением $\frac{1}{\pi}\int_{-\pi}^{\pi} f(x)g(x)\,dx$. Тогда

система функций $(1/2, \sin x, \cos x,$
$\sin 2x, \cos 2x, \ldots)$ ортонормирована и пространство H, ей порожденное, плотно в L в том смысле, что если для функции $f(x) \in L$ имеют место равенства

$$\int_{-\pi}^{\pi} f(x) \sin nx \, dx = \int_{-\pi}^{\pi} f(x) \cos nx \, dx = 0$$

для любого натурального n, то функция $f(x)$ тождественно равна 0. Доказательство этого факта мы здесь не приводим (см. [П, гл. 17, §10]). Следовательно, имеет место равенство $H^{\perp} = \mathbf{0}$, хотя не всякая функция из L является тригонометрическим многочленом. Отметим простейшие свойства ортогонального дополнения.

А. $H^{\perp}$ – *подпространство.*

Действительно, если $\mathbf{v}_1, \mathbf{v}_2 \in H^{\perp}$ и элемент $\mathbf{w} \in H$ произволен, то

$$(\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2)\mathbf{w} = \lambda_1(\mathbf{v}_1 \mathbf{w}) + \lambda_2(\mathbf{v}_2 \mathbf{w}) = 0$$

для любых $\lambda_1, \lambda_2 \in \mathbb{R}$. Отсюда и следует утверждение.

Б. $H \cap H^{\perp} = 0$

Это равенство – следствие невырожденности скалярного произведения.

В. *Если $H_1 \subseteq H_2$ для двух подпространств, то $H_1^{\perp} \supseteq H_2^{\perp}$;*

Г. $H^{\perp\perp} \supseteq H$.

Действительно, если $\mathbf{v} \in H$ и $\mathbf{w} \in H^{\perp}$ – произвольны, то $\mathbf{wv} = \mathbf{vw} = 0$, откуда и следует утверждение. Пример тригонометрической ортонормированной системы, приведенный выше, показывает, что равенства в общем случае здесь может и не быть.

Любое подпространство H абстрактного линейного пространства L имеет дополнение: такое подпространство W, что $H \cap W = 0$ и $H + W = L$. Для доказательства этого утверждения достаточно продолжить какой-либо базис подпространства H до базиса всего пространства, и в качестве W взять линейную оболочку базисных векторов не вошедших в H. Для пространств со скалярным произведением ортогональное дополнение $W = H^{\perp}$ может не обладать свойством $H + W = L$, как показывает пример, приведенный выше, но если H конечномерно, то это заведомо так. Для того чтобы доказать это важное утверждение, а также обеспечить существование хотя бы одного ортонормированного базиса в евклидовом пространстве, докажем сначала теорему.

Теорема 3 (об ортогональной проекции). *Пусть H – конечномерное подпространство в L, имеющее ортонормированный базис*
$\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_k)$, и $\mathbf{a} \in L$ – какой-либо элемент. Тогда

$$\mathbf{a}_H = (\mathbf{f}_1\mathbf{a})\mathbf{f}_1 + (\mathbf{f}_2\mathbf{a})\mathbf{f}_2 + \ldots + (\mathbf{f}_k\mathbf{a})\mathbf{f}_k$$

будет ОРТОГОНАЛЬНОЙ ПРОЕКЦИЕЙ $\mathbf{a}$ *на* H*, т. е.*

$$\mathbf{a}_H \in H, \qquad \mathbf{a} - \mathbf{a}_H \in H^{\perp}$$

.
В частности,

$$H + H^{\perp} = L,$$

т. е. любой элемент из L *представим в виде суммы элементов из* H *и* $H^{\perp}$*. Для любого элемента* $\mathbf{b} \in H$ *имеет место неравенство*

$$|\mathbf{a} - \mathbf{a}_H| \leq |\mathbf{a} - \mathbf{b}|$$

и равенство здесь достигается только в случае $\mathbf{b} = \mathbf{a}_H$*.*

Если к тому же $\mathbf{a} \notin H$*, то и* $\mathbf{a} - \mathbf{a}_H \notin H$ *и семейство* $(\mathcal{F}, (\mathbf{a} - \mathbf{a}_H)^0)$ *образует ортонормированный базис пространства* $H + \mathbf{a}\mathbb{R}$ *(рис. 2).*

Рис. 2. Ортогональная проекция

Доказательство. Легко проверяется с использованием ортогональности элементов $\mathbf{f}_i$, что $\mathbf{a}_H\mathbf{f}_i = \mathbf{a}\mathbf{f}_i$ для любого i. Отсюда следует, что $\mathbf{a} - \mathbf{a}_H \in H^{\perp}$. Далее, $\mathbf{a} = \mathbf{a}_H + (\mathbf{a} - \mathbf{a}_H)$ – искомое разложение в сумму компонент из H и $H^{\perp}$ соответственно. Пусть $\mathbf{b} \in H$. Тогда

$$(\mathbf{a} - \mathbf{b})^2 = (\mathbf{a} - \mathbf{a}_H + \mathbf{a}_H - \mathbf{b})^2) =$$
$$= (\mathbf{a} - \mathbf{a}_H)^2 + 2(\mathbf{a} - \mathbf{a}_H)(\mathbf{a}_H - \mathbf{b}) + (\mathbf{a}_H - \mathbf{b})^2 = (\mathbf{a} - \mathbf{a}_H)^2 + (\mathbf{a}_H - \mathbf{b})^2$$

(теорема Пифагора). Отсюда следует требуемое решение экстремальной задачи: величина $|\mathbf{a} - \mathbf{b}|$ достигает наименьшего значения только для $\mathbf{b} = \mathbf{a}_H$.

Если $\mathbf{a} - \mathbf{a}_H \in H$, то $\mathbf{a} - \mathbf{a}_H \in H \cap H^{\perp} = 0$, откуда $\mathbf{a} = \mathbf{a}_H \in H$. Значит, если $\mathbf{a} \notin H$, то $\mathbf{a} - \mathbf{a}_H \notin H$. Так как $\mathbf{a}_H \in H$, то $(\mathbf{a} - \mathbf{a}_H)^0\mathbb{R} + H = \mathbf{a}\mathbb{R} + H$. Это завершает доказательство теоремы. $\square$

Следствие. *В евклидовом пространстве L существует ортонормированный базис и для любого подпространства H имеют место равенства*

$$\dim H + \dim H^{\perp} = \dim L; \quad H = (H^{\perp})^{\perp} \tag{3.18}$$

Более того, любой ортонормированный базис подпространства H можно продолжить до ортонормированного базиса всего пространства L.

Доказательство. Используем индукцию по размерности пространства L. Если $\dim L = 1$, то все утверждения тривиальны. Предположим, что утверждение доказано для всех евклидовых пространств размерности $< n$ и сейчас $\dim L = n$.

Случай 1. $0 \neq H \neq L$. Тогда $\dim H < \dim L$ (следствие теоремы о размерности, §3.3), и в H существует ортонормированный базис $\mathbf{f}_1, \ldots, \mathbf{f}_k$ по предположению индукции. Далее, $H^{\perp} \neq L$ (например, $\mathbf{f}_1 \notin H^{\perp}$), значит и в $H^{\perp}$ найдется ортонормированный базис $\mathbf{f}_{k+1}, \ldots, f_m$. Семейство $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_m)$ состоит из попарно ортогональных элементов; следовательно, оно линейно независимо (см. абзац после определения 3). С другой стороны, $H + H^{\perp} = L$ по только что доказанной теореме. Значит, семейство $\mathcal{F}$ полно. Следовательно, $\mathcal{F}$ – ортонормированный базис в L, и $m = n$, а

$$\dim H + \dim H^{\perp} = k + (n - k) = n = \dim L.$$

Второе равенство в (3.18) следует из включения Г и совпадения размерностей:

$$\dim(H^{\perp})^{\perp} = n - \dim H^{\perp} = n - (n - \dim H) = \dim H$$

Случай 2. $H = L$. Тогда $H^{\perp} = 0$ и утверждения следствия – тривиальности.

Случай 3. $H = 0$. Тогда $H^{\perp} = L$ и соотношения (3.18) – тривиальности. Докажем последнее утверждение следствия в этом случае. Возьмем $H_1 = \mathbf{f}_1\mathbb{R}$, где $\mathbf{f}_1$ – какой-либо единичный вектор и применим к подпространству H_1 либо случай 1, либо случай 2. □

Задача 4. Пусть H_1, H_2 – два подпространства евклидова пространства. Тогда

$$(H_1 + H_2)^{\perp} = H_1^{\perp} \cap H_2^{\perp} \text{ и } (H_1 \cap H_2)^{\perp} = H_1^{\perp} + H_2^{\perp}$$

3.5 Векторное произведение

3.5.1 Бивекторы

Если вектор – это направленный отрезок, то бивектор это площадка на плоскости с выбранным направлением вращения плоскости (рис. 1, а)). Мы знаем, что два вектора равны тогда и только тогда, когда они сонаправлены и их длины совпадают. Подобно этому два бивектора равны, если и только если они лежат в одинаковых или параллельных плоскостях, их площади совпадают, а также совпадают направления вращения плоскостей (рис. 1, б)).

Рис 1. Равенство бивекторов

Одной из задач физики, в которой требуется привлечение понятия бивектора, является вычисление момента силы $\mathbf{F}$ относительно точки O. Предположим, что сила $\mathbf{F}$ приложена в точке A. Можно себе представить вектор $\mathbf{a} = \overrightarrow{OA}$ рычагом с шарниром в точке O позволяющим рычагу двигаться во все стороны (рис. 2).

Рис 2. Момент силы.

В этой ситуации сила $\mathbf{F}$ создает вращательный момент $\mathbf{M}$. Нетрудно сообразить, что рычаг начнет вращаться в плоскости τ, проходящей через точку O и коллинеарной векторам $\mathbf{a}$ и $\mathbf{F}$. Гораздо труднее догадаться, что момент другой силы $\mathbf{G}$, приложенной в точке B, относительно той же точки O будет равен $\mathbf{M}$, если и только, если а) точка B принадлежит плоскости τ, б) площади параллелограммов, построенных на векторах $\mathbf{G}$ и $\mathbf{b} = \overrightarrow{OB}$, а также векторах $\mathbf{F}$ и $\mathbf{a}$ совпадают, и в) сила $\mathbf{F}$ вращает "рычаг" $\mathbf{a}$ в ту же сторону, что и $\mathbf{G}$ вращает $\mathbf{b}$. Иными словами, величина момента $\mathbf{M}$ должна быть пропорциональна $|\mathbf{F}|\,|\mathbf{a}|\sin(\widehat{\mathbf{F},\mathbf{a}})$.

Приведем формальные определения. Пусть L – линейное пространство над полем K. *Бивектор* – это выражение вида

$$\mathbf{g} = r_1\mathbf{a}_1 \wedge \mathbf{b}_1 + r_2\mathbf{a}_2 \wedge \mathbf{b}_2 + \ldots + r_m\mathbf{a}_m \wedge \mathbf{b}_m, \tag{3.19}$$

где $r_i \in K$, $\mathbf{a}_i, \mathbf{b}_i \in L$. Считаем, что бивектор $\mathbf{g}$ равен бивектору

$$\mathbf{g}' = r_1'\mathbf{a}_1' \wedge \mathbf{b}_1' + r_2'\mathbf{a}_2' \wedge \mathbf{b}_2' + \ldots + r_{m'}'\mathbf{a}_{m'}' \wedge \mathbf{b}_{m'}' \tag{3.20}$$

в том и только том случае, когда $\mathbf{g}$ можно получить из $\mathbf{g}'$ применением следующих правил:

а) Перестановка слагаемых в сумме вида (3.19).

б) Линейность по каждому из аргументов в любом слагаемом $r_i\mathbf{a}_i \wedge \mathbf{b}_i$, т. е. замена $(r' + r'')\mathbf{a} \wedge \mathbf{b}$ на $r'\mathbf{a} \wedge \mathbf{b} + r''\mathbf{a} \wedge \mathbf{b}$; $r(\mathbf{a}' + \mathbf{a}'') \wedge \mathbf{b}$ на $r\mathbf{a}' \wedge \mathbf{b} + r\mathbf{a}'' \wedge \mathbf{b}$; $r\mathbf{a} \wedge (\mathbf{b}' + \mathbf{b}'')$ на $r\mathbf{a} \wedge \mathbf{b}' + r\mathbf{a} \wedge \mathbf{b}''$ и $(\lambda r)\mathbf{a} \wedge \mathbf{b}$ на $r(\lambda\mathbf{a}) \wedge \mathbf{b}$ или на $r\mathbf{a} \wedge (\lambda\mathbf{b})$ и наоборот.

в) Кососимметричность: замена $\mathbf{a} \wedge \mathbf{b}$ на $-\mathbf{b} \wedge \mathbf{a}$ (Если в поле K 2=0, то добавляем возможность замены $\mathbf{a} \wedge \mathbf{a}$ на $\mathbf{0} \wedge \mathbf{0}$ и наоборот.)

Заметим, что если $\mathbf{g}'$ можно получить из $\mathbf{g}$ применением коммутативности, линейности и кососимметричности, то и $\mathbf{g}$ получается из $\mathbf{g}'$ обратной цепочкой преобразований. Далее, если бивектор $\mathbf{g}''$ получается из $\mathbf{g}'$, а $\mathbf{g}'$ получается из $\mathbf{g}$ применением правил а), б), в), то и $\mathbf{g}''$ получается из $\mathbf{g}$ применением этих же правил. Это доказывает корректность введения определения равенства двух бивекторов.

Например, если $L = \mathcal{V}(\mathbb{E}^3)$, то

$$(2\mathbf{i}+\mathbf{j}+\mathbf{k})\wedge(\mathbf{i}-\mathbf{j}) = 2\mathbf{i}\wedge\mathbf{i}+\mathbf{j}\wedge\mathbf{i}+\mathbf{k}\wedge\mathbf{i}-2\mathbf{i}\wedge\mathbf{j}-\mathbf{j}\wedge\mathbf{j}-\mathbf{k}\wedge\mathbf{j}=$$
$$=-\mathbf{i}\wedge\mathbf{j}+\mathbf{k}\wedge\mathbf{i}-2\mathbf{i}\wedge\mathbf{j}-\mathbf{j}\wedge\mathbf{k}=-3\mathbf{i}\wedge\mathbf{j}+\mathbf{j}\wedge\mathbf{k}+\mathbf{k}\wedge\mathbf{i}.$$

Символ $\wedge$ – знак внешнего произведения, т. е. аргументы $\mathbf{c}$ и $\mathbf{d}$ – вектора, а $\mathbf{c}\wedge\mathbf{d}$ – новый объект, не принадлежащий пространству векторов.

Задача 1. Доказать, что если пары векторов $(\mathbf{c},\mathbf{d})$, $(\mathbf{c}',\mathbf{d}')$, лежащие в одной плоскости таковы, что площади параллелограммов, построенных на этих векторах, совпадают, а также совпадают направления вращения от $\mathbf{c}$ к $\mathbf{d}$ и от $\mathbf{c}'$ к $\mathbf{d}'$, то $\mathbf{c}\wedge\mathbf{d}=\mathbf{c}'\wedge\mathbf{d}'$. Для этого надо сначала доказать, что при сделанных предположениях найдется 2×2-матрица $\begin{pmatrix} x & y\\ z & t\end{pmatrix}$ с единичным определителем такая, что

$$(\mathbf{c},\mathbf{d}) = (\mathbf{c}',\mathbf{d}')\begin{pmatrix} x & y\\ z & t\end{pmatrix}.$$

Далее учесть, что

$$\begin{pmatrix} x & y\\ z & t\end{pmatrix} = \begin{pmatrix} 1 & t^{-1}y\\ 0 & 1\end{pmatrix}\begin{pmatrix} x-t^{-1}zy & 0\\ 0 & t\end{pmatrix}\begin{pmatrix} 1 & 0\\ t^{-1}z & 1\end{pmatrix}.$$

Множество всех бивекторов, обозначим его $L\wedge L$, превратим в линейное пространство, для чего сначала определим сложение бивекторов и умножение бивектора на элемент поля K. Если $\mathbf{g}$, как и выше в (3.19), а $\mathbf{f}=\sum_{i=1}^{i=k} s_i\mathbf{c}_i\wedge\mathbf{d}_i$, то

$$\mathbf{g}+\mathbf{f}=\sum_{i=1}^{i=m} r_i\mathbf{a}_i\wedge\mathbf{b}_i+\sum_{i=1}^{i=k} s_i\mathbf{c}_i\wedge\mathbf{d}_i,\quad \lambda\cdot\mathbf{f}=\lambda\sum_{i=1}^{i=m}(\lambda s_i)\mathbf{c}_i\wedge\mathbf{d}_i$$

Выполнены все аксиомы линейного пространства. Роль нулевого элемента играет бивектор $\mathbf{0}\wedge\mathbf{0}$ (обозначаем его далее как $\mathbf{0}$). Действительно,

$$\mathbf{a}\wedge\mathbf{b}+\mathbf{0}\wedge\mathbf{0}=\mathbf{a}\wedge\mathbf{b}+\mathbf{0}\wedge 0\cdot\mathbf{b}=\mathbf{a}\wedge\mathbf{b}+0\cdot\mathbf{0}\wedge\mathbf{b}=(\mathbf{a}+0\cdot\mathbf{0})\wedge\mathbf{b}=\mathbf{a}\wedge\mathbf{b}.$$

Противоположным к бивектору $\mathbf{g}$ будет бивектор $(-1)\mathbf{g}$. Это следует из замечания: *если* $\mathbf{a}\parallel\mathbf{b}$, *то* $\mathbf{a}\wedge\mathbf{b}=\mathbf{0}$. Докажем это. Коллинеарность означает, что $\mathbf{a}=\lambda\mathbf{b}$, либо $\mathbf{b}=\lambda\mathbf{a}$ для некоторого числа λ. Достаточно разобрать первый случай.

$$\mathbf{a}\wedge\mathbf{b}=(\lambda\mathbf{b})\wedge\mathbf{b}=\lambda(\mathbf{b}\wedge\mathbf{b})$$

Но $\mathbf{b}\wedge\mathbf{b}=-\mathbf{b}\wedge\mathbf{b}$ в силу кососимметричности. Отсюда $2\mathbf{b}\wedge\mathbf{b}=\mathbf{0}$ и, значит $\mathbf{b}\wedge\mathbf{b}=\mathbf{0}$.

Теорема 1. *Пусть L – конечномерное пространство с базисом $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$. Тогда $L \wedge L$ пространство размерности $C_n^2 = \frac{n(n-1)}{2}$, где семейство бивекторов $\{\mathbf{f}_i \wedge \mathbf{f}_j\}$ $(1 \leq i < j \leq n)$ является базисом.*

Доказательство. Так как

$$(\sum_{i=1}^{n} r_i \mathbf{f}_i) \wedge (\sum_{j=1}^{n} s_j \mathbf{f}_j) = (\sum_{1 \leq i,j \leq n} r_i s_j \mathbf{f}_i \wedge \mathbf{f}_j)$$

и $\mathbf{f}_i \wedge \mathbf{f}_j = -\mathbf{f}_j \wedge \mathbf{f}_i$ в силу билинейности и кососимметричности, то система $\{\mathbf{f}_i \wedge \mathbf{f}_j\}$ $(1 \leq i < j \leq n)$ полна. Предположим, что она линейно зависима. Тогда один из бивекторов, скажем $\mathbf{f}_1 \wedge \mathbf{f}_2$, линейно выражается через остальные:

$$\mathbf{f}_1 \wedge \mathbf{f}_2 = \sum_{i<j,(i,j) \neq (1,2)} r_{ij} \mathbf{f}_i \wedge \mathbf{f}_j \tag{3.21}$$

По определению равенства это значит, что от левой части в (3.19) можно перейти к правой части преобразованиями а), б), в). С каждой записью вида (3.19) свяжем сумму определителей

$$r_1 \begin{vmatrix} a_{11} & a_{12} \\ b_{11} & b_{12} \end{vmatrix} + r_2 \begin{vmatrix} a_{21} & a_{22} \\ b_{21} & b_{22} \end{vmatrix} + \ldots + r_m \begin{vmatrix} a_{m1} & a_{m2} \\ b_{m1} & b_{m2} \end{vmatrix}, \tag{3.22}$$

где $\mathbf{a}_i = \sum_{j=1}^{n} a_{ij} \mathbf{f}_j$ и $\mathbf{b}_i = \sum_{j=1}^{n} b_{ij} \mathbf{f}_j$ – разложения по базисным элементам. Заметим, что величина (3.22) не меняется при преобразованиях а), б), в). Таким образом эта величина определена корректно для любого бивектора. Но левая часть в (3.21) имеет $1 \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$ в качестве такой величины, а правая имеет значение $\sum r_{ij} \Delta_{ij} = 0$, так как в каждом из определителей Δ_{ij} одна из строк нулевая. Противоречие показывает, что равенства вида (3.21) быть не может. Следовательно, система $\{\mathbf{f}_i \wedge \mathbf{f}_j\}$ $(1 \leq i < j \leq n)$ линейно независима и образует базис пространства бивекторов. □

Следствие. *В пространстве $\mathcal{V}(\mathbb{E}^3) \wedge \mathcal{V}(\mathbb{E}^3)$ бивектора $\mathbf{j} \wedge \mathbf{k}$, $\mathbf{k} \wedge \mathbf{i}$, $\mathbf{i} \wedge \mathbf{j}$ образуют базис. Если $\mathbf{a} = X_1 \mathbf{i} + Y_1 \mathbf{j} + Z_1 \mathbf{k}$ и $\mathbf{b} = X_2 \mathbf{i} + Y_2 \mathbf{j} + Z_2 \mathbf{k}$, то*

$$\mathbf{a} \wedge \mathbf{b} = \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix} \mathbf{j} \wedge \mathbf{k} - \begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix} \mathbf{k} \wedge \mathbf{i} + \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix} \mathbf{i} \wedge \mathbf{j}.$$

3.5.2 Определение и свойства векторного произведения

В трехмерном пространстве $\mathcal{V}(\mathbb{E}^3)$ имеется счастливая возможность установить геометрически прозрачный изоморфизм между пространством бивекторов и пространством векторов, т. е. биекцию, сохраняющую операции сложения и умножения на скаляры. Заметим сразу, что такой возможности, скажем, в четырехмерном пространстве нет. Определим сначала понятие правой и левой тройки векторов. Неформально, тройка $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ называется правой, если эти вектора некомпланарны и глядя из конца вектора $\mathbf{c}$ вращение от $\mathbf{a}$ к $\mathbf{b}$ кажется проходящим против часовой стрелки. Это эквивалентно *правилу буравчика*: если вращать буравчик (или болт с обычной, правой, резьбой) от вектора $\mathbf{a}$ к вектору $\mathbf{b}$, то направление движения буравчика покажет на направление третьего вектора $\mathbf{c}$. Приведем еще одно эквивалентное определение: тройка векторов $\mathbf{a}, \mathbf{b}, \mathbf{c}$ правая, если эти вектора некомпланарны и могут быть непрерывно деформированы в стандарный базис $\mathbf{i}, \mathbf{j}, \mathbf{k}$ так, что в каждый момент времени сохраняется свойство некомпланарности. Строгое определение следующее:

Тройку векторов $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$, $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$ и $\mathbf{c} = X_3\mathbf{i} + Y_3\mathbf{j} + Z_3\mathbf{k}$ назовем *правой*, если

$$\begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix} > 0.$$

Если этот определитель меньше нуля, то тройку векторов $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ назовем *левой*. Заметим, что в случае равенства нулю этого определителя вектора $\mathbf{a}, \mathbf{b}, \mathbf{c}$ компланарны и такая тройка ориентации в пространстве $\mathcal{V}(\mathbb{E}^3)$ не имеет.

Определим теперь *векторное произведение вектора* $\mathbf{a}$ *на вектор* $\mathbf{b}$ как вектор $\mathbf{c}$, удовлетворяющий следующим свойствам:

- $\mathbf{c} \perp \mathbf{a}$ и $\mathbf{c} \perp \mathbf{b}$;
- $|\mathbf{c}| = |\mathbf{a}||\mathbf{b}| \sin(\widehat{\mathbf{a}, \mathbf{b}})$;
- либо $\mathbf{a} \parallel \mathbf{b}$ и тогда $\mathbf{c} = \mathbf{0}$, либо тройка векторов $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ правая

Векторное произведение обозначаем $\mathbf{a} \times \mathbf{b}$. Заметим, что

$$|\mathbf{a} \times \mathbf{b}| = S_{\ \mathbf{a},\mathbf{b}}$$

– площадь параллелограмма, построенного на векторах $\mathbf{a}$ и $\mathbf{b}$. На рис. 2 $\mathbf{M} = \mathbf{F} \times \mathbf{a}$ – момент силы $\mathbf{F}$ относительно точки O.

Теорема 2 (вычисление векторного произведения в координатах). *Если* $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$ *и* $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$, *то*

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \end{vmatrix} = \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix} \mathbf{i} - \begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix} \mathbf{j} + \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix} \mathbf{k} \tag{3.23}$$

Доказательство. Обозначим вектор, определяемый правой частью равенства (3.23) через $\mathbf{c}$. Применяя критерий ортогональности, проверим, что $\mathbf{c} \perp \mathbf{a}$:

$$\mathbf{a} \cdot \mathbf{c} = X_1 \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix} - Y_1 \begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix} + Z_1 \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix} = 0$$

Аналогично доказывается, что $\mathbf{c} \perp \mathbf{b}$. Далее

$$|\mathbf{c}|^2 = \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix}^2 + \begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix}^2 + \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix}^2 =$$
$$= (X_1^2 + Y_1^2 + Z_1^2)(X_2^2 + Y_2^2 + Z_2^2) - (X_1X_2 + Y_1Y_2 + Z_1Z_2)^2 =$$
$$= |\mathbf{a}|^2|\mathbf{b}|^2 - (\mathbf{a}\cdot\mathbf{b})^2 = |\mathbf{a}|^2|\mathbf{b}|^2(1 - \cos^2(\widehat{\mathbf{a},\mathbf{b}})) = |\mathbf{a}|^2|\mathbf{b}|^2\sin^2(\widehat{\mathbf{a},\mathbf{b}})$$

Отсюда вытекает равенство $|\mathbf{c}| = |\mathbf{a}||\mathbf{b}|\sin(\widehat{\mathbf{a},\mathbf{b}})$.

Проверим третье условие. Предположим, что вектора $\mathbf{a}$ и $\mathbf{b}$ неколлинеарны. Докажем, что тройка $\mathbf{a}, \mathbf{b}, \mathbf{c}$ – правая.

$$\begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix} & -\begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix} & \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix} \end{vmatrix} = \begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix}^2 + (-1)^2\begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix}^2 + \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix}^2 > 0$$

Здесь определитель 3×3 мы разложили по третьей строке. □

Следствие. *Площадь параллелограмма, построенного на векторах* $\mathbf{a}$ *и* $\mathbf{b}$ *равна*

$$S_{\mathbf{a},\mathbf{b}} = \sqrt{\begin{vmatrix} Y_1 & Z_1 \\ Y_2 & Z_2 \end{vmatrix}^2 + \begin{vmatrix} X_1 & Z_1 \\ X_2 & Z_2 \end{vmatrix}^2 + \begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix}^2}.$$

В частности, если $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j}$ *и* $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j}$ *- вектора на плоскости, то площадь параллелограмма. построенного на векторах* $\mathbf{a}$ *и* $\mathbf{b}$ *вычисляется по следующей формуле*

$$S_{\ \mathbf{a},\mathbf{b}} = \mathrm{mod}\begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix}.$$

Из доказанной выше теоремы и из свойств определителей легко следуют

Свойства векторного произведения

ВП1. *Билинейность:* $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c}$ и $\lambda(\mathbf{a} \times \mathbf{b}) = (\lambda\mathbf{a}) \times \mathbf{b} = \mathbf{a} \times (\lambda\mathbf{b})$.

ВП2. *Кососимметричность:* $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$ *для всех векторов* $\mathbf{a}$ *и* $\mathbf{b}$.

ВП3. $\mathbf{i} \times \mathbf{j} = \mathbf{k}$; $\mathbf{j} \times \mathbf{k} = \mathbf{i}$; $\mathbf{k} \times \mathbf{i} = \mathbf{j}$.

Теперь, взяв бивектор $\mathbf{g} = \sum_{i=1}^{i=n} r_i\mathbf{a}_i \wedge \mathbf{b}_i \in \mathcal{V}(\mathbb{E}^3) \wedge \mathcal{V}(\mathbb{E}^3)$, сопоставим ему вектор $\mathbf{g}^\times = \sum_{i=1}^{i=n} r_i\mathbf{a}_i \times \mathbf{b}_i$. Проверим корректность этого отображения. Пусть бивектор $\mathbf{g}$ получается из бивектора $\mathbf{f}$ применением правил билинейности и кососимметричности. Тогда вектор $\mathbf{f}^\times$ получается из вектора $\mathbf{g}^\times$ применением тех же самых правил и в той же последовательности, а поэтому $\mathbf{f}^\times = \mathbf{g}^\times$. Ясно, что отображение $\mathbf{g} \to \mathbf{g}^\times$ согласовано с операциями сложения и умножения на скаляры. Под этим понимается выполнение следующих равенств:

$$(\mathbf{g}+\mathbf{f})^\times = \mathbf{g}^\times + \mathbf{f}^\times; \qquad (\lambda\mathbf{g})^\times = \lambda\mathbf{g}^\times.$$

Соответствие $\mathbf{g} \to \mathbf{g}^\times$ очевидно будет отображением "на". Докажем его взаимную однозначность. Предположим, что $\mathbf{g}^\times = \mathbf{f}^\times$. Отсюда следует, что $(\mathbf{g}-\mathbf{f})^\times = \mathbf{g}^\times - \mathbf{f}^\times = \mathbf{0}$. Пусть $\mathbf{g}-\mathbf{f} = x\mathbf{j}\wedge\mathbf{k} + y\mathbf{k}\wedge\mathbf{i} + z\mathbf{i}\wedge\mathbf{j}$ (см. следствие теоремы 1). Тогда

$$\mathbf{0} = (\mathbf{g}-\mathbf{f})^\times = x(\mathbf{j}\wedge\mathbf{k})^\times + y(\mathbf{k}\wedge\mathbf{i})^\times + z(\mathbf{i}\wedge\mathbf{j})^\times = x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$$

Значит $x = y = z = 0$ и $\mathbf{g}-\mathbf{f} = \mathbf{0}$, т.е $\mathbf{g} = \mathbf{f}$.

Вывод: *отображение* $\mathbf{g} \to \mathbf{g}^\times$ *– биекция пространства* $\mathcal{V}(\mathbb{E}^3)\wedge\mathcal{V}(\mathbb{E}^3)$ *на пространство векторов* $\mathcal{V}(\mathbb{E}^3)$*, сохраняющая операции сложения и умножения на скаляры (т. е. изоморфизм в смысле определения 1 §3.7).*

3.6 Смешанное произведение

3.6.1 Тривекторы.

Понятие тривектора вводится по аналогии с понятием бивектора – это свободно плавающее в пространстве тело с некоторым фиксированным объёмом и выбранной в пространстве ориентацией. Для равенства векторов требуется коллинеарность прямых, на которых они расположены, а для равенства бивекторов требуется коллинеарность плоскостей их содержащих. Для пространства геометрических векторов подобное требование (быть расположенными в коллинеарных трехмерных подпространствах) выполнено автоматически, ибо пространство, содержащее три некомпланарных геометрических вектора только одно – $\mathcal{V}(\mathbb{E}^3)$. Итак, *тривектор над линейным пространством* L – это выражение вида:

$$\alpha = r_1\mathbf{a}_1\wedge\mathbf{b}_1\wedge\mathbf{c}_1 + r_2\mathbf{a}_2\wedge\mathbf{b}_2\wedge\mathbf{c}_2 + \ldots + r_n\mathbf{a}_n\wedge\mathbf{b}_n\wedge\mathbf{c}_n \quad (r_i \in K; \mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i \in L)$$

Считаем, что тривектор α *равен тривектору* $\alpha' = \sum r_i'\mathbf{a}_i'\wedge\mathbf{b}_i'\wedge\mathbf{c}_i'$ тогда и только тогда, когда α' может быть получен из α применением правил а), б), в) предыдущего параграфа, т. е. перестановкой слагаемых, линейностью по каждому аргументу в произведении $r\mathbf{a}\wedge\mathbf{b}\wedge\mathbf{c}$ (полилинейность) и кососимметричностью, которая для случая тривекторов может быть записана следующим образом:

$$\mathbf{a}\wedge\mathbf{b}\wedge\mathbf{c} = -\mathbf{b}\wedge\mathbf{a}\wedge\mathbf{c} = -\mathbf{a}\wedge\mathbf{c}\wedge\mathbf{b} = -\mathbf{c}\wedge\mathbf{b}\wedge\mathbf{a}.$$

Так же как и для бивекторов вводятся операции сложения тривекторов и умножения тривектора на элемент поля K. А именно, суммой тривектора α и тривектора $\beta = \sum s_i\mathbf{p}_i\wedge\mathbf{q}_i\wedge\mathbf{r}_i$ назовем тривектор

$$\alpha + \beta = \sum r_i\mathbf{a}_i\wedge\mathbf{b}_i\wedge\mathbf{c}_i + \sum s_i\mathbf{p}_i\wedge\mathbf{q}_i\wedge\mathbf{r}_i,$$

а произведением тривектора α на число λ назовем тривектор

$$\lambda\alpha = (\lambda r_1)\mathbf{a}_1 \wedge \mathbf{b}_1 \wedge \mathbf{c}_1 + (\lambda r_2)\mathbf{a}_2 \wedge \mathbf{b}_2 \wedge \mathbf{c}_2 + \ldots + (\lambda r_n)\mathbf{a}_n \wedge \mathbf{b}_n \wedge \mathbf{c}_n.$$

Множество тривекторов образует линейное пространство $L \wedge L \wedge L$ (или $\wedge^3 L$).

Теорема 1. *Если $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис пространства L, то система $\{\mathbf{f}_i \wedge \mathbf{f}_j \wedge \mathbf{f}_k\}$, где $1 \leq i < j < k \leq n$, состоящая из $C_n^3 = \frac{n(n-1)(n-2)}{3}$ элементов, образует базис пространства $\wedge^3 L$.*

Доказательство этой теоремы в точности такое же, как у теоремы 1, §3.5.1

Следствие. *Пространство $\wedge^3\mathcal{V}(\mathbb{E}^3)$ одномерно и порождено тривектором $\mathbf{i} \wedge \mathbf{j} \wedge \mathbf{k}$. Если $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$, $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$ и $\mathbf{c} = X_3\mathbf{i} + Y_3\mathbf{j} + Z_3\mathbf{k}$, то*

$$\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix} (\mathbf{i} \wedge \mathbf{j} \wedge \mathbf{k})$$

Доказательство. Применяем билинейность и кососимметричность к внешнему произведению

$$(X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}) \wedge (X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}) \wedge (X_3\mathbf{i} + Y_3\mathbf{j} + Z_3\mathbf{k})$$

и сразу получаем результат. □

Задача 1. Доказать, что, если тройки геометрических векторов $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, $(\mathbf{a}', \mathbf{b}', \mathbf{c}')$ с одинаковой ориентацией (т. е. либо обе правые, либо обе левые) таковы, что объемы параллепипедов, построенных на этих векторах совпадают, то $\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \mathbf{a}' \wedge \mathbf{b}' \wedge \mathbf{c}'$. Для этого сначала доказать, что при сделанных предположениях найдется 3×3-матрица C с единичным определителем такая, что $(\mathbf{a}, \mathbf{b}, \mathbf{c}) = (\mathbf{a}', \mathbf{b}', \mathbf{c}')C$.

Тривектор $\alpha = \mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c}$ можно рассматривать как внешнее произведение вектора $\mathbf{a}$ на бивектор $\mathbf{b} \wedge \mathbf{c}$. Этой операции можно придать прозрачный гидромеханический смысл, если интерпретировать вектор $\mathbf{a}$ как скорость жидкости, считая ее одинаковой в различных точках, а $\mathbf{b} \wedge \mathbf{c}$ как ориентированную площадку в пространстве. Тогда тривектор α имеет смысл объема жидкости, протекающей через заданную площадку в единицу времени. При этом этот объем берется со знаком "$+$", если тройка $\mathbf{a}, \mathbf{b}, \mathbf{c}$ правая, и берется со знаком "$-$", если эта тройка левая. Чтобы обосновать всё это, потребуется понятие смешанного произведения.

3.6.2 Определение смешанного произведения и его свойства.

Смешанным произведением векторов $\mathbf{a}, \mathbf{b}, \mathbf{c}$ называется число $\mathbf{a} \cdot (\mathbf{b} \times \mathbf{c})$. Смешанное произведение обозначается как $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Теорема 2 (вычисление смешанного произведения в координатах) *Если $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$, $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$ и $\mathbf{c} = X_3\mathbf{i} + Y_3\mathbf{j} + Z_3\mathbf{k}$, то*

$$(\mathbf{a},\mathbf{b},\mathbf{c}) = \begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix}$$

Доказательство. Применяя формулу вычисления скалярного произведения к векторам $X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$ и $\begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix}$, получаем результат. □

Определение правой и левой тройки векторов можно переформулировать так: $\mathbf{a},\mathbf{b},\mathbf{c}$ будет правой тройкой, если $(\mathbf{a},\mathbf{b},\mathbf{c}) > 0$; если же $(\mathbf{a},\mathbf{b},\mathbf{c}) < 0$, тройка векторов $\mathbf{a},\mathbf{b},\mathbf{c}$ будет левой.

Свойства смешанного произведения

ВП1. *Полилинейность, т. е. линейность по каждому аргументу*

ВП2. *Кососимметричность: – при перестановке любых двух векторов смешанное произведение меняет знак.*

ВП3. $(\mathbf{i},\mathbf{j},\mathbf{k}) = 1$.

Из этих свойств вытекает, что отображение

$$\mathbf{a}\wedge\mathbf{b}\wedge\mathbf{c} \to (\mathbf{a},\mathbf{b},\mathbf{c}) \tag{3.24}$$

корректно задано и согласовано с операциями сложения и умножения на скаляры. В частности, тривектор $\mathbf{i}\wedge\mathbf{j}\wedge\mathbf{k}$ переходит в 1, и поэтому $\mathbf{i}\wedge\mathbf{j}\wedge\mathbf{k} \neq 0$. Следовательно, отображение (3.24) задает изоморфизм между пространством $\wedge^3\mathcal{V}(\mathbb{E}^3)$ и пространством действительных чисел.

Теорема 3 (геометрический смысл смешанного произведения и определителя третьего порядка). *Смешанное произведение* $(\mathbf{a},\mathbf{b},\mathbf{c})$ *равно объему параллепипеда, построенного на векторах* $\mathbf{a},\mathbf{b},\mathbf{c}$*, если*
тройка $\mathbf{a},\mathbf{b},\mathbf{c}$ *правая, и равно этому объему со знаком "$-$", если тройка* $\mathbf{a},\mathbf{b},\mathbf{c}$ *левая.*

Доказательство. Рассмотрим случай, когда данная тройка векторов правая. Обозначаем угол между векторами $\mathbf{a}$ и $\mathbf{b}\times\mathbf{c}$ через φ (см. рис. 1).

Рис. 1. Объем параллепипеда.

Тогда

$$V = H \cdot S_{\mathbf{b},\mathbf{c}} = |\mathbf{a}| \cos\varphi |\mathbf{b} \times \mathbf{c}| = \mathbf{a} \cdot (\mathbf{b} \times \mathbf{c}),$$

что и требовалось доказать. □

Напомним, что семейство векторов компланарно, если все вектора этого семейства коллинеарны одной и той же плоскости.

Теорема 4 (критерий компланарности). *Следующие условия относительно векторов* $\mathbf{a} = X_1\mathbf{i} + Y_1\mathbf{j} + Z_1\mathbf{k}$, $\mathbf{b} = X_2\mathbf{i} + Y_2\mathbf{j} + Z_2\mathbf{k}$ *и* $\mathbf{c} = X_3\mathbf{i} + Y_3\mathbf{j} + Z_3\mathbf{k}$ *эквивалентны:*

1. *тройка векторов* $\mathbf{a}, \mathbf{b}, \mathbf{c}$ *компланарна;*

2. $(\mathbf{a}, \mathbf{b}, \mathbf{c}) = 0$*;*

3. $$\begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix} = 0;$$

4. *существует нетривиальная линейная зависимость, т. е. существуют числа* λ, μ, ν*, не все равные нулю, что* $\lambda\mathbf{a} + \mu\mathbf{b} + \nu\mathbf{c} = \mathbf{0}$*;*

5. *один из векторов выражается через другие в виде линейной комбинации.*

6. $\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \mathbf{0}$

Доказательство. $1 \Rightarrow 2$. Можно считать, что вектора $\mathbf{b}$ и $\mathbf{c}$ неколлинеарны. Вектор $\mathbf{b} \times \mathbf{c}$ ортогонален плоскости, содержащей эти вектора, тем самым он ортогонален $\mathbf{a}$. Отсюда $(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \mathbf{a}(\mathbf{b} \times \mathbf{c}) = 0$.

$2 \Rightarrow 3$ верно в силу теоремы о вычислении смешанного произведения в координатах.

$3 \Rightarrow 4$. В силу следствия правила Крамара существуют α, β, γ не все равные 0 такие, что

$$\begin{pmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Отсюда следует, что $\alpha\mathbf{a} + \beta\mathbf{b} + \gamma\mathbf{c} = \mathbf{0}$ – нетривиальная линейная зависимость.

$4 \Rightarrow 5$ Если $\alpha\mathbf{a} + \beta\mathbf{b} + \gamma\mathbf{c} = \mathbf{0}$ нетривиальная линейная зависимость и, скажем, $\alpha \neq 0$, то $\alpha = -\frac{\beta}{\alpha}\mathbf{b} - \frac{\gamma}{\alpha}\mathbf{c}$.

$5 \Rightarrow 1$. Если, например, $\alpha = -\frac{\beta}{\alpha}\mathbf{b} - \frac{\gamma}{\alpha}\mathbf{c}$, то все три вектора $\mathbf{a}, \mathbf{b}, \mathbf{c}$ коллинеарны плоскости, содержащей вектора $\mathbf{b}$ и $\mathbf{c}$.

$2 \Leftrightarrow 6$ в силу изоморфизма (3.24). $\square$

3.7 Линейные операторы

В этом параграфе будет развито достаточно широкое обобщение идеи линейных функций одной и нескольких переменных: $y = kx$, $y = A_1x_1 + A_2x_2 + \ldots + A_nx_n$.

Определение 1. Пусть L и M - линейные пространства над полем K. Отображение $\psi : L \to M$ называется *линейным*, если

$$\psi(\mathbf{a}+\mathbf{b}) = \psi(\mathbf{a}) + \psi(\mathbf{b}); \quad \psi(\lambda\mathbf{a}) = \lambda\psi(\mathbf{a})$$

для любых элементов $\mathbf{a}, \mathbf{b} \in L$ и для любого $\lambda \in K$. Если, к тому же, ψ - биекция, то ψ называется *изоморфизмом.* В случае $L = M$, линейное отображение называем также *линейным оператором.*

Примеры линейных отображений и операторов

1. *Нулевое* отображение: $\psi(\mathbf{a}) = \mathbf{0}$ для любого $\mathbf{a} \in L$.

2. *Единичный оператор* $Id_L : L \to L$ (или просто Id): $Id(\mathbf{a}) \equiv \mathbf{a}$.

3. *Гомотетия* в k раз – линейный оператор h_k на пространстве L такой, что $h_k(\mathbf{a}) = k\mathbf{a}$ для любого $\mathbf{a} \in L$

4. Поворот плоскости на угол α относительно начала координат. Обозначим этот оператор через r_α. Линейным будет также поворот трехмерного пространства на угол α относительно оси, проходящей через начало координат.

5. Симметрия плоскости относительно начала координат ($\equiv$ гомотетия с коэффициентом -1). Симметрия плоскости относительно прямой ℓ, проходящей через начало координат (обозначаем s_ℓ). Симметрия пространства относительно прямой или плоскости, проходящих через начало координат.

6. Проекция пространства геометрических векторов на прямую или плоскоскость.

7. Дифференцирование (L - пространство бесконечно дифференцируемых функций, либо пространство многочленов).

8. Интегрирование ($f(x) \to \int_a^b f(x)\,dx$) - линейное отображение пространства интегрируемых на отрезке $[a, b]$ функций в $\mathbb{R}$.

9. Этот пример в некотором смысле общий для всех конечномерных линейных пространств. Пусть A – матрица $m \times n$. Она задает линейное отображение ${}^nK \to {}^mK$ по следующему правилу:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in {}^nK \to A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in {}^mK \tag{3.25}$$

Задача 1. Доказать, что любое линейное отображение ${}^nK \to {}^mK$ выглядит как и в (3.25)

Для линейного отображения ψ определим *образ* $\psi(L)$ как совокупность всех элементов $\psi(\mathbf{a})$, когда $\mathbf{a}$ пробегает L. Определим также *ядро* $\operatorname{Ker}\psi$ *линейного отображения* ψ как множество всех элементов $\mathbf{a} \in L$ таких, что $\psi(\mathbf{a}) = \mathbf{0}$.

Предложение 1. *Образ линейного отображения $\psi : L \to M$ – подпространство пространства M. Ядро – подпространство пространства L. Линейное отображение ψ будет изоморфизмом тогда и только тогда, когда ядро нулевое, а образ совпадает со всем пространством M.*

Доказательство. Первые два утверждения следуют сразу из линейности отображения ψ. В третьем утверждении часть "только тогда" – непосредственное следствие определения биекции.

Пусть $\operatorname{Ker}\psi = 0$ и $\psi(L) = M$. Тогда ψ – отображение "на". Докажем его взаимную однозначность. Предположим, что $\psi(\mathbf{a}_1) = \psi(\mathbf{a}_2)$. Тогда $\psi(\mathbf{a}_1 - \mathbf{a}_2) = \mathbf{0}$ и, следовательно, $\mathbf{a}_1 - \mathbf{a}_2 \in \operatorname{Ker}\psi = 0$. Отсюда получаем равенство $\mathbf{a}_1 = \mathbf{a}_2$, что и требовалось доказать. □

Линейное пространство L *изоморфно* линейному пространству M над тем же полем, если существует изоморфизм $\varphi : L \to M$. Изоморфизм – отношение эквивалентности (см. задачу 1, §1.4.3), обозначаемое как $L \cong M$. Оказывается, с точки зрения линейных пространств все n-мерные пространства над фиксированным полем устроены одинаково. Точный смысл этой фразы следующий:

Теорема 1. *Любое пространство размерности n изоморфно пространству строк K^n*

Доказательство. Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис пространства L. Тогда соответствие

$$(x_1, x_2, \ldots, x_n) \to x_1\mathbf{f}_1 + x_2\mathbf{f}_2 + \ldots + x_n\mathbf{f}_n$$

задает изоморфизм K^n на L. □

Следствие. *Все n-мерные пространства над полем K изоморфны между собой (n фиксировано !).*

Задача 2. Построить изоморфизм следующих пространств над полем действительных чисел:

$$\mathcal{P}_6; \quad \mathcal{M}at_{\,2\times 3}(\mathbb{R}); \quad \mathcal{M}at_{\,3\times 2}(\mathbb{R}); \quad \mathbb{R}^6; \quad {}^6\mathbb{R}$$

Определим линейные операторы проекции и симметрии в общем случае. Пусть $L = H + T$ – *прямая сумма двух подпространств*, т. е. $H \cap T = 0$. Тогда *проекцией пространства L на H вдоль T* назовем оператор $\mathrm{pr}_H^T : L \to L$, который сопоставляет каждому элементу $h + t$ $(h \in H, t \in T)$ первое слагаемое, т. е. $\mathrm{pr}_H^T(h + t) = h$.

Симметрией пространства L относительно H вдоль T назовем оператор sym_H^T : $L \to L$, который сопоставляет каждой сумме $h + t$ $(h \in H, t \in T)$ разность, т. е. $\mathrm{sym}_H^T(h + t) = h - t$.

Если L – евклидово пространство, то очень часто в качестве T берут ортогональное дополнение $H^\perp$ и тогда говорят об *ортогональной проекции на H* ($\mathrm{pr}_H(\mathbf{a}) = \mathbf{a}_H$, см. теорема 3, §3.4.3) и *ортогональной симметрии относительно H*: $\mathrm{sym}_H(\mathbf{a}) = 2\mathbf{a}_H - \mathbf{a}$.

Пусть $\mathcal{F} = (\mathbf{f}_1, \dots, \mathbf{f}_n)$ – базис пространства L. Рассмотрим какой-либо линейный оператор $\psi : L \to L$. Разложим элементы $\psi(\mathbf{f}_i)$ по базису $\mathcal{F}$:

$$\begin{cases} \psi(\mathbf{f}_1) & = a_{11}\mathbf{f}_1 + a_{21}\mathbf{f}_2 + \dots a_{n1}\mathbf{f}_n \\ \psi(\mathbf{f}_2) & = a_{12}\mathbf{f}_1 + a_{22}\mathbf{f}_2 + \dots a_{n2}\mathbf{f}_n \\ \dots & \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \psi(\mathbf{f}_n) & = a_{1n}\mathbf{f}_1 + a_{2n}\mathbf{f}_2 + \dots a_{nn}\mathbf{f}_n \end{cases} \tag{3.26}$$

Тогда $n \times n$-матрица $A = (a_{ij})$ называется *матрицей линейного оператора ψ относительно базиса $\mathcal{F}$*. Заметим, что i-ая строка коэффициентов в разложении (3.26) ставится на место i-го столбца матрицы A.

Предложение 2. *Пусть $\mathbf{b} = b_1\mathbf{f}_1 + b_2\mathbf{f}_2 + \dots + b_n\mathbf{f}_n \in L$. Тогда столбец координат вектора $\psi(\mathbf{b})$ равен*

$$A \begin{pmatrix} b_1 \\ \cdot \\ \cdot \\ b_n \end{pmatrix}.$$

Доказательство.

$$\psi(\mathbf{b}) = \sum_{i=1}^n b_i \psi(\mathbf{f}_i) = \sum_{i=1}^n b_i \sum_{j=1}^n a_{ji}\mathbf{f}_j = \sum_{j=1}^n (\sum_{i=1}^n a_{ji} b_i)\mathbf{f}_j$$

□

Обозначим множество всех линейных операторов пространства L через $\mathrm{End}\,L$. Это множество образует кольцо относительно операций сложения операторов $(\varphi+\psi)(\mathbf{a}) = \varphi(\mathbf{a})+\psi(\mathbf{a})$ и композиции в качестве умножения. Фиксируя базис $\mathcal{F}$ на линейном пространстве L можно сопоставить каждому оператору $\varphi \in \mathrm{End}\,L$ матрицу A_φ размера

$n \times n$ этого оператора в выбранном базисе $\mathcal{F}$. Легко проверить, что такого рода сопоставление обладает следующими свойствами

$$A_{\varphi+\psi} = A_\varphi + A_\psi; \quad A_{\varphi\circ\psi} = A_\varphi \cdot A_\psi$$

Второе равенство следует из предложения 2. Более того, отображение $\varphi \to A_\varphi$ – биекция, а значит, является изоморфизмом колец $\operatorname{End} L$ и $\mathcal{M}at_{\,n\times n}(K)$.

Примеры матриц геометрических линейных преобразований плоскости

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

– матрицы поворота на угол α, гомотетии в λ раз, симметрии относительно оси OX и проекции на ось OX соответственно.

Пусть снова $L = H + T$ – прямая сумма подпространств H и T, и $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – базис пространства L такой, что

$$H = \mathbf{f}_1 K + \ldots + \mathbf{f}_m K; \qquad T = \mathbf{f}_{m+1} K + \ldots + \mathbf{f}_m K$$

Тогда матрица проекции pr_H^T и симметрии sym_H^T в базисе $\mathcal{F}$ будут диагональными:

$$\mathrm{diag}(1, \ldots, 1, 0, \ldots, 0), \qquad \mathrm{diag}(1, \ldots, 1, -1, \ldots, -1)$$

На диагонали в обоих случаях стоят m единиц.

Предложение 3. *Пусть A - матрица линейного оператора $\psi : L \to L$ относительно базиса $\mathcal{F}$. Предположим, что $\mathcal{F}'$ – новый базис пространства L с матрицей перехода C от старого базиса к новому. Тогда $A' = C^{-1}AC$ – матрица оператора ψ в новом базисе.*

Доказательство. Сохраняем обозначения такие же, как в формулах (3.7), (3.8), (3.9) в §3.3. Если

$$\mathbf{b} = b_1\mathbf{f}_1 + \ldots + b_n\mathbf{f}_n = b_1'\mathbf{f}_1' + \ldots + b_n'\mathbf{f}_n' \in L$$

– произвольный элемент, то $\psi(\mathbf{b})$ имеет столбец $A(b_1, b_2, \ldots, b_n)^\top$ в качестве старых координат и
$A'(b_1', b_2', \ldots, b_n')^\top$ в качестве новых координат (предложение 1). Тогда

$$C^{-1}A(b_1, b_2, \ldots, b_n)^\top = A'(b_1', b_2', \ldots, b_n')^\top \quad \text{и} \quad (b_1, b_2, \ldots, b_n)^\top = \\ = C(b_1', b_2', \ldots, b_n')^\top$$

согласно формулам (3.9) и (3.8). Подставляя $C(b_1', b_2', \ldots, b_n')^\top$ вместо $(b_1, b_2, \ldots, b_n)^\top$ в первое соотношение, получим равенство

$$C^{-1}AC(b_1', b_2', \ldots, b_n')^\top = A'(b_1', b_2', \ldots, b_n')^\top$$

верное для любых $b_1', \ldots, b_n' \in K$. Это влечет равенство матриц $C^{-1}AC = A'$. $\square$

В связи с предложением 2 возникает естественная задача: найти базис пространства L, в котором матрица заданного линейного оператора ψ имеет наиболее простой вид. Иными словами из *класса сопряженности* $\{C^{-1}AC \mid C \in \mathrm{GL}(n,K)\}$ данной матрицы A требуется выбрать представитель наиболее простого вида. Именно к такому классу задач относится следующая

Проблема диагонализации линейного оператора. Найти базис, в котором матрица данного линейного оператора диагональна.

Диагональные матрицы удобны для вычислений. Очень часто для матричной функции $F : \mathcal{M}at \to \mathcal{M}at$ оказывается, что

$$F(\mathrm{diag}(\lambda_1,\ldots,\lambda_n)) = \mathrm{diag}(F(\lambda_1),\ldots,F(\lambda_n))$$

Например определим *матричную экспоненту*
$\exp : \mathcal{M}at_{n\times n}(\mathbb{R}) \to \mathcal{M}at_{n\times n}(\mathbb{R})$ как сумму ряда

$$\exp(A) = E + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \frac{A^4}{4!} + \ldots \tag{3.27}$$

Используя *матричную норму*
$\|A\| = \max\left\{A(u_1,u_2,\ldots,u_n)^\top \mid u_1^2+u_2^2+\ldots+u_n^2 = 1\right\}$ и неравенство
$\|AB\| \le \|A\|\,\|B\|$ доказываем сначала мажорируемость ряда (3.27) сходящимся числовым рядом $\sum_{k=0}^{\infty}\frac{\|A\|^k}{k!}$. Отсюда следует сходимость ряда (3.27) и, более того, равномерная сходимость в любом круге $\|A\| \le R$.

Задача 3. Доказать равенства

$$\exp(\mathrm{diag}(\lambda_1,\lambda_2,\ldots,\lambda_n)) = \mathrm{diag}(\exp(\lambda_1),\ldots,\exp(\lambda_n))$$

$$\exp(\begin{pmatrix} 0 & \varphi \\ -\varphi & 0 \end{pmatrix}) = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

Задача 4. Доказать, что оператор поворота плоскости на угол $\varphi \ne 0,\pi$ не диагонализируем.

Проблема диагонализации решается в следующем параграфе.

3.8 Собственные числа и собственные векторы

3.8.1 Инвариантные подпространства

Определение 1. Пусть H подпространство линейного пространства L, и ψ – линейный оператор на L. Подпространство H называется *инвариантным относительно линейного оператора* ψ, если $\psi(\mathbf{a}) \in H$ для всякого элемента $\mathbf{a} \in H$.

Конечно, нулевое подпространство, а также все пространство будут инвариантны относительно любого оператора, остальные инвариантные подпространства называются *собственными*. Именно в случае инвариантного подпространства имеется возможность сузить действие оператора ψ на H, при этом получается уже оператор пространства H. Теперь можно сделать первый шаг на пути диагонализации линейного оператора.

Предложение 1. *Пусть $\mathcal{F}$ - базис линейного пространства L такой, что вектора $\mathbf{f}_1, \ldots, \mathbf{f}_k$ составляют базис подпространства H, инвариантного относительно опера-тора ψ. Тогда матрица оператора ψ в базисе $\mathcal{F}$ имеет "блочный" вид:*

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

где B – $k \times k$-матрица, а блок нулей имеет размер $(n-k) \times k$.

Доказательство. Так как $\psi(H) \subseteq H$, то $\psi(\mathbf{f}_i)$ для $i = 1, \ldots, k$ раскладывается лишь по элементам $(\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_k)$. Далее применяем определение матрицы линейного оператора. □

Ещё лучше, когда пространство L разложимо в прямую сумму инвариантных относительно операторы ψ подпространств H и T. В этом случае, взяв базис $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ так, что $H = \mathbf{f}_1 K + \ldots + \mathbf{f}_k K$ и $T = \mathbf{f}_{k+1} K + \ldots + \mathbf{f}_n K$ получим блочнодиагональную матрицу $\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$ оператора ψ в базисе $\mathcal{F}$. Это следствие предложения 1.

3.8.2 Собственные элементы.

Среди всех возможных собственных инвариантных подпространств фиксированного оператора ψ особенно интересны те, которые имеют наименьшую возможную размерность – единица. Это тот случай, когда ψ
$(\mathbf{a}K) \subseteq \mathbf{a}K$ для некоторого ненулевого элемента $\mathbf{a}$. На геометрическом уровне это значит, что вектор $\mathbf{a}$ лишь растягивается или сжимается во сколько-то раз, оставаясь лежать на той же самой прямой. Так мы приходим к следующему определению.

Определение 2. Пусть ψ - линейный оператор линейного пространства L. Ненулевой элемент $\mathbf{a} \in L$ называется *собственным элементом с собственным числом* λ, если $\psi(\mathbf{a}) = \lambda \mathbf{a}$.

Элемент $\mathbf{a} \in L$ является собственным вектором оператора ψ в том и только том случае, когда "прямая" $\mathbf{a}K = \{\lambda \mathbf{a} \,|\, \lambda \in K\}$ является инвариантным подпространством.

Задача 1. Основываясь только на определении, найти собственные вектора операторов поворота, проекции, отражения.

Задача 2. Пусть L – вещественное пространство бесконечно дифференцируемых функций и D – оператор дифференцирования. Какие из следующих функций будут собственными для оператора D: x^2, Const, e^{kx}, $\sin\omega x$, $\cos\omega x$? А для оператора D^2?

Задача 3.* Найти все собственные функции операторов D и D^2 в задаче 2.

Задача 4. Пусть $\psi^2 = \psi$ для некоторого оператора ψ линейного пространства L. Доказать, что а) все собственные числа оператора ψ либо 0, либо 1, б) L разложимо в прямую сумму подпространств $H = \operatorname{Ker}\psi$ и $T = \operatorname{Ker}(\operatorname{Id}-\psi)$, в) ψ есть проекция на H вдоль T.

Задача 5. Пусть $\psi^2 = \operatorname{Id}$ для некоторого оператора ψ линейного пространства L. Доказать, что а) все собственные числа оператора ψ либо -1, либо 1, б) L разложимо в прямую сумму подпространств $H = \operatorname{Ker}(\operatorname{Id}-\psi)$ и $T = \operatorname{Ker}(\operatorname{Id}+\psi)$, в) ψ есть симметрия относительно H вдоль T.

Теорема 1. *Пусть A – матрица линейного оператора ψ относительно базиса $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ и*

$$\mathbf{a} = a_1\mathbf{f}_1 + a_2\mathbf{f}_2 + \ldots + a_n\mathbf{f}_n \in L$$

– какой-либо элемент. Элемент **a** *будет собственным с собственным числом λ тогда и только тогда, когда λ является корнем* ХАРАКТЕРИСТИЧЕСКОГО УРАВНЕНИЯ*:*

$$\det(A - \lambda E) = 0, \tag{3.28}$$

а столбец $(a_1, a_2, \ldots, a_n)^\top$ - ненулевое решение следующей однородной системы линейных уравнений:

$$(A - \lambda E)X = 0 \tag{3.29}$$

Доказательство. Соотношение $\psi(\mathbf{a}) = \lambda\mathbf{a}$ на матричном языке означает, что $A(a_1, a_2, \ldots, a_n)^\top = \lambda(a_1, a_2, \ldots, a_n)^\top$. Перенося все в левую часть, получаем однородную систему (3.29). Эта однородная система имеет ненуле-

вое решение тогда и только тогда, когда $\det(A - \lambda E) = 0$ (см. теорема 2, §2.7). $\square$

Заметим, что левая часть равенства (3.28) представляет из себя многочлен степени n с коэффициентом $(-1)^n$ при старшей степени. Он называется *характеристическим многочленом* оператора ψ или матрицы A.

Задача 1. Доказать, что в характеристическом многочлене свободный член равен $\det A$, а коэффициент при λ^{n-1} равен $(-1)^{n-1}\operatorname{Tr} A$, где $\operatorname{Tr} A$ – *след матрицы* A, по определению равный сумме диагональных коэффициентов.

Докажем, что

Характеристический многочлен не зависит от выбора базиса.

Действительно, пусть $\mathcal{F}' = (\mathbf{f}'_1, \mathbf{f}'_2, \dots, \mathbf{f}'_n)$ – другой, новый базис пространства L, связанный со старым базисом матрицей перехода C. Тогда матрица оператора ψ в новом базисе равна $A' = C^{-1}AC$ (предложение 2, §3.7) и

$$\det(A' - \lambda E) = \det(c^{-1}AC - \lambda E) = \det(C^{-1}AC - \lambda C^{-1}C) =$$
$$= \det C^{-1}(A - \lambda E)C =$$
$$= \det C^{-1}\det(A - \lambda E)\det C = \det C^{-1}\det C\det(A - \lambda E) = \det(A - \lambda E),$$

что и требовалось доказать.

Лемма 1. *Собственные элементы, отвечающие различным собственным значениям, линейно независимы.*

Доказательство. Пусть $\mathbf{b}_1, \dots, \mathbf{b}_n$ – собственные вектора линейного оператора $\psi : L \to L$ с собственными числами $\lambda_1, \dots, \lambda_n$. Предположим, что $x_1\mathbf{b}_1 + \ldots + x_n\mathbf{b}_n = \mathbf{0}$ для некоторых $x_i \in K$. Подействуем на левую и правую часть этого соотношения $n-1$ раз оператором ψ. Учитывая, что $\psi^i(\mathbf{b}_j) = \lambda_j^i\mathbf{b}_j$, получим систему

$$\begin{cases} x_1\mathbf{b}_1 + \ldots + x_n\mathbf{b}_n = & \mathbf{0}, \\ \lambda_1 x_1\mathbf{b}_1 + \ldots + \lambda_n x_n\mathbf{b}_n = & \mathbf{0}, \\ \lambda_1^2 x_1\mathbf{b}_1 + \ldots + \lambda_n^2 x_n\mathbf{b}_n = & \mathbf{0}, \\ \dots\dots\dots\dots\dots\dots\dots\dots & \dots \\ \lambda_1^{n-1} x_1\mathbf{b}_1 + \ldots + \lambda_n^{n-1} x_n\mathbf{b}_n = & \mathbf{0}, \end{cases}$$

Перепишем эту систему в матричном виде

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_n^2 \\ \dots & \dots & \dots & \dots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \dots & \lambda_n^{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_1\mathbf{b}_1 \\ x_2\mathbf{b}_2 \\ \dots \\ x_n\mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{pmatrix} \tag{3.30}$$

Определитель Вандермонда, стоящий в левой части (3.30) не равен 0, так как λ_i-ые попарно различны (см. §2.6.2). Следовательно, эта матрица обратима. Умножение слева соотношения (3.30) на обратную к ней матрицу дает равенства $x_1\mathbf{b}_1 = x_2\mathbf{b}_2 = \ldots = x_n\mathbf{b}_n = \mathbf{0}$. Отсюда $x_1 = x_2 = \ldots = x_n = 0$, так как вектора $\mathbf{b}_i$ по определению ненулевые. Доказательство линейной независимости векторов $\mathbf{b}_i$ завершено. □

Теорема 2 (диагонализация линейного оператора в случае простого спектра). *Пусть ψ – линейный оператор n-мерного линейного пространства, и характеристическое уравнение оператора ψ имеет n различных корней. Тогда оператор ψ диагонализируем: существует базис из собственных векторов.*

Доказательство. Действительно, таковым базисом будут собственные вектора $\mathbf{f}_1, \dots, \mathbf{f}_n$ отвечающие n попарно различным собственным значениям $\lambda_1, \dots, \lambda_n$ – корням характеристического уравнения. Собственные вектора существуют по теореме 1, линейно независимы по лемме 1 и образуют базис по теореме о размерности, см. §3.3. Матрица оператора ψ в базисе $\{\mathbf{f}_i\}$ имеет вид $\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$. □

Задача 5. Рассмотрим оператор r поворота плоскости $\mathbf{e}_1\mathbb{R}+\mathbf{e}_2\mathbb{R}$ на 90^0. Доказать, что он не диагонализируем. Продолжим действие r на комплексное двумерное пространство $\mathbf{e}_1\mathbb{C}+\mathbf{e}_2\mathbb{C}$ с той же матрицей. Продолжение обозначим $r^{\mathbb{C}}$. Диагонализировать оператор $r^{\mathbb{C}}$.

Задача 6*. Из n^2-мерного куба $[-R, R]^{n^2}$ ($R > 0$ – фиксировано) наудачу выбирается n^2 чисел и строится матрица $A = (a_{ij}) \in \mathcal{M}at_{\,n\times n}(\mathbb{R})$. Доказать, что с вероятностью единица эта матрица имеет простой спектр над полем комплексных чисел, т. е. имеет n различных (комплексных корней).

Теорему 2 можно обобщить, предварительно заметив, что *множество всех собственных векторов, отвечающих фиксированному собственному числу λ, вместе с нулевым вектором образуют подпространство.* Действительно, это множество не что иное как ядро оператора $\psi - \lambda\,\mathrm{Id}$, а ядро является всегда подпространством (см. предложение 1, §3.7).

Теорема 3. *Пусть $\lambda_1, \ldots \lambda_k$ – все различные корни характеристического многочлена оператора ψ, действующего на линейном пространстве L размерности n. Обозначим $n_i = \dim \mathrm{Ker}(\psi - \lambda_i\,\mathrm{Id})$. Тогда оператор ψ диагонализируем тогда и только тогда, когда выполняется равенство $n_1 + n_2 + \ldots + n_k = n$.*

Доказательство. Во-первых отметим, что сумма $H = \sum_{i=1}^{k} \mathrm{Ker}(\psi - \lambda_i\,\mathrm{Id})$ прямая, т. е. любой элемент из H единственным образом разложим в сумму слагаемых из $\mathrm{Ker}(\psi - \lambda_i\,\mathrm{Id})$. Отсюда вытекает, что $\dim H = n_1 + n_2 + \ldots + n_k$. Если теперь предположить, что имеет место равенство $n_1 + n_2 + \ldots + n_k = n$, то $H = L$ из соображений размерности. Значит, у оператора ψ есть базис из собственных векторов; он может быть получен объединением базисов подпространств $\mathrm{Ker}(\psi - \lambda_i\,\mathrm{Id})$. В этом базисе матрица оператора ψ диагональна.

Наоборот, пусть ψ обладает базисом $\{\mathbf{f}_i\}$, в котором матрица ψ диагональна – $\mathrm{diag}(\mu_1, \mu_2, \ldots, \mu_n)$. Заметим, что тогда все $\mathbf{f}_i$-е будут собственными векторами. Перенумерацией базисных элементов можно добиться того, чтобы

$$\lambda_1 = \mu_1 = \ldots = \mu_s, \quad \lambda_2 = \mu_{s+1} = \ldots = \mu_t, \ldots, \lambda_k = \mu_q = \ldots = \mu_n.$$

Обозначим $H_1 = \mathbf{f}_1K + \ldots + \mathbf{f}_sK, \ldots, H_k = \mathbf{f}_qK + \ldots + \mathbf{f}_nK$. Так как заведомо $H_j \subseteq \mathrm{Ker}(\psi - \lambda_j\,\mathrm{Id})$, то сумма $H_1 + \ldots + H_k$ прямая. Но эта сумма равна L, ибо она содержит все базисные элементы. Тогда

$$n_1 + \ldots + n_k \geq \dim H_1 + \ldots + \dim H_k = \dim L = n$$

Неравенство $\sum_{i=1}^{k} n_i \leq n$ верно во всех случаях. Из этих двух оценок получаем равенство $\sum_{i=1}^{k} n_i = n$. □

Как же вычислить размерности пространства $\mathrm{Ker}(\psi - \lambda_i \,\mathrm{Id})$ и тем самым проверить равенство $\sum_{i=1}^{k} n_i = n$? Заметим, что подпространство $\mathrm{Ker}(\psi - \lambda_i \,\mathrm{Id})$ в координатах это не что иное как пространство решений однородной системы (3.29). Следовательно, все сводится к каким-то манипуляциям с матрицей A оператора ψ. Это и составит содержание следующего параграфа.

3.9 Ранг матрицы.

С высоты развитой теории о линейных пространствах и отображениях взглянем снова на систему линейных уравнений над полем K:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = b_2 \\ \ldots\ldots\ldots & \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = b_m \end{cases} \tag{3.31}$$

Левые части системы (3.31) можно интерпретировать как линейное отображение $\psi : {}^nK \to {}^mK$, задаваемое $m \times n$-матрицей $A = (a_{ij})$ (см. пример 9 из § 3.7). Совместность системы (3.31), таким образом, будет эквивалентна принадлежности столбца $(b_1, b_2, \ldots, b_m)^\top$ образу $\psi({}^nK)$. В частности, если размерность этого образа равна m, то $\psi({}^nK) = {}^mK$ и система (3.31) совместна, какова бы ни была ее правая часть. В противном случае, если $\dim \psi({}^nK) < m$, система (3.31) не является совместной в случае $(b_1, b_2, \ldots, b_m)^\top \notin \psi({}^nK)$. Из этого видно, что имеет смысл для системы (3.31) ввести характеристику – размерность образа отображения ψ. Эта размерность полностью определяется матрицей A; она равна размерности линейной оболочки столбцов матрицы A, что в свою очередь, совпадает с максимальным числом линейно независимых столбцов матрицы. Оказывается,

для матрицы имеет место совпадение следующих чисел

(а) *максимальное число линейно независимых столбцов,*

(б) *максимальное число линейно независимых строк,*

(в) *максимальный размер минора, не равного 0*

Достаточно доказать совпадение чисел, определенных в (б) и (в). Обозначим их r_1 и r_2 соответственно. При элементарных преобразованиях строк, числа r_1 и r_2 не меняются. Следовательно, можно считать, что матрица A приведена к ступенчатому виду с единицами в его углах:

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & \dots & a_{kn} \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{3.32}$$

Но теперь ясно, что числа r_1 и r_2 равны числу ненулевых строк матрицы A.

Определение 1. Число, определяемое одним из эквивалентных условий (а), (б), (в), называется *рангом матрицы* A и обозначается $\operatorname{rang} A$.

Теорема Кронекера-Капелли. *Система (3.31) совместна тогда и только тогда, когда ранг матрицы A совпадает с рангом расширенной матрицы.*

Доказательство. Пусть A_* – расширенная матрица.
Если $\operatorname{rang} A = \operatorname{rang} A_*$, то последний столбец матрицы A_*, т. е. $(b_1, b_2, \dots, b_m)^\top$ принадлежит линейной оболочке столбцов матрицы A. Следовательно, найдутся элементы x_1^0, x_2^0,…, x_n^0 поля K такие, что

$$\sum_{i=1}^{n} (a_{1i}, a_{2i}, \dots, a_{mi})^\top x_i^0 = (b_1, b_2, \dots, b_m)^\top \tag{3.33}$$

Но это и значит, что $(x_1^0, x_2^0, \dots, x_m^0)$ – решение системы (3.31). Наоборот, если $(x_1^0, x_2^0, \dots, x_m^0)$ – решение системы (3.31), то имеет место равенство (3.33); следовательно линейные оболочки столбцов матриц A и A_* совпадают, значит совпадают и их размерности, т. е. ранги. □

Задача 1 (метод окаймляющих миноров). Пусть M – ненулевой минор матрицы A размера $r \times r$ и любой окаймляющий минор равен 0. Тогда $r = \operatorname{rang} A$.

3.10 Самосопряженные операторы.

В этом параграфе L – вещественное линейное пространство со скалярным произведением.

Определение 1. Оператор $\psi : L \to L$ называется *самосопряженным*, если равенство

$$\mathbf{a} \cdot \psi(\mathbf{b}) = \psi(\mathbf{a}) \cdot \mathbf{b} \tag{3.34}$$

выполняется для любых $\mathbf{a}, \mathbf{b} \in L$.

Предложение 1. *Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_n)$ – ортонормированный базис пространства L. Оператор ψ самосопряжен тогда и только тогда, когда матрица A оператора ψ в базисе $\mathcal{F}$ симметрична: $A^\top = A$.*

Доказательство. В матричном виде равенство (3.34) выглядит так:

$$(a_1, a_2, \ldots, a_n)A \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = (b_1, b_2, \ldots, b_n)A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \tag{3.35}$$

Левая и правая часть в (3.35) – линейные функции аргументов $a_1, \ldots, a_n$, $b_1, \ldots, b_n$. Следовательно, (3.35) выполняется для любых строк $(a_1, a_2, \ldots, a_n)$и $(b_1, b_2, \ldots, b_n)$, если и только если оно верно для элементов e_i и e_j стандартного базиса строк. Подставляя в (3.35) e_i вместо $(a_1, a_2, \ldots, a_n)$ и e_j вместо $(b_1, b_2, \ldots, b_n)$, получим соотношение $a_{ij} = a_{ji}$. Это соотношение, верное для всех пар индексов (i, j), и характеризует симметричные матрицы. □

Предложение 2. *Пусть H – инвариантное подпространство самосопряженного оператора ψ. Тогда ортогональное дополнение $H^\perp$ также инвариантно.*

Доказательство. Пусть $\mathbf{a} \in H$, $\mathbf{b} \in H^\perp$ – произвольные элементы. Тогда

$$\psi(\mathbf{b})\mathbf{a} = \mathbf{b}\psi(\mathbf{a}) = 0,$$

так как $\psi(\mathbf{a}) \in H$ и $\mathbf{b} \perp H$. Отсюда следует, что $\psi(\mathbf{b}) \perp H$, т. е. $\psi(\mathbf{b}) \in H^\perp$ □

Следующее предложение понадобится при доказательстве теоремы о диагонализации самосопряженного оператора. Формально, оно является частным случаем этой теоремы.

Предложение 3. *Самосопряженный оператор на плоскости имеет ортонормированный базис из собственных векторов.*

Доказательство. Пусть $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ – матрица самосопряженного оператора на плоскости относительно стандартного базиса со стандартным скалярным произведением. Эта матрица симметрична в силу предложения 1. Её характеристический многочлен равен $\lambda^2 - (a+c)\lambda + ac - b^2$. Дискриминант этого квадратного трехчлена неотрицателен:

$$D = (a+c)^2 - 4ac + b^2 = (a-c)^2 + b^2$$

Следовательно, существует корень λ_1 и соответствующий ему собственный вектор $\mathbf{f}_1$ единичной длины. Выберем единичный вектор $\mathbf{f}_2$, порождающий ортогональное дополнение $(\mathbf{f}_1\mathbb{R})^\perp$. Тогда $\mathbf{f}_2$ – собственный вектор в силу предложения 2. Тем самым $\mathbf{f}_1, \mathbf{f}_2$ – искомый ортонормированный базис. □

Из предложения 3 вытекает простое геометрическое и механическое описание произвольного самосопряженного оператора на плоскости: найдутся две взаимно перпендикулярные оси, по которым происходит растяжение в λ_1 и λ_2 раз. Оказывается, то же самое верно и для большей размерности.

Теорема 1. *Самосопряженный оператор евклидова пространства диагонализируем. Более того, существует ортонормированный базис, состоящий из собственных векторов.*

Доказательство. Пусть ψ – самосопряженный оператор евклидова пространства L с ортонормированным базисом $(\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$. Доказательство будем вести индукцией по размерности пространства L. Случай $\dim L = 1$ тривиален. Предположим теорема верна для размерностей пространства меньше, чем n, и сейчас $\dim L = n$. Пусть $z \in \mathbb{C}$ – какой-либо корень характеристического уравнения $f(\lambda) = 0$. Он существует по основной теореме алгебры теории комплексных чисел (см. § 1.7.3). Докажем в начале, что $z \in \mathbb{R}$. Предположим противное; тогда сопряженное комплексное число $\overline{z}$ также будет корнем характеристического уравнения, так как

$$\sum a_i z^i = 0 \Rightarrow \sum \overline{a_i z^i} = 0 \Rightarrow \sum a_i \overline{z}^i = 0$$

(здесь $a_i \in \mathbb{R}$). Допуская в качестве коэффициентов любые комплексные числа, найдем собственные вектора $\mathbf{b} = b_1\mathbf{f}_1 + \ldots + b_n\mathbf{f}_n \in \sum \mathbf{f}_i\mathbb{C}$ и $\overline{\mathbf{b}} = \overline{b_1}\mathbf{f}_1 + \ldots + \overline{b_n}\mathbf{f}_n$ отвечающие собственным числам z и $\overline{z}$. Заведомо $\mathbf{b} \notin L$, но $\mathbf{a} := \mathbf{b} + \overline{\mathbf{b}} \in L$ и $\mathbf{c} := \frac{1}{i}(\mathbf{b} - \overline{\mathbf{b}}) \in L$. Тогда двумерное подпространство $H = \mathbf{a}\mathbb{R} + \mathbf{c}\mathbb{R}$ инвариантно относительно ψ, ибо

$$\psi(H) \subseteq ((\mathbf{b}\mathbb{C} + \overline{\mathbf{b}}\mathbb{C}) \cap L) = H.$$

Отсюда получаем, что ограничение ψ на H, будучи самосопряженным оператором, не имеет на H собственного вектора, ибо его характеристический многочлен $(\lambda - z)(\lambda - \overline{z})$ не имеет действительных корней. Это противоречит утверждению предложения 3. Противоречие показывает, что характеристический многочлен оператора ψ имеет действительный корень λ_1. Рассмотрим $H = \operatorname{Ker}(\psi - \lambda_1\mathbb{R})$. Это подпространство инвариантно относительно ψ. Заведомо $H \neq 0$. Если $H = L$, то ψ – гомотетия с коэффициентом λ_1. В этом случае утверждение теоремы очевидным образом выполняется для любого ортонормированного базиса. В противном случае, $L = H + H^{\perp}$ – разложение в прямую сумму инвариантных собственных подпространств (учесть предложение 2), к каждому из которых можно применить индукционное предположение. Объединив ортонормированные базисы подпространств H и $H^{\perp}$, в итоге получаем ортонормированный базис всего пространства. □

Задача 1. Привести пример, показывающий, что произведение самосопряженных операторов не обязано быть самосопряженным оператором.

Задача 2. Пусть φ, ψ – самосопряженные коммутирующие операторы (т. е. $\varphi\psi = \psi\varphi$). Тогда существует ортонормированный базис из собственных векторов как оператора φ, так и оператора ψ. В частности, произведение $\varphi\psi$ будет также самосопряженным оператором. Обобщить это утверждение на любое семейство попарно коммутирующих самосопряженных операторов.

Задача 3*. Описать централизатор самосопряженного оператора ψ, т. е. множество всех операторов φ, коммутирующих с ψ.

3.11 Ортогональные операторы.

Линейный оператор φ пространства L со скалярным произведением называется *ортогональным*, если он сохраняет длины векторов, то есть $|\varphi(\mathbf{x})| = |\mathbf{x}|$ для любого $\mathbf{x} \in L$. Отсюда сразу следует, что *ортогональный оператор взаимно-однозначен, а если к тому же пространство L конечномерно, то ортогональный оператор – биекция.* Так как

$$2(\mathbf{x}, \mathbf{y}) = |\mathbf{x} + \mathbf{y}|^2 - |\mathbf{x}|^2 - |\mathbf{y}|^2 ,$$

то φ ортогонален тогда и только тогда, когда φ сохраняет скалярное произведение. Следовательно, ортогональный оператор сохраняет и углы, ибо

$$\cos(\widehat{\varphi(\mathbf{x}), \varphi(\mathbf{y})}) = \frac{\varphi(\mathbf{x})\varphi(\mathbf{y})}{|\varphi(\mathbf{x})|\,|\varphi(\mathbf{y})|} = \frac{\mathbf{x}\mathbf{y}}{|\mathbf{x}|\,|\mathbf{y}|} = \cos(\mathbf{x}, \mathbf{y})$$

для любых ненулевых $\mathbf{x}, \mathbf{y} \in L$.

Примеры. 1. Поворот плоскости на угол α – ортогональный оператор. Поворот пространства $\mathbb{R}^3$ относительно оси, проходящей через начало координат, также ортогональный оператор.

2. Отражение плоскости относительно прямой $ax + by = 0$ – ортогональный оператор. Симметрия $\mathbb{R}^3$ относительно прямой или плоскости, проходящей через начало координат, – ортогональный оператор.

Очевидно, что композиция ортогональных операторов – снова ортогональный оператор и обратный оператор к ортогональному будет также ортогональным. Следовательно, *множество $\mathcal{O}(L)$ всех ортогональных операторов евклидова пространства L образу-ет группу.*

Пусть $\mathcal{F} = (\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n)$ – ортонормированный базис евклидова пространства L, и A – матрица ортогонального оператора φ в этом базисе. Возьмем произвольные элементы $\mathbf{x} = \sum_i x_i \mathbf{f}_i$ и $\mathbf{y} = \sum_i y_i \mathbf{f}_i$ пространства L. Тогда соотношение $\varphi(\mathbf{x})\varphi(\mathbf{y}) = \mathbf{x}\mathbf{y}$ эквивалентно следующему

$$\left[A \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix} \right]^\top \cdot A \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix} = (x_1, x_2, \ldots, x_n) \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix}$$

В свою очередь это эквивалентно равенству

$$A^\top A = E \tag{3.36}$$

Матрица A с условием (3.36) называется *ортогональной.* Множество ортогональных матриц образует подгруппу $\mathcal{O}(n)$ в группе $\mathrm{GL}(n, \mathbb{R})$ всех невырожденных матриц.

Опишем группу $\mathcal{O}(2)$. Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(2)$ – матрица ортогонального оператора φ . Это эквивалентно системе равенств

$$a^2 + b^2 = 1, \quad b^2 + d^2 = 1, \quad ab + cd = 0.$$

Пусть угол $\alpha \in [0, 2\pi)$ таков, что $a = \cos\alpha$ и $c = \sin\alpha$. Тогда либо $b = -\sin\alpha$ и $d = \cos\alpha$ и A – матрица поворота на угол α, либо $b = \sin\alpha$ и $d = -\cos\alpha$. В этом случае A имеет собственные числа ± 1 и собственные вектора $\mathbf{s}_1 = \cos\alpha\mathbf{f}_1 + \sin\alpha\mathbf{f}_2$ и $\mathbf{s}_2 = -\sin\alpha\mathbf{f}_1 + \cos\alpha\mathbf{f}_2$. Матрица оператора φ в базисе $\mathbf{s}_1$, $\mathbf{s}_2$ имеет диагональный вид $\operatorname{diag}(1, -1)$. Мы доказали следующую теорему

Теорема 1. *Для любого ортогонального оператора плоскости $\mathbb{R}^2$ найдется ортонормированный базис в котором этот оператор будет иметь вид*

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \text{ или } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Прежде чем описывать $\mathcal{O}(3)$ докажем ряд лемм

Лемма 1. *Любая квадратная матрица нечетного размера имеет вещественное собственное число.*

Доказательство. Это следствие известного из анализа результата – любой многочлен нечетной степени имеет хотя один вещественный корень. $\square$

Лемма 2. *Собственные числа ортогонального оператора могут быть только 1 и -1.*

Доказательство. Пусть $\mathbf{x}$ – собственный вектор ортогонального оператора φ с собственным числом λ. Тогда

$$|\mathbf{x}| = |\varphi(\mathbf{x})| = |\lambda\mathbf{x}| = |\lambda|\,|\mathbf{x}|$$

Отсюда следует результат, если учесть, что $|\mathbf{x}| \neq 0$. $\square$

Предложение 1. *Пусть M – подпространство пространства L со скалярным произведением, $\varphi : L \to L$ – ортогональный оператор. Если M – инвариантно относительно φ, то и ортогональное дополнение $M^\top$ также φ-инвариантно.*

Доказательство. Пусть $\mathbf{a} \in M$, $\mathbf{b} \in M^\top$. Тогда $\varphi(\mathbf{b})\mathbf{a} = \mathbf{b}\varphi(\mathbf{a}) = 0$, так как $\varphi(\mathbf{a}) \in M$. Отсюда следует, что $\varphi(\mathbf{b}) \in M^\top$. $\square$

Теорема 2. *Для любого ортогонального оператора φ трехмерного евклидова пространства найдется ортонормированный базис, в котором матрица этого оператора имеет вид:*

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix} \tag{3.37}$$

Доказательство. Пусть $\mathbf{f}_1$ – единичный собственный вектор оператора φ. Тогда подпространство $M = \mathbf{f}_1\mathbb{R}$ инвариантно относительно φ. Следовательно, плоскость $M^\top$ также φ-инвариантна (см. предложение 1). Выберем ортонормированный базис $\mathbf{f}_1$, $\mathbf{f}_2$ на этой плоскости, так что матрица сужения $\varphi_{/M^\top}$ имеет вид как в теореме 1. В случае матрицы вращения, базис $\mathbf{f}_1$, $\mathbf{f}_2$, $\mathbf{f}_3$ искомый. Разберем случай $\varphi(\mathbf{f}_2) = \mathbf{f}_2$, $\varphi(\mathbf{f}_3) = -\mathbf{f}_3$. Если $\varphi(\mathbf{f}_1) = \mathbf{f}_1$, то перенумерацией базиса $\mathbf{f}_i$ получаем искомый базис $\mathbf{s}_1 = \mathbf{f}_3$, $\mathbf{s}_2 = \mathbf{f}_2$, $\mathbf{s}_3 = \mathbf{f}_1$ в котором матрица оператора φ имеет диагональный вид $\mathrm{diag}(-1, 1, 1)$. Иначе, матрица оператора φ в базисе $\mathbf{f}_i$ $(i = 1, 2, 3)$ имеет диагональный вид $\mathrm{diag}(-1, 1, -1)$. Тогда перенумеруем базис $\mathbf{f}_i$ по другому: $\mathbf{s}_1 = \mathbf{f}_2$, $\mathbf{s}_2 = \mathbf{f}_1$, $\mathbf{s}_3 = \mathbf{f}_3$. В базисе $\mathbf{s}_i$ матрица оператора φ имеет требуемый вид:

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \cos\pi & -\sin\pi \\ 0 & \sin\pi & \cos\pi \end{pmatrix}$$

□

3.12 Кватернионы

Кватернионы были изобретены немецким математиком Гамильтоном в 1843 году. Это был первый пример конечномерной некоммутативной алгебры над полем действительных чисел, в которой каждый ненулевой элемент обратим (т. е. *алгебры с делением* или *тела*). Как потом оказалось, это был и последний пример такой алгебры, ибо конечномерная алгебра с делением над $\mathbb{R}$ есть либо само поле $\mathbb{R}$, либо поле комплексных чисел $\mathbb{C}$, либо тело кватернионов $\mathbb{H}$ согласно **теореме Фробениуса** (см.[B], глава 11, §6, теорема 4). Произвольный элемент $q \in \mathbb{H}$ однозначно записывается в виде

$$q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k},$$

где $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Если $a_0 = 0$, то такой кватернион называется *чистым.* Во-первых, превратим $\mathbb{H}$ в четырехмерное линейное пространство на полем $\mathbb{R}$, складывая кватернионы и умножая их на числа покомпонентно:

$$(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) + (a_0' + a_1'\mathbf{i} + a_2'\mathbf{j} + a_3'\mathbf{k}) =$$

$$= (a_0 + a_0') + (a_1 + a_1')\mathbf{i} + (a_2 + a_2')\mathbf{j} + (a_3 + a_3')\mathbf{k};$$

$$\lambda(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) = \lambda a_0 + \lambda a_1\mathbf{i} + \lambda a_2\mathbf{j} + \lambda a_3\mathbf{k}.$$

Чистые кватернионы образуют подпространство $\mathcal{V}(\mathbb{E}^3) = \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R}$, которое будем отождествлять с трехмерным линейным евклидовым пространством со стандартным базисом $\mathbf{i}, \mathbf{j}, \mathbf{k}$. Для определения умножения кватернионов используем скалярное и векторное произведения. Операцию скалярного произведения между векторами $\mathbf{a}, \mathbf{b} \in \mathcal{V}(\mathbb{E}^3)$ придется обозначать, например, как $\mathbf{a} * \mathbf{b}$, оставив $\mathbf{a} \cdot \mathbf{b}$ для обозначения произведения кватернионов. Итак, если даны два кватерниона $q = a + \mathbf{a}$ и $t = b + \mathbf{b}$, где $\mathbf{a}, \mathbf{b}$ – чистые кватернионы, а a, b – числа, то по определению полагаем:

$$q \cdot t = (a + \mathbf{a})(b + \mathbf{b}) = (ab - \mathbf{a} * \mathbf{b}) + (a\mathbf{b} + b\mathbf{a} + \mathbf{a} \times \mathbf{b}).$$

Записывая q и t более подробно и вспоминая записи скалярного и векторного произведений через координаты, получим:

$$\begin{gathered}(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})(b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + \\ +(a_0b_1 + b_0a_1 + a_2b_3 - a_3b_2)\mathbf{i} + (a_0b_2 + b_0a_2 + a_3b_1 - a_1b_3)\mathbf{j} + \\ +(a_0b_3 + b_0a_3 + a_1b_2 - a_2b_1)\mathbf{k}.\end{gathered}$$

В частности из определения умножения кватернионов вытекает, что

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1. \tag{3.38}$$

Именно соотношения (3.38) и были ключевым моментом в изобретении кватернионов. По преданию, они и были вырезаны на мосту, по которому в этот момент прогуливался Гамильтон. Кроме того, из определения умножения кватернионов следует:

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}; \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}; \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j} \tag{3.39}$$

Кватернион $a - \mathbf{a}$ назовем *сопряженным к кватерниону* $q = a + \mathbf{a}$ и будем его обозначать $\overline{q}$. Нетрудно проверить, что

$$q\overline{q} = \overline{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

и поэтому $\overline{q}q = 0 \Leftrightarrow q = 0$. Величина $\overline{q}q$ называется *нормой кватерниона* q и обозначается $\|q\|$, а арифметический корень из нормы называется *модулем кватерниона* q и обозначается $|q|$.

Теорема 1. *Множество кватернионов относительно определенных выше операций сложения и умножения образует кольцо с делением, т.е. тело. Каждый ненулевой кватернион q имеет обратный $q^{-1} = \frac{1}{\|q\|}\overline{q}$. Отображение $\mathbb{R} \to \mathbb{H}$, сопоставляющее числу a кватернион $a + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, является взаимно-однозначным морфизмом.*

Доказательство. Так как сложение и умножение на числа кватернионов покомпонентное, то $\mathbb{H}$ – линейное пространство над $\mathbb{R}$ и, в частности, абелева группа.

Далее, проверим гомоморфность вложения $a \to a + \mathbf{0}$:

$$(a + \mathbf{0}) + (b + \mathbf{0}) = (a + b) + \mathbf{0};$$

$$(a+\mathbf{0})(b+\mathbf{0}) = (ab - \mathbf{0} * \mathbf{0}) + (a\mathbf{0} + b\mathbf{0} + \mathbf{0}\times\mathbf{0}) = ab + \mathbf{0}.$$

При этом $1 = 1+\mathbf{0}$ – единичный элемент. Проверим дистрибутивность, т. е. равенства

$$(s+t)q = sq + tq; \qquad q(s+t) = qs + qt.$$

Обозначим $q = a + \mathbf{a}$, $s = b + \mathbf{b}$, $t = c + \mathbf{c}$, где $a, b, c \in \mathbb{R}$ и $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{V}(\mathbb{E}^3)$. Тогда

$$q(s+t) = (a+\mathbf{a})((b+c) + (\mathbf{b}+\mathbf{c})) =$$
$$= a(b+c) - \mathbf{a} * (\mathbf{b}+\mathbf{c}) + a(\mathbf{b}+\mathbf{c}) + (b+c)\mathbf{a} + \mathbf{a}\times(\mathbf{b}+\mathbf{c}) =$$
$$= ab - \mathbf{a}*\mathbf{b} + a\mathbf{b} + b\mathbf{a} + \mathbf{a}\times\mathbf{b} + ac - \mathbf{a}*\mathbf{c} + c\mathbf{a} + a\mathbf{c} = qs + qt.$$

Аналогично проверяется равенство $(s+t)q = sq+tq$. Ассоциативность умножения, т. е. равенство $q(st) = (qs)t$ достаточно теперь, после доказательства дистрибутивности и гомоморфности вложения $\mathbb{R} \to \mathbb{C}$, проверить только для $q, s, t \in \{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Если какой-либо из элементов $q, s, , t$ равен 1, то равенство $q(st) = (qs)t$ очевидно. Остается $3^3 = 27$ случаев, перебор которых осуществляется непосредственно с помощью соотношений (3.38) и (3.39).

Итак, доказано, что $\mathbb{H}$ – ассоциативное кольцо с единицей. Оно не коммутативно, так как, например, $\mathbf{ij} \neq \mathbf{ji}$. Но действительные числа лежат в центре $\mathbb{H}$, т.е. $rq = qr$ для любых $r \in R$ и $q \in \mathbb{H}$.

Проверим теперь, что кватернион $\frac{1}{\|q\|}\overline{q}$ обратен к ненулевому кватерниону q.

$$q \cdot (\frac{1}{\|q\|}\overline{q}) = \frac{1}{\|q\|}q\overline{q} = \frac{\|q\|}{\|q\|} = 1$$

□

Задача 1. Доказать, что $\mathbb{R}$ совпадает с центром алгебры $\mathbb{H}$.

Свойства операции сопряжения и модуля кватернионов

А. $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$; $\overline{q_1 q_2} = \overline{q_2}\cdot\overline{q_1}$.

Доказательство. Пусть $q_1 = a + \mathbf{a}$, $q_2 = b + \mathbf{b}$ как и ранее. Тогда

$$\overline{q_1+q_2} = \overline{(a+b) + (\mathbf{a}+\mathbf{b})} = (a+b) - \mathbf{a} - \mathbf{b} == \overline{q_1} + \overline{q_2}$$
$$\overline{q_1q_2} = \overline{(ab - \mathbf{a}*\mathbf{b}) + a\mathbf{b} + b\mathbf{a} + \mathbf{a}\times\mathbf{b}} = ab - \mathbf{a}*\mathbf{b} - a\mathbf{b} - b\mathbf{a} - \mathbf{a}\times\mathbf{b} =$$
$$= ab - (-\mathbf{a}) * (-\mathbf{b}) - a\mathbf{b} - b\mathbf{a} + (-\mathbf{b})\times(-\mathbf{a}) = \overline{q_2}\overline{q_1}$$

□

Б. $q \in \mathcal{V}(\mathbb{E}^3)$ тогда и только тогда, когда $\overline{q} = -q$

В. $\overline{\overline{q}} = q$

Г. $|q_1q_2| = |q_1|\,|q_2|$

Доказательство.

$$|q_1q_2|^2 = q_1q_2\overline{q_1q_2} = q_1q_2\overline{q_2}\overline{q_1} = q_1\,|q_2|^2\,\overline{q_1} = |q_1|^2\,|q_2|^2$$

□

Д. (неравенство треугольника) $|q_1 + q_2| \leq |q_1| + |q_2|$

Доказательство. Это общее свойство длины вектора. В данном случае q_1 и q_2 следует интерпретировать как вектора в четырехмерном евклидовом пространстве $\mathbb{H}_{\mathbb{R}}$ с ортонормированным базисом $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$. □

Е. $|q^{-1}| = 1/\,|q_1|$

Это утверждение есть следствие свойства А.

Обозначим через

$$\mathbb{S}^3 = \{q \in \mathbb{H} \mid |q| = 1\}$$

– единичную трехмерную сферу в четырехмерном пространстве. Из свойств Г и Е вытекает, что $\mathbb{S}^3$ – группа по умножению. Каждому кватерниону $u \in \mathbb{S}^3$ сопоставим преобразование $conj_u : \mathcal{V}(\mathbb{E}^3) \to \mathcal{V}(\mathbb{E}^3)$ такое, что

$$conj_u(\mathbf{b}) = u\mathbf{b}u^{-1}. \tag{3.40}$$

Если $\mathbf{b}$ – чистый кватернион, т. е. $\mathbf{b} \in \mathcal{V}(\mathbb{E}^3)$, то нетрудно проверить, что и $u\mathbf{b}u^{-1}$ также чистый кватернион. Предварительно заметим, что $u^{-1} = \overline{u}$ для любого $u \in \mathbb{S}^3$, как следует из теоремы 1. Далее

$$\overline{u\mathbf{b}u^{-1}} = \overline{u\mathbf{b}\overline{u}} = \overline{\overline{u}}\,\overline{\mathbf{b}}\,\overline{u} = u(-\mathbf{b})\overline{u} = -u\mathbf{b}u^{-1}.$$

Тем самым преобразование (3.40) корректно определено, как преобразование сферы $\mathbb{S}^3$. Прежде чем переходить к следующему результату напомним, что ортогональное преобразование пространства сохраняет длины и углы между векторами, но может изменять ориентацию пространства. С алгебраической точки зрения это означает, что определитель матрицы ортогонального преобразования может быть равен -1 как, например, для отражения относительно гиперплоскости. Подмножество ортогональных преобразований с определителем единица (т. е. сохраняющих ориентацию) образует подгруппу $\mathrm{SO}(n)$ в группе $\mathcal{O}(n)$. Это легко следует из свойства: определитель произведения равен произведению определителей.

Предложение 1. *Преобразование (3.40) – ортогональный линейный оператор с единичным определителем, т.е.* $conj_u \in \mathrm{SO}(3)$.

Доказательство. Так как $|u\mathbf{b}u^{-1}| = |u|\,|\mathbf{b}|\,|u^{-1}| = |\mathbf{b}|$, то $conj_u$ сохраняет длины. Линейность следует из соотношений

$$u(r_1\mathbf{b}_1 + r_2\mathbf{b}_2)u^{-1} = r_1(u\mathbf{b}_1u^{-1}) + r_2(u\mathbf{b}_2u^{-1})$$

верным для любых чисел r_1, r_2 и любых кватернионов $\mathbf{b}_1, \mathbf{b}_2$. Остается доказать, что $conj_u$ сохраняет ориентацию пространства $\mathcal{V}(\mathbb{E}^3)$. Запишем $u = c + d\mathbf{f}$, где $\mathbf{f} \in \mathcal{V}(\mathbb{E}^3)$, $|\mathbf{f}| = 1$ и $c, d \in \mathbb{R}$. Так как $|u| = 1$, то $c^2 + d^2 = 1$. Следовательно, можно подобрать $\alpha \in [0, 2\pi)$ такое, что $c = \cos\alpha$, а $d = \sin\alpha$. Если $\alpha = 0$, то $u = 1$ и $conj_u = \mathrm{Id}$ – сохраняет ориентацию. Рассмотрим $\det(conj_u)$ как функцию от α. Обозначим ее $F(\alpha)$. Так как $F(\alpha)$ – определитель 3×3-матрицы с коэффициентами, являющимися комбинацией $\cos\alpha$ и $\sin\alpha$, то $F(\alpha)$ непрерывна. Выше мы доказали, что $conj_u$ – ортогональное преобразование. Значит, $F(\alpha)$ может принимать лишь значения ± 1. Но $F(0) = 1$. Если бы для какого-то угла α_0 значение $F(\alpha_0)$ было бы равно -1, то по теореме Больцано-Коши нашлось бы число $\alpha_* \in (0, \alpha_0)$ такое, что $F(\alpha_*) = 0$. Это противоречит невырожденности преобразования $conj_u$. Противоречие показывает, что $F(\alpha) \equiv 1$, следовательно $conj_u$ – сохраняет ориентацию. □

Предложение 2. *Пусть $u = \cos\alpha + \sin\alpha\,\mathbf{f}$ для некоторых α и $\mathbf{f} \in \mathcal{V}(\mathbb{E}^3)$, $|\mathbf{f}| = 1$. Тогда $conj_u$ – поворот вокруг оси $\mathbf{f}$ на угол 2α.*

Доказательство. Ясно, что $\mathbf{f}u = u\mathbf{f}$, откуда следует равенство
$u\mathbf{f}u^{-1} = \mathbf{f}$. Следовательно, $\mathbf{f}$ – неподвижная ось вращения $conj_u$.

Возьмем какой-либо единичный вектор $\mathbf{b} \in \mathcal{V}(\mathbb{E}^3)$, ортогональный $\mathbf{f}$. Тогда

$$conj_u(\mathbf{b}) = u\mathbf{b}\overline{u} = (\cos\alpha + \sin\alpha\,\mathbf{f})\mathbf{b}(\cos\alpha - \sin\alpha\,\mathbf{f}) =$$
$$= (\cos\alpha + \sin\alpha\,\mathbf{f})(\sin\alpha\,\mathbf{b} * \mathbf{f} + \cos\alpha\,\mathbf{b} - \sin\alpha\,\mathbf{b} \times \mathbf{f}) =$$
$$= (\cos\alpha + \sin\alpha\,\mathbf{f})(\cos\alpha\,\mathbf{b} - \sin\alpha\,\mathbf{b} \times \mathbf{f}) =$$
$$= \cos^2\alpha - (\sin\alpha\,\mathbf{f}) * (\cos\alpha - \sin\alpha\,\mathbf{b} \times \mathbf{f}) + \cos^2\alpha\,\mathbf{b} - \cos\alpha\sin\alpha\,\mathbf{b} \times \mathbf{f} +$$
$$+ \sin\alpha\cos\alpha\,\mathbf{f}\mathbf{b} - \sin^2\alpha\,\mathbf{f} \times (\mathbf{b} \times \mathbf{f}) =$$
$$= \cos^2\alpha\,\mathbf{b} + 2\sin\alpha\cos\alpha\,\mathbf{f} \times \mathbf{b} - \sin^2\alpha\,\mathbf{b} = \cos 2\alpha + \sin 2\alpha\,\mathbf{f} \times \mathbf{b}$$

Если обозначить угол между векторами $\mathbf{b}$ и $conj_u(\mathbf{b})$ через φ, то

$$\cos\varphi = \mathbf{b} * (\cos 2\alpha + \sin 2\alpha\mathbf{f} \times \mathbf{b}) = \cos 2\alpha$$

Отсюда и следует результат. □

Следствие. *Отображение $u \to conj_u$ – морфизм группы $\mathbb{S}^3$ на группу $\mathrm{SO}(3)$. Ядро этого отображения – группа знаков ± 1.*

Доказательство. Проверим гомоморфность, т. е. равенство $conj_{uv} = conj_u \circ conj_v$. Действительно,

$$conj_{uv}(\mathbf{b}) = uv\mathbf{b}(uv)^{-1} = uv\mathbf{b}v^{-1}u^{-1} = u \cdot conj_v(\mathbf{b})u^{-1} =$$
$$= conj_u(conj_v(\mathbf{b})) = conj_u \circ conj_v(\mathbf{b}).$$

Для любого вращения ψ пространства $\mathcal{V}(\mathbb{E}^3)$ вокруг некоторой оси найдется кватернион $u \in \mathbb{S}^3$ такой, что $conj_u = \psi$. Это есть следствие предложения 2. Отсюда вытекает, что $conj$ – отображение "на".

Остается вычислить ядро отображения $u \to conj_u$. Пусть $conj_u = \mathrm{Id}$, т.е. $u\mathbf{b}u^{-1} = \mathbf{b}$ для любого $\mathbf{b} \in \mathcal{V}(\mathbb{E}^3)$. Тогда $\mathbf{b}u = u\mathbf{b}$. Очевидно, что и $bu = ub$ для любого $b \in \mathbb{R}$. Но тогда равенство $qu = uq$ верно для любого кватерниона q. Так как центр тела кватернионов состоит из чисел (см. задача 1), то $u \in \mathbb{R}$. Легко видеть, что $\mathbb{R} \cap \mathbb{S}^3 = \{\pm 1\}$. Это и завершает доказательство. $\square$

Задача 2. Опишите множество всех решений уравнения $x^2 = -1$ в теле кватернионов.

Задача 3. Доказать, что элементы $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ образуют группу по умножению в теле кватернионов. Найти порядки элементов и подгруппы. Коммутативна ли эта группа?

Литература

[Б] Н. Бурбаки. *Теория множеств.* М. Мир. 1965.

[БЛ] Р. Бэлман. *Введение в теорию матриц.* М.Наука. 1969.

[В] Э.Б. Винберг. *Курс алгебры.* М. Факториал Пресс. 2001.

[Д] Н.И. Дубровин. *Конспект лекций по алгебре.* Владимир. ВлГУ. 1997.

[К] А.И. Кострикин. *Введение в алгебру.* М. Наука.1977.

[КМ] А.И. Кострикин, Ю.И. Манин *Линейная алгебра и геометрия.* Из-во МГУ. 1980.

[М] Э. Мендельсон. *Введение в математическую логику.* М. Наука. 1984.

[П] Н.С. Пискунов. *Дифференциальное и интегральное исчисление. Ч.2.* М.Наука.1978.

[ПМ] М.М. Постников. *Лекции по геометрии.* Из-ние второе. М.Наука. 1986.