А. П. Пожидаев, С. Р. Сверчков, И. П. Шестаков

ЛЕКЦИИ ПО АЛГЕБРЕ

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

А. П. Пожидаев, С. Р. Сверчков, И. П. Шестаков

ЛЕКЦИИ ПО АЛГЕБРЕ

Часть 1

Учебное пособие

Новосибирск

2011

УДК 512.64(075)
ББК: В14.5я73-1
Г 144
А. П. Пожидаев, С. Р. Сверчков, И. П. Шестаков, Лекции по алгебре: В 2 ч.: Учеб. пособие / Новосиб. гос. ун-т. Новосибирск, 2011. 102 с.

ISBN 978-5-94356-751-3

Данный курс лекций содержит запись основного курса высшей алгебры, читавшегося авторами в 1989 – 2010 гг. на одном из потоков первого курса механико-математического факультета Новосибирского государственного университета. Часть 1 соответствует программе первого семестра, а часть 2 — программе второго семестра. Для чтения и понимания текста от читателя требуется знание элементарных понятий теории множеств, отображений и принципа математической индукции. Предназначено для студентов и преподавателей по курсу высшей алгебры.

Издание подготовлено для научно-исследовательского университета в рамках реализации Программы развития НИУ-НГУ.

ISBN 978-5-94356-751-3

Оглавление

Введение

Что такое алгебра? Ответить на этот вопрос однозначно, достаточно определенно и к тому же коротко нельзя. С одной стороны, истоки ее уходят вглубь веков — можно сказать, что алгебра началась, когда появились первые алгебраические операции — арифметические действия над $\mathbb{N}$ и $\mathbb{Q}^+$. С другой стороны, можно сказать, что алгебра началась, когда цифры стали заменяться буквами. Точка зрения на то, что является объектом исследования алгебры постоянно менялась. Так, в 17–18 вв. под алгеброй понималась наука о буквенных вычислениях, решение алгебраических уравнений и т.п. В 18–19 вв. алгебра — это алгебра многочленов, теория систем алгебраических уравнений с несколькими неизвестными, теория матриц и определителей. С середины 19 в. центр тяжести в исследованиях смещается на изучение произвольных алгебраических операций, что произошло вследствие расширения понятия числа: появились комплексные числа, кватернионы, октонионы. В конце 19 – начале 20 вв. возникает общая аксиоматическая основа всех старых идей. В принципе, можно сказать, что предметом изучения современной алгебры являются множества с заданными на них алгебраическими операциями. Поэтому, если говорить о современной алгебре и ее приложениях, то нужно описать все ее основные структуры: группы, кольца, поля и т.д. Это, в частности, в самом вводном объеме, будет сделано нами в данном курсе лекций, а более содержательное знакомство с алгеброй будет происходить по мере ее изучения.

Говоря общими словами, можно сказать, что алгебра по отношению ко всей математике играет примерно такую же роль, как математика по отношению к остальным наукам. Наряду с “математизацией” естествознания в наши дни не без основания говорят об “алгебраизации” математики, т. е. о проникновении идей и методов алгебры в самые различные разделы математики, а также физики. В настоящее время алгебраический язык стал играть роль “языка межнационального общения”, связывающего между собой различные дисциплины математики и физику.

Процесс применения алгебры похож на процесс применения математики.

Чтобы изучить методами математики какое-либо явление естествознания, строят его математическую модель. Если она достаточно адекватно отражает свойства явления, то, изучая ее методами математики, мы можем что-то говорить и о самом явлении. Аналогично, различным объектам математического исследования можно сопоставить некоторый алгебраический объект, в той или иной мере отражающий свойства исходного объекта, и т. д. Выдающийся алгебраист И. Р. Шафаревич называет этот процесс "координатизацией", имея в виду, что математические объекты координатизируются алгебраическими.

Самый наглядный пример: декартовы координаты, сводящие геометрические задачи к решению алгебраических уравнений. Здесь координатами служат числа, которые можно складывать и умножать. Однако в других случаях для такой "координатизации" обычных чисел с обычным сложением и умножением далеко не достаточно. Наоборот, сталкиваясь с новым типом объектов, мы вынуждены конструировать (или открывать) новые типы координатизирующих их "величин". Построение и исследование возникающих таким образом "величин" с определенными на них операциями — этим и характеризуется (конечно, очень приближенно) место алгебры в математике.

С этой точки зрения, развитие любого раздела алгебры состоит из двух этапов. Первый из них — рождение нового типа алгебраических объектов из некоторой проблемы координатизации; второй — их дальнейшая жизнь, т. е. систематическое развитие теории этого класса объектов, иногда тесно связанное, а иногда и совсем не связанное с той областью, в связи с которой объекты возникли. Здесь вновь ситуация такая же, как и у математики в целом.

Линейная алгебра. Основное внимание в данном курсе уделяется линейной алгебре. С широкой точки зрения, содержание линейной алгебры состоит в разработке математического языка для выражения одной из самых общих естественно-научных идей — идеи линейности. Возможно, ее важнейшим частным случаем является принцип линейности малых приращений: почти всякий естественный процесс почти всюду в малом линеен (отметим, что "почти" здесь стоит по сути — сейчас и фракталы рассматриваются как естественные объекты, и квантовые вычисления, которые нелинейны при любом "увеличении"). Этот принцип лежит в основе всего математического анализа и его приложений. Основные методы и понятия линейной алгебры являются на самом деле общими для многих разделов математики и ее приложений: математического и

функционального анализа, линейных неравенств математической экономики, теории кодирования (над конечными полями), вычислительных методов линейной алгебры, полилинейной и общей алгебры. Краеугольным камнем в здании линейной алгебры лежит знакомая всем со школы векторная алгебра трехмерного пространства, и на первых порах можно применять ко всем новым понятиям 3-мерную геометрическую интуицию.

Основной модельной задачей линейной алгебры является решение систем линейных уравнений. С изучения линейных уравнений мы и начинаем, однако предварительно вводим понятие поля и, в частности, строим поле комплексных чисел, чтобы в дальнейшем рассматривать системы линейных уравнений в более общей ситуации (однако для простоты читатель всегда может понимать под полем действительные числа). Далее у нас естественно возникают матрицы, векторные пространства и линейные преобразования, затем вводится понятие определителя матрицы, даются его основные свойства и приложения к решению систем линейных уравнений. Все это служит содержанием первой главы. Во второй главе мы рассматриваем основные алгебраические системы: группы, кольца и поля. В третьей главе изучаются многочлены. Четвертая глава дает более глубокий анализ линейных преобразований над алгебраически замкнутым полем, а пятая — над полями $\mathbb{R}$ и $\mathbb{C}$. Шестая глава посвящена основам теории квадратичных форм, а заключительная, седьмая глава посвящена основам теории базисов Грёбнера-Ширшова, которые случае коммутативных алгебр называются базисами Грёбнера. В конце каждой главы приведены задачи для самостоятельной работы. Уровень сложности задач довольно разнообразный: есть как и задачи для закрепления материала, так и задачи, требующие творческого подхода.

Авторы благодарны В. Н. Желябину и В. А. Чуркину за некоторые любезно предоставленные интересные задачи, включенные в настоящее издание.

Обозначения: $A \Rightarrow B$ означает, что из утверждения A следует утверждение B; $A \Leftrightarrow B$ — эквивалентность утверждений A и B; квантор всеобщности $\forall$ служит заменой выражения “для всех”; $\exists$ — квантор существования; $\exists!$ — существует единственный; символ $\models$ заменяет выражение “выполняется”; $\mathbb{N}$ обозначает натуральные числа, $\mathbb{N}_0$ — натуральные числа с нулем, $\mathbb{Z}$ — целые числа, $\mathbb{Q}$ — рациональные, $\mathbb{R}$ — действительные, $\mathbb{C}$ — комплексные числа; $\mathbf{i}$ — мнимая единица в $\mathbb{C}$, символ $:=$ означает равенство по определению, $\lozenge$ порой обозначает начало

доказательства, а конец доказательства обозначается символом $\square$.

Нумерация: нумерация параграфов в каждой части сквозная. Ссылка, например, на утверждение 1 означает утверждение 1 данного параграфа, ссылка же, например, на утверждение 1 §2.4 означает утверждение 1 четвертого параграфа второй части.

Литература:

Э. Б. Винберг, Курс алгебры, М.: Факториал, 1999;

А. И. Кострикин, Введение в алгебру, Части I-III, М.: Физ.-Мат. Литература, 2000;

А. Г. Курош, Курс высшей алгебры, СПб., 2003;

А. И. Мальцев, Основы линейной алгебры, М.: Наука, 2005;

Б. Л. ван дер Варден, Алгебра, М.: Наука, 1976.

Глава 1

Векторные пространства. Матрицы и определители

Эта глава начинается с изучения линейных уравнений, однако предварительно вводится понятие поля и, в частности, строится поле комплексных чисел, чтобы в дальнейшем рассматривать системы линейных уравнений в более общей ситуации (однако для простоты читатель всегда может понимать под полем действительные числа). Далее естественно возникают матрицы, векторные пространства и линейные преобразования, затем вводится понятие определителя матрицы, даются его основные свойства и приложения к решению систем линейных уравнений.

§1. Определение и примеры полей

Декартово произведение $A \times B$ множеств A и B есть множество всех упорядоченных пар (a, b), где $a \in A$, $b \in B$. Таким образом, $A \times B = \{(a, b) : a \in A, \ b \in B\}$. *Декартова n-ая степень* множества A есть множество $A^n = \{(a_1, \ldots, a_n) : a_i \in A\}$.

Пример. Пусть $A = \{1, 2\}$, $B = \{3, 7, 8\}$. Тогда

$$A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\};$$
$$A \times B = \{(1, 3), (1, 7), (1, 8), (2, 3), (2, 7), (2, 8)\}.$$

Пусть X — некоторое множество. Отображение $f : X \times X \to X$ называется *бинарной операцией* на X, т. е. f — бинарная операция, если для любых $x_1, x_2 \in X$ однозначно определен элемент $f(x_1, x_2) \in X$. Запишем $x * y$ вместо $f(x, y)$. Бинарная операция называется *ассоциативной*, если $(a * b) * c = a * (b * c)$ для любых $a, b, c \in X$ и *коммутативной*, если $a * b = b * a$ для любых $a, b \in X$.

Множество F называется *полем*, если в нем определены две ассоциативные и коммутативные бинарные операции $+$ (сложение) и $\cdot$ (умножение) такие, что

1) $(\exists\, 0 \in F : \forall\, a \in F)\ a + 0 = 0 + a = a$;

2) $(\forall\, a \in F\ \exists\, b \in F)\ a + b = b + a = 0$, ($b$ обозначается как $-a$);

3) $(\exists 1 \in F\ (1 \neq 0) : \forall\, a \in F)\ a \cdot 1 = 1 \cdot a = a$;

4) $(\forall\, a \in F\ (a \neq 0)\ \exists\, b \in F)\ a \cdot b = b \cdot a = 1$ (элемент b называется *обратным* к a и обозначается a^{-1});

5) $(\forall\, a, b, c \in F)\ (a + b)c = ac + bc$.

Примеры полей.

- $\langle \mathbb{Q}; +, \cdot \rangle$.
- $\langle \mathbb{R}; + \rangle$.
- $\langle \{0, 1\}; +, \cdot \rangle$, где операции стандартны, кроме $1 + 1 = 0$.
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Заметим, что $\mathbb{N}$ и $\mathbb{Z}$ полями не являются. Всюду далее символом F мы будем обозначать некоторое поле, элементы поля часто называются *скалярами*.

§2. Поле комплексных чисел: конструкция в виде пар действительных чисел

Пусть $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$. Определим на $\mathbb{C}$ операции:

$$(a, b) + (c, d) = (a + c, b + d),\ (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Теорема 1. $\langle \mathbb{C}; +, \cdot \rangle$ *является полем.*

Доказательство. Заметим, что $0 = (0, 0)$ и $1 = (1, 0)$ являются, соответственно, нулём и единицей в $\mathbb{C}$. Элемент $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$ является обратным к (a, b). Далее доказательство состоит в очевидной проверке аксиом поля. □

Запишем $(a, b) = a \cdot (1, 0) + b \cdot (0, 1) := a \cdot 1 + b \cdot \mathbf{i} := a + b\mathbf{i}$, где 1 — единица $\mathbb{C}$, $\mathbf{i}^2 = (-\mathbf{i})^2 = -1$. Тогда $\mathbb{C} = \left\{a \cdot 1 + b \cdot \mathbf{i} : a, b \in \mathbb{R},\ \mathbf{i}^2 = -1\right\}$ называется *полем комплексных чисел*. Отождествляя элементы $(a, 0)$ с элементами a из $\mathbb{R}$, получаем $\mathbb{R} \subseteq \mathbb{C}$. Иногда будем также использовать запись $(a, b) := a + \mathbf{i}b$.

§3. Модуль и аргумент комплексного числа

Любому элементу $z = a + b\mathbf{i} \in \mathbb{C}$ можно поставить в соответствие вектор координатной плоскости, у которого проекция на ось x равна a, на ось y равна b и φ — угол наклона с осью x.

Действительное число $|z| = \sqrt{a^2 + b^2}$ называется модулем комплексного числа z; угол $\varphi := \arg z$ называется аргументом числа z (определён с точностью до $2\pi n$), $\arg 0$ не определен. Число $a := Re\, z$ называют действительной, а $b := Im\, z$ — мнимой частью z. Таким образом, $z = Re\, z + \mathbf{i} Im\, z$. Очевидно, что $Re\,(z_1 + z_2) = Re\,(z_1) + Re\,(z_2)\,, Im\,(z_1 + z_2) = Im\,(z_1) + Im\,(z_2)$.

Можно также использовать тригонометрическую запись комплексного числа z:

$$z = |z| \cdot (\cos\varphi + \mathbf{i}\sin\varphi).$$

Заметим, что $z_1 = z_2 \Leftrightarrow |z_1| = |z_2|\,,\ \arg z_1 = \arg z_2 + 2\pi k,\quad k \in \mathbb{Z}$.

Лемма 1. *Для любых $z_1, z_2 \in \mathbb{C}$ справедливо*
1) $\arg z_1 \cdot z_2 = \arg z_1 + \arg z_2 + 2\pi k, k \in \mathbb{Z}$; $|z_1 \cdot z_2| = |z_1| \cdot |z_2|\,$;
2) если $z_2 \neq 0$, то $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$; $\arg \frac{z_1}{z_2} = \arg z_1 - \arg z_2 + 2\pi k,\ k \in \mathbb{Z}$.

Доказательство. Имеем $z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot (\cos\varphi_1 + \mathbf{i}\sin\varphi_1) \cdot (\cos\varphi_2 + \mathbf{i}\sin\varphi_2) = |z_1| \cdot |z_2| \cdot (\cos(\varphi_1 + \varphi_2) + \mathbf{i}\sin(\varphi_1 + \varphi_2))$. Следовательно, $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ и $\arg z_1 \cdot z_2 = \arg z_1 + \arg z_2 + 2\pi k$. Далее,

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}\frac{(\cos\varphi_1 + \mathbf{i}\sin\varphi_1)}{(\cos\varphi_2 + \mathbf{i}\sin\varphi_2)} = \frac{|z_1|}{|z_2|}(\cos\varphi_1 + \mathbf{i}\sin\varphi_1)(\cos\varphi_2 - \mathbf{i}\sin\varphi_2) =$$

$$= \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + \mathbf{i}\sin(\varphi_1 - \varphi_2))\,. \quad \square$$

§4. Формула Муавра. Извлечение корня из комплексного числа

Формула Муавра: для любого $n \in \mathbb{N}$ справедливо равенство

$$(r(\cos\varphi + \mathbf{i}\sin\varphi))^n = r^n(\cos n\varphi + \mathbf{i}\sin n\varphi)\,.$$

Следствие. Для любого $n \in \mathbb{N}$ справедливо равенство

$$(\cos\varphi + \mathbf{i}\sin\varphi)^n = \left(\cos^n\varphi - C_n^2\cos^{n-2}\varphi\sin^2\varphi + \ldots\right) + \left(C_n^1\cos^{n-1}\varphi\sin\varphi + \ldots\right)\mathbf{i}.$$

Извлечение корня из комплексного числа.

Рассмотрим решения уравнения $x^n = z$, где $z = r(\cos\varphi + \mathbf{i}\sin\varphi)$.

Пусть $x = \rho(\cos\psi + \mathbf{i}\sin\psi)$ — решение, тогда $x^n = \rho^n(\cos n\psi + \mathbf{i}\sin n\psi)$. Следовательно,

$$\begin{cases} \rho^n = r \\ \cos n\psi = \cos\varphi \\ \sin n\psi = \sin\varphi \end{cases} \Leftrightarrow \begin{cases} \rho = \sqrt[n]{r} \\ n\psi = \varphi + 2\pi k,\ k \in \mathbb{Z}, \end{cases}$$

$$\psi = \frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2\pi t}{n} + 2\pi s,\ \text{где } k = ns + t,\ 0 \le t \le n-1,$$

$$\psi_1 = \frac{\varphi}{n}, \psi_2 = \frac{\varphi + 2\pi}{n}, \ldots, \psi_n = \frac{\varphi + 2\pi(n-1)}{n}.$$

Поэтому получаем n корней: $x_i = \sqrt[n]{r}(\cos\psi_i + \mathbf{i}\sin\psi_i)$, $i = 1, \ldots, n$.

Теорема 1. Уравнение $x^n = z$ имеет n решений — это вершины правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|z|}$ с центом в нуле, при этом $(1, 0)$ является вершиной. □

Числа $\varepsilon_k = \cos\frac{2\pi k}{n} + \mathbf{i}\sin\frac{2\pi k}{n}$, $k = 0, 1, \ldots, n-1$, решения уравнения $x^n = 1$, называют *корнями из единицы* степени n.

§5. Отношение эквивалентности и разбиение множества на классы

Любое подмножество $R \subseteq A \times B$ называется *отношением*, определенным на паре множеств A, B. Если $(a, b) \in R$, то пишут $a \underset{R}{\sim} b$ и говорят, что a находится в отношении R к элементу b. Отношение R на паре A, A называется *бинарным* отношением .

Пример. Равенство элементов в множестве $A = \{1, 2\}$ можно понимать как бинарное отношение $R = \{(1, 1), (2, 2)\} \subseteq A \times A$.

Бинарное отношение R на A называется *отношением эквивалентности*, или просто эквивалентностью на A, если для любых $x, y, z \in A$ справедливо

1) $x \underset{R}{\sim} x$ — рефлексивность;

2) $x \underset{R}{\sim} y \Rightarrow y \underset{R}{\sim} x$ — симметричность;

3) $x \underset{R}{\sim} y,\ \ y \underset{R}{\sim} z \Rightarrow x \underset{R}{\sim} z$ — транзитивность.

Пример. Пусть $\mathbb{Z}$ — множество целых чисел. Скажем, что $a \sim b$, если $(a - b)$ делится на 2. Свойства 1) и 2) очевидны. Проверим 3): $a \sim b$, $b \sim c \Leftrightarrow$

$a-b=2k$, $b-c=2\ell$, где $k,\ell\in\mathbb{Z}$. Тогда $(a-b)+(b-c)=a-c=2(k+\ell)$ и $a\sim c$.

Множество $S=\{B_\alpha : B_\alpha\subseteq A, \alpha\in I\}$ называется *разбиением A на классы*, если $B_\alpha\neq\varnothing$ для любого $\alpha\in I$ и для любого $a\in A$ существует единственное B_α такое, что $a\in B_\alpha$. Очевидно, что при этом $A=\bigcup\limits_{\alpha\in I}B_\alpha$ и для любых $\alpha,\beta\in I$ таких, что $\alpha\neq\beta$ имеем равенство $B_\alpha\bigcap B_\beta=\varnothing$.

Теорема 1. 1) *Любое отношение эквивалентности R на A определяет разбиение A на классы.* 2) *Любое разбиение A на классы определяет на A отношение эквивалентности.*

Доказательство. 1) Определим $K_a=\{b\in A : b\underset{R}{\sim}a\}$ (далее $\underset{R}{\sim}:=\sim$). Заметим, что $K_a\neq\varnothing$ для любого $a\in A$: так как $a\sim a$, то $a\in K_a$. Пусть $K_a\cap K_b\neq\varnothing$, тогда существует $c\in K_a\cap K_b\Rightarrow c\sim a,\ \ b\sim c\Rightarrow a\sim b\Rightarrow a\in K_b$. Тогда для любого $x\in K_a$, если $x\sim a$, $a\sim b$, то $x\sim b$ и $x\in K_b$. Следовательно, $K_a\subseteq K_b$. Аналогично $K_b\subseteq K_a$ и $K_a=K_b$. Таким образом, для любых $a,b\in A$ либо $K_a\cap K_b=\varnothing$, либо $K_a=K_b$. Подмножества K_a будем называть смежными классами A по R. Пусть S — это множество всех различных смежных классов A по R. Очевидно, что S — разбиение A на классы.

2) Пусть $S=\{B_\alpha : B_\alpha\subseteq A, \alpha\in I\}$ — разбиение A на классы. Для любых $x,y\in A$ положим $x\sim y$ тогда и только тогда, когда существует $\alpha\in I$ такой, что $x,y\in B_\alpha$. Тогда $x\sim x$, так как существует $\alpha\in I$ такой, что $x\in B_\alpha$. Если $x\sim y$, то $y\sim x$ — очевидно. Если $x\sim y$ и $y\sim z$, то $x,y\in B_\alpha,\ y,z\in B_\beta$; следовательно, $\alpha=\beta,\ x,y,z\in B_\alpha$. Поэтому $x\sim z$. □

§6. Эквивалентность систем линейных уравнений при элементарных преобразованиях

Пусть F — некоторое поле. Система линейных уравнений (с.л.у.):

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n=b_1,\\ ----------\\ a_{m1}x_1+\ldots+a_{mn}x_n=b_m, \end{cases} \tag{1}$$

где a_{ij} — *коэффициенты системы*, b_i — *свободные члены системы*, x_j — *неизвестные*, $a_{ij},b_i\in F$, $i=1,\ldots,m$, $j=1,\ldots,n$. Символ $m\times(n+1)$ означает размерность системы. С.л.у. называется *однородной*, если $b_1=\ldots=$

$b_m = 0$. Однородная с.л.у.

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ - - - - - - - - - - - \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0, \end{cases}$$

называется *приведённой* системой для с.л.у. (1).

Набор $(y_1, \ldots, y_n) \in F^n$ называется *решением* системы (1), если при замене неизвестных x_i на числа y_i, $i = 1, \ldots, n$, каждое из уравнений системы (1) обращается в равенство.

Обозначим через $S \subseteq F^n$ множество решений с.л.у. (1), т. е. $S = \{(y_1, \ldots, y_n) : (y_1, \ldots, y_n) —$ решение с.л.у. (1)$\}$. Тогда система называется: *несовместной*, если $S = \varnothing$; *совместной*, если $S \neq \varnothing$; *определенной*, если S состоит из одного элемента; и *неопределенной*, если S содержит более одного элемента.

Примеры.

- $\begin{cases} x_1 + x_2 = 2 \\ 2x_1 + 2x_2 = -1 \end{cases}$ - – –;
- $x_1 + x_2 = 2$ — неопределенная система;
- $x_1 = 1$ — определенная система.

Наша цель — найти необходимые и достаточные условия совместности произвольной системы (1), и если система (1) совместна, то найти все ее решения.

Рассмотрим еще одну с.л.у.

$$\begin{cases} c_{11}x_1 + \ldots + c_{1n}x_n = d_1, \\ - - - - - - - - - - - \\ c_{m1}x_1 + \ldots + c_{mn}x_n = d_m. \end{cases} \tag{2}$$

Системы (1) и (2) называются *эквивалентными*, если либо они обе несовместны, либо совместны и обладают одними и теми же решениями. Эквивалентность систем (1) и (2) будем обозначать символом (1) $\approx$ (2). Таким образом, если S_i — множество решений системы (i), $i = 1, 2$, то (1) $\approx$ (2) тогда и только тогда, когда $S_1 = S_2$. Заметим, что введенное отношение на с.л.у. размерности $m \times (n + 1)$ является отношением эквивалентности. Действительно, очевидно, что (1) $\approx$ (1) и (1) $\approx$ (2) $\Rightarrow$ (2) $\approx$ (1).

Теперь если (1) $\approx$ (2), (2) $\approx$ (3) $\Rightarrow S_1 = S_2, S_2 = S_3 \Rightarrow S_1 = S_3 \Rightarrow$ (1) $\approx$ (3). Таким образом, по теореме 1 §5 множество с.л.у. разбивается на классы эквивалентности.

Будем говорить, что система (2) получена из системы (1) при помощи: *элементарного преобразования I типа*, если система (2) получена из (1) перестановкой i-го и j-го уравнений ($i \neq j$); *элементарного преобразования II типа*, если система (2) получена из (1) добавлением к i-уравнению j-уравнения ($i \neq j$), умноженного на некоторое $\alpha \in F$, т. е. i-ое уравнение системы (2) имеет вид

$$(a_{i1} + \alpha a_{j1})\, x_1 + \ldots + (a_{in} + \alpha a_{jn})\, x_n = b_i + \alpha b_j, \tag{3}$$

а остальные уравнения системы (2) совпадают с уравнениями системы (1).

Будем обозначать соответственно: $(1) \underset{I}{\rightsquigarrow} (2)$, $(1) \underset{II}{\rightsquigarrow} (2)$. Элементарные преобразования I или II типа будем называть элементарными преобразованиями с.л.у. и обозначать $(1) \rightsquigarrow (2)$.

Лемма 1. *Имеют место следующие утверждения*:
1) $(1) \rightsquigarrow (2) \Rightarrow (2) \rightsquigarrow (1)$;
2) $(1) \rightsquigarrow (2) \Rightarrow (1) \approx (2)$.

Доказательство. 1) Если $(1) \underset{I}{\rightsquigarrow} (2)$, то, очевидно, меняя обратно i-ое и j-ое уравнения с.л.у. (2), получим (1), т. е. $(2) \underset{I}{\rightsquigarrow} (1)$. Если $(1) \underset{II}{\rightsquigarrow} (2)$ по формуле (3), то добавляя к i-му уравнению (2) j-ое уравнение (2), умноженное на $(-\alpha)$, получим i-ое уравнение (1), т. е. $(2) \underset{II}{\rightsquigarrow} (1)$.

2) Если $(1) \underset{I}{\rightsquigarrow} (2)$, то уравнения системы не изменились, следовательно $(1) \approx (2)$.

Рассмотрим $(1) \underset{II}{\rightsquigarrow} (2)$ по формуле (3). Пусть $S_1 \neq \varnothing$ и $(y_1, \ldots, y_n) \in S_1$ — произвольное решение системы (1). Тогда $(a_{i1} + \alpha a_{j1})\, y_1 + \ldots + (a_{in} + \alpha a_{jn})\, y_n = (a_{i1}y_1 + \ldots + a_{in}y_n) + \alpha\,(a_{j1}y_1 + \ldots + a_{jn}y_n) = b_i + \alpha b_j$. Следовательно, $(y_1, \ldots, y_n) \in S_2$, и система (2) совместна. В силу доказанного, $S_1 \subseteq S_2$. Так как, $(2) \underset{II}{\rightsquigarrow} (1)$, то $S_2 \subseteq S_1 \Rightarrow S_1 = S_2$.

Пусть $S_1 = \varnothing$. Так как $(2) \underset{II}{\rightsquigarrow} (1)$, то $S_2 = \varnothing$ и опять $S_1 = S_2$. Поэтому $(1) \approx (2)$. □

Теорема 1. *Если с.л.у.* (2) *получена из* (1) *путем применения конечной последовательности элементарных преобразований, то* $(1) \approx (2)$.

Доказательство. Пусть $(1) \rightsquigarrow (a_1) \rightsquigarrow \ldots \rightsquigarrow (a_{n-1}) \rightsquigarrow (2)$. Докажем, что $(1) \approx (2)$ индукцией по n — числу преобразований. Базис индукции при $n = 1$ следует из леммы 1. Предположим, что для $(n-1)$ преобразований утверждение истинно. Тогда по лемме 1, $(1) \approx (a_1)$. По предположению индукции $(a_1) \approx (2)$. Следовательно, $(1) \approx (2)$. □

§7. Приведение к ступенчатому виду методом Гаусса

Таблица $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$, где $a_{ij} \in F$, $i = 1, \dots, m$, $j = 1, \dots, n$, называется *матрицей* размера $m \times n$ над F. Пусть $B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$. Матрицы A и B называются равными, если они совпадают поэлементно, т. е. $A = B \Leftrightarrow a_{ij} = b_{ij}$ для всех $1 \le i \le m$, $1 \le j \le n$. Матрица состоящая из одних нулей называется нулевой и обозначается также через 0. Множество всех матриц размера $m \times n$ над F обозначается через $M_{m,n}(F)$, т. е.

$$M_{m,n}(F) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} : a_{ij} \in F \right\}.$$

Матрица $A_i = (a_{i1} \dots a_{in}) \in M_{1,n}(F)$, $1 \le i \le m$, называется *i-ой строкой* (*i-строкой*) матрицы A.

Матрица $A^{(j)} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in M_{m,1}(F)$ называется j-столбцом матрицы A.

Матрицу A можно формально записать через строки или столбцы:

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} = \begin{pmatrix} A^{(1)} & \dots & A^{(n)} \end{pmatrix}.$$

Определим элементарные преобразования строк матрицы.

Элементарные преобразования (*строк*) *I типа*:

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \underset{I}{\rightsquigarrow} B = \begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_m \end{pmatrix}, \quad \text{где} \quad i \neq j,$$

т. е. матрица B получена из матрицы A перестановкой i и j строки.

Элементарные преобразования строк II типа:

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix} \underset{II}{\rightsquigarrow} B = \begin{pmatrix} A_1 \\ \vdots \\ A_i + \alpha A_j \\ \vdots \\ A_j \\ \vdots \\ A_m \end{pmatrix}, \quad \text{где } i \neq j, \quad \alpha \in F,$$

и $A_i + \alpha A_j = ((a_{i1} + \alpha a_{j1}) \dots (a_{in} + \alpha a_{jn}))$. Говорят, что матрица B получена из матрицы A добавлением к i-строке j-строки, умноженной на $\alpha \in F$.

Элементарные преобразования I и II типа будем называть просто элементарными преобразованиями строк матрицы A и записывать $A \rightsquigarrow B$.

Матрица

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_{1k_1} & \cdots & \cdots & \cdots & \cdots & a_{1n} \\ 0 & \cdots & 0 & \cdots & a_{2k_2} & \cdots & \cdots & \cdots & a_{1n} \\ \vdots & & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & 0 & \cdots & \cdots & 0 & a_{rk_r} & \cdots & a_{rn} \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix},$$

где $a_{1k_1}, \dots, a_{rk_r} \neq 0$, $1 \leq k_1 < \dots < k_r \leq n$, $1 \leq r \leq m$, называется матрицей *ступенчатого вида* (*ступенчатой матрицей*).

Лемма 1. *Пусть $A \in M_{m,n}(F)$ и $A \neq 0$. Тогда A элементарными преобразованиями приводится к ступенчатому виду.*

Доказательство. Индукция по m — числу строк матрицы A. При $m = 1$ ненулевая матрица уже является ступенчатой. Предположим, что утверждение верно для всех матриц из $M_{m-1,n}(F)$. Рассмотрим $A \in M_{m,n}(F)$. Так как $A \neq 0$, то существуют i, j, $1 \leq i \leq m$, $1 \leq j \leq n$, такие, что $a_{ij} \neq 0$. Выберем минимальное j и произвольное i с этим свойством. Переставим 1-ю и i-ю строки матрицы A. Получим матрицу

$$B = \begin{pmatrix} 0 & \cdots & 0 & b_{1j} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{mj} & \cdots & b_{mn} \end{pmatrix}, \quad \text{где} \quad b_{1j} \neq 0.$$

К каждой i-строке матрицы B, $i = 2, \ldots, m$, добавим 1-ю строку матрицы B, умноженную на $\alpha = -\frac{b_{ij}}{b_{1j}}$. Получим матрицу

$$C = \begin{pmatrix} B_1 & \\ B_2 & -\left(\frac{b_{2j}}{b_{1j}}\right) B_1 \\ \vdots & \\ B_m & -\left(\frac{b_{mj}}{b_{1j}}\right) B_1 \end{pmatrix} = \left(\begin{array}{cccc|ccc} 0 & \cdots & 0 & c_{1j} & \cdots & \cdots & c_{1n} \\ 0 & \cdots & 0 & 0 & c_{2j+1} & \cdots & c_{2n} \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & \cdots \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & c_{mj+1} & \cdots & c_{mn} \end{array}\right),$$

где $c_{1j} = b_{1j} \neq 0$. Рассмотрим матрицу

$$\overline{C} = \begin{pmatrix} c_{2j+1} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots \\ c_{mj+1} & \cdots & c_{mn} \end{pmatrix} \in M_{m-1,n-j}(F)$$

(можно считать, что $\overline{C} \in M_{m-1,n}$). По предположению индукции, матрица $\overline{C}$ элементарными преобразованиями приводится к ступенчатой матрице $\overline{D}$. Совершим те же элементарные преобразования со строками $C_2, \ldots, C_m$ матрицы C и получим ступенчатую матрицу

$$D = \left(\begin{array}{cccc|ccc} 0 & \cdots & 0 & b_{1j} & \cdots & \cdots & b_{1n} \\ 0 & \cdots & 0 & 0 & & & \\ & & & & & \bar{D} & \\ 0 & & 0 & 0 & & & \end{array}\right).$$

□

Рассмотрим с.л.у.

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ - - - - - - - - - - \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{1}$$

Матрица $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(F)$ называется *матрицей* с.л.у. (1), матрица $\overline{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix} \in M_{m,n+1}(F)$ называется *расширенной матрицей* системы (1). Расширенную матрицу $\overline{A}$ формально записывают в

виде $\overline{A} = (A|B)$, где $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(F)$ — столбец свободных членов с.л.у. (1).

Таким образом, мы устанавливаем взаимно однозначное соответствие между с.л.у. размерности $m \times (n+1)$ и множеством матриц $M_{m,n+1}(F)$. Нетрудно заметить, что элементарным преобразованиям с.л.у. однозначно соответствуют элементарные преобразования матриц и наоборот.

С.л.у. (1) называется системой *ступенчатого вида*, если расширенная матрица $\overline{A}$ системы (1) является ступенчатой.

Теорема 1. *Всякая с.л.у.* (1) *эквивалентна с.л.у. ступенчатого вида.*

Доказательство. В силу леммы 1, приведем расширенную матрицу $\overline{A}$ системы элементарными преобразованиями к ступенчатому виду. Совершая те же элементарные преобразования с системой, приведем ее к системе ступенчатого вида. По теореме 1 §6, полученная ступенчатая система эквивалентна (1). □

§8. Исследование систем линейных уравнений. Необходимые и достаточные условия совместности и определенности

Исследуем с.л.у.

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ - - - - - - - - - - - - \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{1}$$

Если расширенная матрица системы $\overline{A}$ нулевая, то, очевидно, система совместна и имеет бесконечное множество решений $S = F^n$. Пусть $\overline{A} \neq 0$. Приведем ее элементарными преобразованиями к системе ступенчатого вида:

$$\begin{cases} c_{1k_1}x_{k_1} + \ldots\ldots + c_{1n}x_n = d_1, \\ - - - - - - - - - - - - \\ c_{rk_r}x_{k_r} + \ldots + c_{rn}x_n = d_r, \\ 0 = d_{r+1}, \\ 0 = 0, \\ \vdots \\ 0 = 0, \end{cases} \tag{2}$$

где $c_{1k_1}, \ldots, c_{rk_r} \neq 0$, $1 \leq k_1 < \ldots < k_r \leq n$. В силу теоремы 1 §7, (1) $\approx$ (2). Поэтому для исследования системы (1) достаточно исследовать систему (2).

1) *Несовместность.* Если в системе (2) $d_{r+1} \neq 0$, то система (2) несовместна. Так как уравнению $0 \cdot x_1 + \ldots + 0 \cdot x_n = d_{r+1} \neq 0$ не удовлетворяет никакой набор $(y_1, \ldots, y_n) \in F^n$.

2) *Совместность.* Пусть $d_{r+1} = 0$. Докажем, что система (2) совместна. Имеем

$$\left\{\begin{array}{l} c_{1k_1}x_{k_1} + \ldots + c_{1n}x_n = d_1, \quad c_{1k_1} \neq 0, \\ - \\ c_{rk_r}x_{k_r} + \ldots + c_{rn}x_n = d_r, \quad c_{rk_r} \neq 0, \end{array}\right. \tag{3}$$

где $1 \leq k_1 < \ldots < k_r \leq n$, $1 \leq r \leq n$.

Переменные $x_{k_1}, \ldots, x_{k_r}$ назовем *главными*, все остальные переменные — *свободными*. Заметим, что по определению мы имеем r главных переменных и $(n - r)$ свободных переменных.

Введем обозначения для линейных комбинаций свободных переменных, входящих в каждое уравнение (3):

$$\left\{\begin{array}{l} \ell_1 = \ell_1(x_1, \ldots, \widehat{x}_{k_1}, \ldots, \widehat{x}_{k_r}, \ldots, x_n) = \sum\limits_{i \neq k_1, \ldots, k_r} c_{1i}x_i, \\ - \\ \ell_r = \ell_r(x_1, \ldots, \widehat{x}_{k_1}, \ldots, \widehat{x}_{k_r}, \ldots, x_n) = \sum\limits_{i \neq k_1, \ldots, k_r} c_{ri}x_i \end{array}\right.$$

(здесь и всюду далее символ $\widehat{X}$ означает отсутствие выражения X). Тогда

$$\left\{\begin{array}{l} x_{k_1} = \frac{1}{c_{1k_1}} \left(d_1 - \ell_1 - \sum\limits_{i=2}^{r} c_{1k_i}x_{k_i} \right), \\ - - - - - - - - - - - - - - - - - - \\ x_{k_{r-1}} = \frac{1}{c_{r-1k_{r-1}}} \left(d_{r-1} - \ell_{r-1} - c_{rk_r}x_{k_r} \right), \\ x_{k_r} = \frac{1}{c_{rk_r}} \left(d_r - \ell_r \right). \end{array}\right. \tag{4}$$

Придадим свободным переменным произвольные значения из F и подставим их в (4). Тогда из последнего уравнения однозначно найдем x_{k_r}, подставим это значение в $(r-1)$-ое уравнение и однозначно найдем $x_{k_{r-1}}$. Продолжая так далее, подставим найденные значения в первое уравнение и однозначно найдем x_1. Следовательно, система (2) (а потому и (1)) совместна. Найденные решения из (4) называются общим решением системы (1).

с) *Определенность.* Если система (3) содержит хотя бы одну свободную переменную, то она, очевидно, является неопределенной, т. е. если $r < n$, то система (3), а, следовательно, (2) и (1) являются неопределенными. Пусть

система (3) не содержит свободных переменных, т. е. $r = n$. Тогда в системе (4) n уравнений и отсутствуют $\ell_1, \ldots, \ell_r$. Поэтому $x_1, \ldots, x_n$ определяются однозначно.

Таким образом, доказана теорема:

Теорема 1. *С.л.у.* (1) *с ненулевой расширенной матрицей является*:

1) *совместной тогда и только тогда, когда в ступенчатой системе* (2) $d_{r+1} = 0$. *В этом случае свободным переменным можно придать произвольные значения, а главные переменные при этих условиях определяются однозначно*;

2) *определенной тогда и только тогда, когда в ступенчатой системе* (2) $r = n$.

Пример. Исследовать с.л.у. методом Гаусса:

$$\begin{cases} 2x_1 + x_2 = 0, \\ x_1 + 2x_2 + x_3 = 0, \\ x_2 + 2x_3 = 4. \end{cases}$$

Решение. Приведем расширенную матрицу системы к ступенчатому виду:

$$\left(\begin{array}{ccc|c} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 4 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 2 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & 1 & 0 \\ 0 & 1 & 2 & 4 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 2 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & 1 & 0 \\ 0 & 0 & \frac{4}{3} & 4 \end{array}\right).$$

Поэтому система является определенной и $x_3 = 3,\ x_2 = -2,\ x_1 = 1$.

§9. Векторные пространства: определение и примеры. Пространство решений однородной системы линейных уравнений

Произвольное множество элементов $V \neq \varnothing$ называется *векторным* (или линейным) пространством над полем F, если на V задана ассоциативная коммутативная бинарная операция *сложения* и, для любого $\alpha \in F$, унарная операция *умножения на скаляр*, удовлетворяющие следующим аксиомам:

1) существует *нулевой элемент* (*ноль*) $0 \in V$ такой, что $a + 0 = 0 + a = a$ для любого $a \in V$; для любого $a \in V$ существует $b \in V$такой, что $a + b = b + a = 0$;

2) для любых $\alpha, \beta \in F,\ a, b \in V$ выполняется:

а) $(\alpha\beta)\, a = \alpha\, (\beta a)$ (ассоциативность умножения на скаляр);

б) $(\alpha+\beta)\,a=\alpha a+\beta a$, $\alpha\,(a+b)=\alpha a+\alpha b$ (дистрибутивность);

в) $1a=a$, где $1\in F$.

Элементы пространства V называются *векторами*, элементы из F называются *скалярами*.

Простейшие свойства операций векторного пространства:

1) В V существует только один нулевой элемент.

$\Diamond$ Пусть 0_1 и 0_2 — два нулевых элемента из V, тогда: $0_1+0_2=0_1=0_2$. $\square$

2) $(\forall x\in V\ \ \exists!\ y\in V)\ x+y=y+x=0$.

$\Diamond$ Пусть $x+y_1=x+y_2=0$. Тогда $(x+y_1)+y_2=0+y_2=y_2=x+(y_1+y_2)=x+(y_2+y_1)=(x+y_2)+y_1=0+y_1=y_1$. $\square$

3) $0a=0$, где $0\in F$, $a\in V$.

$\Diamond$ $(1+0)a=1a=a=1a+0a=a+0a\Rightarrow 0=0a$. $\square$

4) $(\forall\alpha\in F)\ \alpha 0=0$, где $0\in V$.

$\Diamond$ $\alpha 0=\alpha(0+0)=\alpha 0+\alpha 0\Rightarrow 0=\alpha 0$. $\square$

5) $(\forall\,\alpha\in F,\ \ \forall\,a\in V)\ \ \alpha a=0\Rightarrow\alpha=0$ или $a=0$.

$\Diamond$ Если $\alpha\neq 0$, то $\alpha^{-1}(\alpha a)=(\alpha^{-1}\alpha)a=1a=a=\alpha^{-1}0=0$. $\square$

6) $(\forall a,b\in V)\ -(-a)=a$, $-(a+b)=-a-b$.

$\Diamond$ Доказательство очевидно. $\square$

7) $(\forall\alpha\in F,\ \forall a\in V)\ -(\alpha a)=(-\alpha)a$.

$\Diamond$ $\alpha a+(-\alpha)a=(\alpha+(-\alpha))a=0a=0\Rightarrow\alpha a=-(-\alpha a)$. $\square$

Примеры векторных пространств.

1) E_3 — множество векторов 3-х мерного пространства над $\mathbb{R}$ с началом в точке 0 относительно операций векторного сложения и умножения на скаляр.

2) *Пространство строк*:

Множество $F_n=\{X=(x_1,\ldots,x_n):x_1,\ldots,x_n\in F\}$ с операциями:

$$\begin{cases} X+Y=(x_1,\ldots,x_n)+(y_1,\ldots,y_n)=(x_1+y_1,\ldots,x_n+y_n)\,, \\ \alpha X=\alpha\,(x_1,\ldots,x_n)=(\alpha x_1,\ldots,\alpha x_n)\,, \quad \text{где}\ \ \alpha\in F. \end{cases} \tag{1}$$

Докажем, что F_n с заданными операциями является линейным пространством.

Ноль: $0=(0,\ldots,0):0+X=X+0=0$ для любого $X\in F_n$.

Обратный: Для любого $X=(x_1,\ldots,x_n)$ существует $-X=(-x_1,\ldots,-x_n):X+(-X)=(-X)+X=0$.

Дистрибутивность: $\alpha\,(X+Y)=\alpha\,(x_1+y_1,\ldots,x_n+y_n)=(\alpha x_1+\alpha y_1,\ldots,\alpha x_n+\alpha y_n)=(\alpha x_1,\ldots,\alpha x_n)+(\alpha y_1,\ldots,\alpha y_n)=\alpha X+\alpha Y$.

$(\alpha+\beta)\,X = ((\alpha+\beta)\,x_1,\ldots,(\alpha+\beta)\,x_n) = (\alpha x_1+\beta x_1,\ldots,\alpha x_n+\beta x_n) = (\alpha x_1,\ldots,\alpha x_n)+(\beta x_1,\ldots,\beta x_n) = \alpha X+\beta X.$

Остальные аксиомы проверяются аналогично.

Аналогично определяется и F^n — линейное пространство столбцов.

3) *Пространство решений* однородной системы линейных уравнений.

Рассмотрим однородную систему линейных уравнений

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n=0, \\ ----------- \\ a_{m1}x_1+\ldots+a_{mn}x_n=0. \end{cases} \tag{2}$$

Обозначим $V_s = \{(\lambda_1,\ldots,\lambda_n) : (\lambda_1,\ldots,\lambda_n) - \text{решение (2)}\}$.

Определим на V_s операции по правилу (1). Проверим все аксиомы: $V_s \neq \varnothing$, так как $0=(0,\ldots,0)\in V_s$. Покажем, что операции на V_s, заданные правилом (1), определены корректно.

Пусть $X=(x_1,\ldots,x_n)$, $Y=(y_1,\ldots,y_n)\in V_s$, т. е. при подстановке X и Y в (2) уравнения обращаются в тождества. Тогда, для $i=1,\ldots,m$, имеем

$$0=\sum_{k=1}^{n}a_{ik}x_k+\sum_{k=1}^{n}a_{ik}y_k=\sum_{k=1}^{n}a_{ik}(x_k+y_k), \text{ т. е. } X+Y\in V_s.$$

Для любого $\alpha\in F$ имеем $0=\alpha\sum\limits_{k=1}^{n}a_{ik}x_k=\sum\limits_{k=1}^{n}\alpha a_{ik}x_k=\sum\limits_{k=1}^{n}a_{ik}(\alpha x_k)$, т. е. $\alpha X\in V_s$.

Так как по определению $V_s\subseteq F_n$ и операции на V_s определены также как и на F_n, то и остальные аксиомы выполнены. Таким образом, множество решений однородной системы линейных уравнений V_s является линейным пространством.

§10. Подпространство, линейная зависимость

Пусть V — векторное пространство над F и $a_1,\ldots,a_n\in V$. Множество $L(a_1,\ldots,a_n)=\{\alpha_1a_1+\ldots+\alpha_na_n : \alpha_i\in F\}$ называется *линейной оболочкой* системы векторов $a_1,\ldots,a_n$. Непустое подмножество U векторного пространства V называется *подпространством* в V, если U — векторное пространство над F с теми же операциями, что определены в V.

Лемма 1. *U — подпространство в $V\Leftrightarrow \alpha a+\beta b\in U$ для всех $\alpha,\beta\in F$, $a,b\in U$.*

Доказательство. Необходимость очевидна. Обратно, положим $\alpha = \beta = 1$. Тогда $a + b \in U$ для любых $a, b \in U$. Далее, положим $\beta = 0$. Тогда $\alpha a \in U$ для любых $\alpha \in F$, $a \in U$. Остальные аксиомы выполнены в силу того, что V — векторное пространство. □

Следствие. *$L = L(a_1, \ldots, a_n)$ — подпространство в V.*

Доказательство. Заметим, что $L \neq \varnothing$. Далее, для любых $\alpha, \beta \in F$ и $a = \sum\limits_{i=1}^{n} \alpha_i a_i$, $b = \sum\limits_{i=1}^{n} \beta_i a_i \in L$ имеем: $\alpha a + \beta b = \sum\limits_{i=1}^{n} (\alpha\alpha_i + \beta\beta_i) a_i \in L$. □

Векторы $a_1, \ldots, a_n \in U$ называются *линейно зависимыми*, если существуют такие $\alpha_1, \ldots, \alpha_n \in F$, одновременно не равные нулю, что $\sum\limits_{i=1}^{n} \alpha_i a_i = 0$. Векторы $a_1, \ldots, a_n \in U$ *линейно независимы*, если из равенства $\sum\limits_{i=1}^{n} \alpha_i a_i = 0$ следует, что $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

Примеры. 1) $\ell_1 = (1, 0, \ldots, 0), \ldots, \ell_n = (0, 0, \ldots, 1)$ линейно независимы в F_n.

2) векторы a и $2a$ линейно зависимы для любого $a \in V$.

Теорема 1. 1) *Если некоторая подсистема векторов $a_1, \ldots, a_n$ линейно зависима, то векторы $a_1, \ldots, a_n$ линейно зависимы.*

2) *Если $a_1, \ldots, a_n$ линейно независимы, то любая их подсистема линейно независима.*

3) *Если $a_1, \ldots, a_n$ линейно зависимы, то существует i такой, что $a_i \in L(a_1, \ldots \hat{a}_i \ldots, a_n)$.*

4) *Если $a_i \in L(a_1, \ldots \hat{a}_i \ldots, a_n)$, то $a_1, \ldots, a_n$ линейно зависимы.*

5) *Если $a_1, \ldots, a_n$ линейно независимы, но $a_1, \ldots, a_n$, a линейно зависимы, то $a \in L(a_1, \ldots, a_n)$.*

6) *Если $a_1, \ldots, a_n$ линейно независимы и $a \notin L(a_1, \ldots, a_n)$, то $a_1, \ldots, a_n$, a линейно независимы.*

Доказательство. 1) Пусть $\alpha_{i_1} a_{i_1} + \ldots + \alpha_{i_s} a_{i_s} = 0$, где $1 \leq i_1 < \ldots < i_s \leq n$ и $\alpha_{i_1}, \ldots, \alpha_{i_s}$ одновременно не равны нулю. Тогда $\sum\limits_{i=1}^{n} \beta_i a_i = 0$, где $\beta_k = \begin{cases} 0, & k \notin \{i_1, \ldots, i_s\} \\ \alpha_k, & k \in \{i_1, \ldots, i_s\} \end{cases}$ и все β_i одновременно не равны нулю.

2) Следует из 1).

3) Если $\sum\limits_{i=1}^{n} \alpha_i a_i = 0$, то существует $\alpha_k \neq 0$ такое, что $a_k = -\frac{\alpha_1}{\alpha_k} a_1 - \ldots - \widehat{a_k} - \ldots - \frac{\alpha_n}{\alpha_k} a_n$.

4) Если $a_i = \beta_1 a_1 + \ldots + \widehat{\beta_i a_i} + \ldots + \beta_n a_n$, то $\beta_1 a_1 + \ldots + (-1) a_i + \ldots + \beta_n a_n = 0$.

5) Существуют такие $\alpha_1, \ldots, \alpha_n, \alpha \in F$, одновременно не равные нулю, что $\sum\limits_{i=1}^{n} \alpha_i a_i + \alpha a = 0$. Поэтому $\alpha \neq 0$ и $a = -\frac{1}{\alpha} \sum\limits_{i=1}^{n} \alpha_i a_i$.

6) Следует из 5). □

§11. Базис и размерность векторного пространства: существование и свойства. Координаты вектора

Пусть V — векторное пространство над F. Пространство V называется *конечномерным*, если существуют $a_1, \ldots, a_n \in V$ такие, что $V = L(a_1, \ldots, a_n)$. Набор векторов $a_1, \ldots, a_n$ называется *базисом* пространства V, если $a_1, \ldots, a_n$ линейно независимы и $V = L(a_1, \ldots, a_n)$.

Предложение 1. *a) Пусть $V = L(a_1, \ldots, a_n)$. Тогда для любого $x \in V$ существуют $\alpha_1, \ldots, \alpha_n \in F$ такие, что $x = \sum\limits_{i=1}^{n} \alpha_i a_i$. b) Если $a_1, \ldots, a_n$ — базис V, то для любого $x \in V$ существуют единственные $\alpha_1, \ldots, \alpha_n \in F$ такие, что $x = \sum\limits_{i=1}^{n} \alpha_i a_i$.*

Доказательство. a) Очевидно. *b)* Пусть $x = \sum\limits_{i=1}^{n} \alpha_i a_i = \sum\limits_{i=1}^{n} \beta_i a_i$. Тогда $\sum\limits_{i=1}^{n} (\alpha_i - \beta_i) a_i = 0$. Следовательно, для любого $1 \leq i \leq n$, $\alpha_i - \beta_i = 0$ и $\alpha_i = \beta_i$. □

Примеры. 1. $\ell_1, \ldots, \ell_n$ — (*стандартный*) базис F_n.

2. Пусть $a_i = \sum\limits_{k=1}^{i} \ell_k$, где $1 \leq i \leq n$. Тогда $a_1, \ldots, a_n$ — базис F_n.

Существование и единственность базиса конечномерного пространства.

Лемма 1. *С.л.у.* $\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ - - - - - - - - - - - - \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases}$ *при $m < n$ имеет ненулевое решение.*

Доказательство. Система совместна, так как имеет нулевое решение. Приведем ее к ступенчатому виду методом Гаусса. По теореме 1 §8 получим,

что система примет вид

$$\begin{cases} b_{1k}x_k + \ldots + b_{1n}x_n = 0 \\ \ldots \quad \ldots \quad \ldots \\ b_{rs}x_s + \ldots + b_{rn}x_n = 0 \\ 0 = 0 \\ \vdots \\ 0 = 0, \end{cases}$$

где $1 \le k < \ell < \ldots < s \le n, r \le m$ и $b_{1k}, \ldots, b_{rs} \ne 0$. Число свободных переменных равно $(n-r) \ge (n-m) > 0$, т. е. существует ненулевое решение. □

Лемма 2. *Пусть $V = L(a_1, \ldots, a_n)$ и векторы $b_1, \ldots, b_m \in V$ линейно независимы. Тогда $m \le n$.*

Доказательство. Пусть $b_1 = \sum\limits_{i=1}^{n} \alpha_{1i}a_i, \ldots, b_m = \sum\limits_{i=1}^{n} \alpha_{mi}a_i$, где $\alpha_{ij} \in F$ и $m > n$. Рассмотрим линейную комбинацию $\sum\limits_{i=1}^{m} x_i b_i$, где $x_i \in F$. Имеем

$$\sum_{i=1}^{m} x_i b_i = \sum_{i=1}^{m}(x_i \sum_{j=1}^{n} \alpha_{ij}a_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}x_i a_j = \sum_{j=1}^{n}(\sum_{i=1}^{m} \alpha_{ij}x_i)a_j.$$

Рассмотрим с.л.у. $\begin{cases} \sum\limits_{i=1}^{m} \alpha_{ij}x_i = 0, \quad 1 \le j \le n. \end{cases}$ Так как число уравнений меньше числа неизвестных, то по лемме 1 система имеет ненулевое решение $(x_1, \ldots, x_n) \in F_n$, т. е. $\sum\limits_{i=1}^{m} x_i b_i = 0$. Противоречие и $m \le n$. □

Теорема 1. *Каждое ненулевое конечномерное пространство $V = L(a_1, \ldots, a_n)$ обладает конечным базисом. Все базисы V состоят из одинакового числа $r \le n$ векторов (это число называется размерностью пространства V над F и обозначается $\dim_F V = r$).*

Доказательство. Существование. Так как $V \ne 0$, то существует ненулевой $x_1 \in V$. Если $V = L(x_1)$, то x_1 — базис; если $V \ne L(x_1)$, то существует $x_2 \in V$, $x_2 \notin L(x_1)$. По теореме 1 §10, x_1, x_2 линейно независимы. Если $V = L(x_1, x_2)$, то x_1, x_2 — базис. Если $V \ne L(x_1, x_2)$, то продолжаем процесс. По лемме 2 число линейно независимых векторов $\le n$, поэтому через r шагов, где $r \le n$, получим: $x_1, \ldots, x_r$ линейно независимы и $x_{r+1} \in L(x_1, \ldots, x_r)$ для любого $x_{r+1} \in V$. Следовательно, $V = L(x_1, \ldots, x_r)$ и $x_1, \ldots, x_r$ — базис V.

Единственность. Пусть $V = L(x_1, \ldots, x_r) = L(y_1, \ldots, y_s)$, где $x_1, \ldots, x_r$ линейно независимы и $y_1, \ldots, y_s$ линейно независимы. По лемме 2, $r \leq s$ и $s \leq r$, т. е. $r = s$. $\square$

Если $a_1, \ldots, a_n$ — базис V, то для любого $x \in V$ существуют единственные $\alpha_1, \ldots, \alpha_n \in F$ такие, что $x = \sum\limits_{i=1}^{n} \alpha_i a_i$. Строка $[x]_{a_1,\ldots,a_n} = (\alpha_1, \ldots, \alpha_n) \in F_n$ называется *координатами вектора* x в базисе $a_1, \ldots, a_n$.

§12. Изоморфизм векторных пространств одной размерности

Пусть A, B — множества, $\varphi : A \to B$ — отображение. *Образом* отображения φ называется множество $Im\ (\varphi) = \{\varphi(a) : a \in A\} \subseteq B$. Отображение φ — *сюръективное* (отображение на), если $Im\ (\varphi) = B$, т. е. для любого $b \in B$ существует $a \in A$ такой, что $\varphi(a) = b$; φ — *инъективное* (*отображение в*; *вложение*), если $\varphi(a_1) \neq \varphi(a_2)$ для любых $a_1, a_2 \in A$, $a_1 \neq a_2$; φ — *биективное* (взаимно однозначное), если φ — однозначное отображение на, т. е. φ — сюръективное и инъективное отображение.

Векторные пространства U и V называются *изоморфными*, если существует взаимно однозначное отображение $\varphi : U \mapsto V$ такое, что $\varphi(\alpha a + \beta b) = \alpha\varphi(a) + \beta\varphi(b)$ для любых $\alpha, \beta \in F$, $a, b \in U$. Отображение φ называется *изоморфизмом*. Обозначение: $U \approx V$.

Теорема 1. *Если* $\dim_F V = n$, *то* $V \approx F_n$.

Доказательство. Пусть $V = L(a_1, \ldots, a_n)$, где $a_1, \ldots, a_n$ — базис V. Пусть $x = \sum\limits_{i=1}^{n} \alpha_i a_i \in V$, где $\alpha_1, \ldots, \alpha_n \in F$. Построим $\varphi : V \to F_n$ по правилу: $\varphi(x) = [x]_{a_1,\ldots,a_n}$. Тогда для любого $(\alpha_1, \ldots, \alpha_n) \in F_n$ существует $x = \sum\limits_{i=1}^{n} \alpha_i a_i$ такой, что $\varphi(x) = (\alpha_1, \ldots, \alpha_n)$, т. е. φ — отображение на. Более того, если $x, y \in V$, $x \neq y$, то $[x]_{a_1,\ldots,a_n} \neq [y]_{a_1,\ldots,a_n}$. Следовательно, φ — это однозначное отображение и, в итоге, φ взаимно однозначное.

Для любых $\alpha, \beta \in F$, $x = \sum\limits_{i=1}^{n} \alpha_i a_i$, $y = \sum\limits_{i=1}^{n} \beta_i a_i \in V$ имеем

$$\varphi(\alpha x + \beta y) = \varphi(\sum_{i=1}^{n} (\alpha\alpha_i + \beta\beta_i) a_i) = (\alpha\alpha_1 + \beta\beta_1, \ldots, \alpha\alpha_n + \beta\beta_n) =$$

$$= \alpha(\alpha_1, \ldots, \alpha_n) + \beta(\beta_1, \ldots, \beta_n) = \alpha\varphi(x) + \beta\varphi(y). \qquad \square$$

§13. Базис подпространства векторного пространства

Лемма 1. *Пусть* $V = L(a_1, \ldots, a_n)$ *и* $a_{i_1}, \ldots, a_{i_r}$ *— любой максимальный набор линейно независимых векторов из системы* $a_1, \ldots, a_n$. *Тогда* $a_{i_1}, \ldots, a_{i_r}$ *— базис* V.

Доказательство. Если $r = n$, то $a_1, \ldots, a_n$ — базис V по определению. Пусть $r < n$. Для любого i, $1 \leq i \leq n$, векторы $a_{i_1}, \ldots, a_{i_r}$, a_i линейно зависимы. По теореме 1 §10, $a_i \in L(a_{i_1}, \ldots, a_{i_r})$. Следовательно, $V = L(a_1, \ldots, a_n) \subseteq L(a_{i_1}, \ldots, a_{i_r}) \subseteq L(a_1, \ldots, a_n) = V$. Поэтому $V = L(a_{i_1}, \ldots, a_{i_r})$ и $a_{i_1}, \ldots, a_{i_r}$ — базис V. □

Лемма 2. *Пусть* V *— векторное пространство размерности* n *над* F, $a_1, \ldots, a_r$ *линейно независимы в* V *и* $r < n$. *Тогда существуют такие* $a_{r+1}, \ldots, a_n \in V$, *что* $a_1, \ldots, a_n$ *— базис пространства* V.

Доказательство. Так как $r < n$, то $L(a_1, \ldots, a_r) \neq V$. Выберем произвольный $a_{r+1} \notin L(a_1, \ldots, a_n) \in V$. По теореме 1 §10, $a_1, \ldots, a_{r+1}$ линейно независимы. Если $L(a_1, \ldots, a_{r+1}) = V$, то $a_1, \ldots, a_{r+1}$ — базис V. Если нет, то повторяем процесс. За $(n - r)$ шагов найдем базис $a_1, \ldots, a_n$. □

Теорема 1 (*о размерности подпространства*). *Подпространство* U *конечномерного пространства* V *является конечномерным, т. е. для любого подпространства* U *пространства* $V = L(a_1, \ldots, a_n)$ *существует базис* $b_1, \ldots, b_r$, $U = L(b_1, \ldots, b_r)$ *и* $r \leq n$.

Доказательство. Если $U = 0$, то $U = L(0)$ — конечномерное пространство. Пусть $U \neq 0$. Рассмотрим $M = \{(b_1, \ldots, b_r) : r \in \mathbb{N}, b_1, \ldots, b_r \text{ линейно независимы}\}$. Тогда $M \neq \varnothing$: так как $U \neq 0$, то существует $a \in U$ такой, что $a \neq 0$. Следовательно, $(a) \in M$. Далее, $r \leq n$ в силу леммы 2 §11.

Выберем произвольный набор $(b_1, \ldots, b_r) \in M$, где r — максимальное число. Докажем, что $b_1, \ldots, b_r$ — базис U. По определению множества M, для любого $b \in U$ векторы $b_1, \ldots, b_r, b$ линейно зависимы. Тогда, по теореме 1 §9, $b \in L(b_1, \ldots, b_r)$. Следовательно, $U \subseteq L(b_1, \ldots, b_r) \subseteq U$. Поэтому $U = L(b_1, \ldots, b_r)$, $b_1, \ldots, b_r$ — базис U и $r \leq n$. □

Следствие. *Пусть* $U \leq V$ *и* $\dim U = \dim V$, *тогда* $U = V$.

Доказательство. Имеем $U \subseteq V$. Если $U \neq V$, то мы можем дополнить базис U до базиса V, но тогда $\dim U < \dim V$. □

Как практически искать базис U?

1) Если $U = 0$, то базиса нет и $U = L(0)$.

2) Если $U \neq 0$, то существует ненулевой $x_1 \in U$. Если $U = L(x_1)$, то x_1 — базис. Если $U \neq L(x_1)$, то существует $x_2 \in U$ такой, что $x_2 \notin L(x_1)$. Следовательно, по теореме 1 §11, x_1, x_2 линейно независимы. Повторим процедуру и за $r \leq n$ шагов получим $U = L(x_1, \ldots, x_r)$, где $x_1, \ldots, x_r$ — базис U.

§14. Сумма и пересечение подпространств, связь их размерностей

Пусть $U_1, \ldots, U_k$ — подпространства V. Тогда $\bigcap\limits_{i=1}^{k} U_i = U_1 \cap \ldots \cap U_k = \{a \in V : a \in U_1, \ldots, a \in U_k\}$ — *пересечение* $U_1, \ldots, U_k$; $\sum\limits_{i=1}^{k} U_i = U_1 + \ldots + U_k = \{a \in V : a = a_1 + \ldots + a_k : a_i \in U_i\}$ — *сумма* $U_1, \ldots, U_k$.

Лемма 1. $\bigcap\limits_{i=1}^{k} U_i$ *и* $\sum\limits_{i=1}^{k} U_i$ — *подпространства в* V.

Доказательство. Очевидно, что $0 \in \bigcap\limits_{i=1}^{k} U_i$, $0 \in \sum\limits_{i=1}^{k} U_i \Rightarrow \bigcap\limits_{i=1}^{k} U_i \neq \varnothing$, $\sum\limits_{i=1}^{k} U_i \neq \varnothing$.

Для любых $\alpha, \beta \in F$, $a, b \in \bigcap\limits_{i=1}^{k} U_i$ имеем $a, b \in U_1, \ldots, a, b \in U_k$. Тогда, по лемме 1 §10, $\alpha a + \beta b \in U_1, \ldots, \alpha a + \beta b \in U_k$, т. е. $\alpha a + \beta b \in \bigcap\limits_{i=1}^{k} U_i$. Далее, для любых $\alpha, \beta \in F$, $a, b \in \sum\limits_{i=1}^{k} U_i$ имеем $a = a_1 + \ldots + a_k$, $b = b_1 + \ldots + b_k$, где $a_i, b_i \in U_i$. Следовательно, по лемме 1 §10, $\alpha a_i + \beta b_i \in U_i$ и $\alpha a + \beta b = \alpha \sum\limits_{i=1}^{k} a_i + \beta \sum\limits_{i=1}^{k} b_i = \sum\limits_{i=1}^{k} \alpha a_i + \beta b_i \in \sum\limits_{i=1}^{k} U_i$. По лемме 1 §10, $\bigcap\limits_{i=1}^{k} U_i$ и $\sum\limits_{i=1}^{k} U_i$ — подпространства в V. □

Задача. В общем случае $U_1 \bigcup U_2$ не является подпространством в V.

Теорема 1. *Пусть* U_1, U_2 — *подпространства в* V. *Тогда* $\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$.

Доказательство. Пусть $\dim U_1 = n_1$, $\dim U_2 = n_2$, $\dim(U_1 \cap U_2) = m$. Пусть $a_1, \ldots, a_m$ — базис $U_1 \cap U_2$. Так как $U_1 \cap U_2 \subseteq U_1$, то, по лемме 3, мы можем дополнить $a_1, \ldots, a_m$ векторами $b_1, \ldots, b_k \in U_1$ до базиса пространства U_1, тогда $m + k = n_1$. Аналогично, $a_1, \ldots, a_m, c_1, \ldots, c_\ell$ — базис U_2, где $m + \ell = n_2$. Докажем, что $a_1, \ldots, a_m, b_1, \ldots, b_k, c_1, \ldots, c_\ell$ — базис $U_1 + U_2$.

1) Пусть $u \in U_1 + U_2$, $u = u_1 + u_2$, где $u_1 \in U_1$, $u_2 \in U_2$. Тогда

$$u_1 = \sum_{i=1}^{m} \alpha_i a_i + \sum_{i=1}^{k} \beta_i b_i, \quad \alpha_i, \beta_i \in F, \; u_2 = \sum_{i=1}^{m} \gamma_i a_i + \sum_{i=1}^{\ell} \delta_i c_i, \quad \gamma_i, \delta_i \in F,$$

$u = u_1 + u_2 = \sum\limits_{i=1}^{m} (\alpha_i + \gamma_i) a_i + \sum\limits_{i=1}^{k} \beta_i b_i + \sum\limits_{i=1}^{\ell} \delta_i c_i \in L(a_1, \ldots, a_m, b_1, \ldots, b_k, c_1, \ldots, c_\ell)$. Таким образом, $U_1 + U_2 = L(a_1, \ldots, a_m, b_1, \ldots, b_k, c_1, \ldots, c_\ell)$.

2) Пусть $\sum\limits_{i=1}^{m} \alpha_i a_i + \sum\limits_{i=1}^{k} \beta_i b_i + \sum\limits_{i=1}^{\ell} \gamma_i c_i = 0$, где $\alpha_i, \beta_i, \gamma_i \in F$. Тогда $\sum\limits_{i=1}^{m} \alpha_i a_i + \sum\limits_{i=1}^{k} \beta_i b_i = -\sum\limits_{i=1}^{\ell} \gamma_i c_i = c$. Следовательно, $c \in U_2$, $c \in U_1$, т. е. $c \in U_1 \bigcap U_2$ и $c = -\sum\limits_{i=1}^{\ell} \gamma_i c_i = \sum\limits_{i=1}^{m} \delta_i a_i$. Тогда $\sum\limits_{i=1}^{m} \delta_i a_i + \sum\limits_{i=1}^{\ell} \gamma_i c_i = 0$ и $\delta_i, \gamma_i = 0 \Rightarrow c = 0 = \sum\limits_{i=1}^{m} \alpha_i a_i + \sum\limits_{i=1}^{k} \beta_i b_i = 0$, откуда $\alpha_i, \beta_i = 0$ и $\dim(U_1 + U_2) = m + k + \ell = (m + k) + (m + \ell) - m = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$. □

Пусть U_1, U_2 — подпространства в V. Сумма $U_1 + U_2$ называется *прямой* и обозначается $U_1 \oplus U_2$, если $U_1 \cap U_2 = 0$.

Лемма 2. *Пусть U_1, U_2 — подпространства в V и $U = U_1 + U_2$. Тогда $U = U_1 \oplus U_2 \iff$ для любого $u \in U$ существуют единственные $u_1 \in U_1, u_2 \in U_2$ такие, что $u = u_1 + u_2$.*

Доказательство. Если $U = U_1 \oplus U_2$ и $u \in U$, то $u = u_1 + u_2$ для некоторых $u_1 \in U_1, u_2 \in U_2$. Если при этом $u = v_1 + v_2$ для некоторых $v_1 \in U_1, v_2 \in U_2$, то $u_1 - v_1 = v_2 - u_2 \in U_2 \cap U_1$, т. е. $u_1 = v_1, u_2 = v_2$.

Обратно, если $U_1 \cap U_2 \neq 0$, то существует ненулевой $u \in U_1 \cap U_2$, но тогда $u = u + 0$ и $u = 0 + u$ — два различных разложения элемента u. □

§15. Пространство линейных отображений $L(U, V)$ и пространство матриц $M_{m,n}(F)$

Пусть U и V — векторные пространства над F. Отображение $\varphi : U \to V$ называется линейным, если $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(\alpha x) = \alpha\varphi(x)$ для любых $x, y \in U, \alpha \in F$. Данное эквивалентно тому, что $\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$ для любых $\alpha, \beta \in F$, $x, y \in U$.

Примеры. 1) *Нулевое*: $\varphi : F_n \to F_m$, для любого $x \in F_n$ полагаем $\varphi(x) = 0 \in F_m$. Обозначим это отображение через 0, $\varphi := 0$.

2) *Единичное*: $\varphi : F_n \to F_n$, для любого $x \in F_n$ полагаем $\varphi(x) = x \in F_n$. Обозначаем $\varphi := id$.

3) *Проекция на i-ю координату*: $\varphi : F_n \to F_1$, для любого $x = (x_1, \ldots, x_n) \in F_n$ полагаем $\varphi(x) = x_i$. Обозначаем $\varphi := Pr_i$.

Обозначим через $L(U, V)$ множество всех линейных отображений из U в V. Определим операции на $L(U, V)$:
1) $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$ для любых $\varphi, \psi \in L(U, V)$;
2) $(\alpha\varphi)(x) = \alpha\varphi(x)$ для любых $\alpha \in F$, $\varphi \in L(U, V)$.

Лемма 1. *$L(U, V)$ с заданными операциями — это векторное пространство над F.*

Доказательство. $L(U, V) \neq \varnothing$, так как $0 \in L(U, V)$. Проверим, что $L(U, V)$ замкнуто относительно операций: для любых $\varphi, \psi \in L(U, V)$, $\alpha, \beta, \gamma \in F$, $x, y \in U$ имеем

$$(\varphi + \psi)(\alpha x + \beta y) = \varphi(\alpha x + \beta y) + \psi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$$

$$+\alpha\psi(x) + \beta\psi(y) = \alpha(\varphi(x) + \psi(x)) + \beta(\varphi(y) + \psi(y)) =$$

$$= \alpha(\varphi + \psi)(x) + \beta(\varphi + \psi)(y),$$

$$(\gamma\varphi)(\alpha x + \beta y) = \gamma(\varphi(\alpha x + \beta y)) = \gamma(\alpha\varphi(x) + \beta\varphi(y)) =$$

$$= \alpha\gamma\varphi(x) + \beta\gamma\varphi(y) = \alpha(\gamma\varphi)(x) + \beta(\gamma\varphi)(y).$$

$$0 \in L(U, V); \quad -\varphi := (-1)\varphi \Rightarrow \varphi + (-\varphi) = 0.$$

Остальные аксиомы проверяются аналогично. □

Рассмотрим множество $M_{n,m}(F)$ всех матриц над F и определим на нем операции:

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1m} + b_{1m} \\ \vdots & & \vdots \\ a_{n1} + b_{n1} & \cdots & a_{nm} + b_{nm} \end{pmatrix},$$

$$\alpha \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \cdots & \alpha a_{1m} \\ \vdots & & \vdots \\ \alpha a_{n1} & \cdots & \alpha a_{nm} \end{pmatrix}, \text{ где } \alpha \in F.$$

Матричной единицей E_{ij} в $M_{n,m}(F)$ называется матрица, у которой на пересечении i-строки и j-столбца стоит 1, а остальные элементы нулевые.

Лемма 2. 1) $M_{n,m}(F)$ — *векторное пространство над* F. 2) *Для* $1 \leq i \leq n,\ \ 1 \leq j \leq m$, *матричные единицы* E_{ij} *образуют базис* $M_{n,m}(F)$ *и* $\dim_F M_{n,m}(F) = n \cdot m$.

Доказательство. 1) Прямая проверка аксиом векторного пространства.

2) Пусть $A = (\alpha_{ij}) \in M_{n,m}(F)$. Тогда $A = \sum\limits_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \alpha_{ij}E_{ij}$, т. е. $M_{n,m}(F) = L(E_{ij} : 1 \leq i \leq n,\ \ 1 \leq j \leq m)$. Пусть $\sum\limits_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \alpha_{ij}E_{ij} = 0 = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix}$. Тогда $\alpha_{ij} = 0$ для любых i, j. □

§16. Изоморфизм пространств $L(U, V)$ и $M_{m,n}(F)$

Умножение строки на матрицу: Пусть $X \in F_m$, $A \in M_{m,n}(F)$. Определим

$$XA = (x_1, \ldots, x_m) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} := \left(\sum_{k=1}^{m} a_{k1}x_k, \ldots, \sum_{k=1}^{m} a_{kn}x_k \right).$$

Имеем $XA = ((a_{11}x_1 + \ldots + a_{m1}x_m), \ldots, (a_{1n}x_1 + \ldots + a_{mn}x_m)) =$

$$= (a_{11}x_1, \ldots, a_{1n}x_1) + \ldots + (a_{m1}x_m, \ldots, a_{mn}x_m) =$$

$$= x_1 (a_{11}, \ldots, a_{1n}) + \ldots + x_m (a_{m1}, \ldots, a_{mn}) = x_1A_1 + \ldots + x_mA_m,$$

где $A_i = (a_{i1}, \ldots, a_{in})$ — i-строка матрицы A, $i = 1, \ldots, m$.

Заметим, что для любых $X \in F_m$, $A \in M_{m,n}(F)$ имеем $XA \in F_n$.

Для любой $A \in M_{m,n}(F)$ определим отображение $\varphi_A : F_m \to F_n$ по правилу: $\varphi_A(X) = XA$ для любого $X \in F_m$.

Лемма 1. $\varphi_A \in L(F_m, F_n)$ *для любой* $A \in M_{m,n}(F)$.

Доказательство. Для любых $\alpha, \beta \in F$, $X, Y \in F_m$, $A \in M_{m,n}(F)$ имеем $\varphi_A(\alpha X + \beta Y) = (\alpha X + \beta Y)A = (\alpha x_1 + \beta y_1)A_1 + \ldots + (\alpha x_m + \beta y_m)A_m = \sum\limits_{i=1}^{m} \alpha x_i A_i + \sum\limits_{i=1}^{m} \beta y_i A_i = \alpha \sum\limits_{i=1}^{m} x_i A_i + \beta \sum\limits_{i=1}^{m} y_i A_i = \alpha(XA) + \beta(YA) = \alpha\varphi_A(x) + \beta\varphi_A(y)$. Следовательно, $\varphi_A \in L(F_m, F_n)$. □

Определим отображение $L : M_{m,n}(F) \to L(F_m, F_n)$ по правилу: для $A \in M_{m,n}(F)$ положим $L(A) = \varphi_A$.

Теорема 1. $L : M_{m,n}(F) \to L(F_m, F_n)$ — *изоморфизм пространств* $M_{m,n}(F)$ *и* $L(F_m, F_n)$.

Доказательство. Докажем, что L — это взаимно однозначное отображение.

Сюръективность. Для любых $\varphi \in L(F_m, F_n)$, $X = (x_1, \ldots, x_m) \in F_m$ имеем

$$X = (x_1, \ldots, x_m) = (x_1, 0, \ldots, 0) + \ldots + (0, \ldots, 0, x_m) =$$

$$= x_1 \cdot (1, 0, \ldots, 0) + x_2 \cdot (0, 1, \ldots, 0) + \ldots + x_m \cdot (0, 0, \ldots, 1) = \sum_{i=1}^{m} x_i \ell_i,$$

где $\ell_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Поэтому, $\varphi(X) = \varphi\left(\sum\limits_{i=1}^{m} x_i \ell_i\right) = \sum\limits_{i=1}^{m} x_i \varphi(\ell_i)$, где $\varphi(\ell_i) \in F_n$.

Обозначим $\varphi(\ell_i) = A_i$, $i = 1, \ldots, m$, и $A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$. Тогда

$$\varphi(X) = \sum_{i=1}^{m} x_i \varphi(\ell_i) = \sum_{i=1}^{m} x_i A_i = XA.$$

Следовательно, по определению, $\varphi(X) = \varphi_A(X)$. Тогда $L(A) = \varphi_A = \varphi$.

Инъективность. Пусть $A, B \in M_{m,n}(F)$ и $A \neq B$. Тогда существуют i, j такие, что $\alpha_{ij} \neq \beta_{ij}$. Поэтому

$$\varphi_A(\ell_i) = 0 \cdot A_1 + \ldots + 1 \cdot A_i + \ldots + 0 \cdot A_m = A_i,$$

$$\varphi_B(\ell_i) = 0 \cdot B_1 + \ldots + 1 \cdot B_i + \ldots + 0 \cdot B_m = B_i.$$

Но $A_i \neq B_i$, так как $\alpha_{ij} \neq \beta_{ij}$. Поэтому $\varphi_A(\ell_i) \neq \varphi_B(\ell_i)$ и $\varphi_A \neq \varphi_B$, откуда следует $L(A) = \varphi_A \neq L(B) = \varphi_B$.

Сохранение операций. Для любых $\alpha, \beta \in F$, $A, B \in M_{m,n}(F)$, $X \in F_m$ имеем:

$$L(\alpha A + \beta B) = \varphi_{(\alpha A + \beta B)}, \alpha L(A) = \alpha \varphi_A, \beta L(B) = \beta \varphi_B.$$

Далее, $\varphi_{(\alpha A+\beta B)}(X) = X \cdot (\alpha A + \beta B) = \sum\limits_{i=1}^{m} x_i (\alpha A + \beta B)_i =$ $\sum\limits_{i=1}^{m} x_i (\alpha A_i + \beta B_i) = \sum\limits_{i=1}^{m} \alpha x_i A_i + \sum\limits_{i=1}^{m} \beta x_i B_i = \alpha \sum\limits_{i=1}^{m} x_i A_i + \beta \sum\limits_{i=1}^{m} x_i B_i = \alpha (X \cdot A) +$ $\beta (X \cdot B) = \alpha \varphi_A(X) + \beta \varphi_B(X) = (\alpha \varphi_A + \beta \varphi_B)(X)$. Следовательно, $\varphi_{(\alpha A+\beta B)} = \alpha \varphi_A + \beta \varphi_B$ и $L(\alpha A + \beta B) = \alpha L(A) + \beta L(B)$, т. е. L — изоморфизм. □

Пусть $\varphi \in L(F_m, F_n)$, матрица $A = \begin{pmatrix} \varphi(\ell_1) \\ \vdots \\ \varphi(\ell_m) \end{pmatrix}$, где $\ell_1, \ldots, \ell_m$ — стандартный базис F_m, называется *матрицей преобразования* φ *в базисе* $\ell_1, \ldots, \ell_m$ и обозначается через $[\varphi]$.

Определим отображение $[\ ] : L(F_m, F_n) \to M_{m,n}(F)$ правилом: $[\ ](\varphi) = [\varphi]$.

Лемма 2. *Отображение* $[\ ]$ *является биективным.*

Доказательство. Заметим, что для любой $A \in M_{m,n}(F)$ справедливо

$$[\varphi_A] = \begin{pmatrix} \varphi_A(\ell_1) \\ \vdots \\ \varphi_A(\ell_m) \end{pmatrix} = \begin{pmatrix} \ell_1 A \\ \vdots \\ \ell_m A \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} = A, \tag{1}$$

т. е. $[\ ]$ сюръективно. Далее, если $\varphi, \psi \in L(F_m, F_n)$ и $\varphi \neq \psi$, то по теореме 1 $\varphi = \varphi_A, \psi = \varphi_B$, для некоторых различных $A, B \in M_{m,n}(F)$, и $\varphi_A \neq \varphi_B$. Тогда $[\varphi] = [\varphi_A] = A \neq B = [\varphi_B] = [\psi]$. Таким образом, отображение $[\ ]$ является инъективным. □

§17. Суперпозиция линейных отображений и произведение матриц

Суперпозиция двух отображений $\psi : U \to V$ и $\varphi : V \to W$ есть отображение $\psi \circ \varphi : U \to W$, определенное по правилу: $(\psi \circ \varphi)(x) = \varphi(\psi(x))$ для любого $x \in U$, т. е.

$$x \xrightarrow{\psi} \psi(x) \xrightarrow{\varphi} \varphi(\psi(x)).$$
$$\searrow \_\_\_\_\_ \nearrow_{(\psi\circ\varphi)}$$

Лемма 1. *a) Для любых* $\varphi_1 : V_1 \to V_2$, $\varphi_2 : V_2 \to V_3$, $\varphi_3 : V_3 \to V_4$ *имеем* $\varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3$ *— суперпозиция отображений ассоциативна.*

b) Если $\psi \in L(U, V)$, $\varphi \in L(V, W)$, *то* $\psi \circ \varphi \in L(U, W)$ *— суперпозиция линейных отображений является линейным отображением.*

c) Для любых линейных отображений $\psi \in L(U, V)$, $\phi \in L(V, W), \theta \in L(V, W), \kappa \in L(W, U)$ *верно* $\psi \circ (\phi + \theta) = \psi \circ \phi + \psi \circ \theta$, $(\phi + \theta) \circ \kappa = \phi \circ \kappa + \theta \circ \kappa$ *— суперпозиция отображений дистрибутивна.*

Доказательство. a) Для любого $v \in V_1$ имеем $(\varphi_1 \circ (\varphi_2 \circ \varphi_3))(v) = (\varphi_2 \circ \varphi_3)(\varphi_1(v)) = \varphi_3(\varphi_2(\varphi_1(v))) = \varphi_3((\varphi_1 \circ \varphi_2)(v)) = ((\varphi_1 \circ \varphi_2) \circ \varphi_3)(v) \Rightarrow \varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3$.

b) Для любых $\alpha, \beta \in F$, $x, y \in U$ имеем: $(\psi \circ \varphi)(\alpha x + \beta y) = \varphi(\psi(\alpha x + \beta y)) = \varphi(\alpha\psi(x) + \beta\psi(y)) = \alpha\varphi(\psi(x)) + \beta\varphi(\psi(y)) = \alpha(\psi \circ \varphi)(x) + \beta(\psi \circ \varphi)(y)$.

c) Для любого $u \in U$ имеем $(\psi \circ (\phi + \theta))(u) = (\phi + \theta)(\psi(u)) = \phi(\psi(u)) + \theta(\psi(u)) = (\psi \circ \phi)(u) + (\psi \circ \theta)(u) = (\psi \circ \phi + \psi \circ \theta)(u)$. Для любого $w \in W$ имеем $((\phi + \theta) \circ \kappa)(w) = \kappa((\phi + \theta)(w)) = \kappa(\phi(w)) + \kappa(\theta(w)) = (\phi \circ \kappa)(w) + (\theta \circ \kappa)(w) = (\phi \circ \kappa + \theta \circ \kappa)(w)$. □

Примеры. 1) Рассмотрим суперпозицию отображений L и $[\ ]$. По определению $L \circ [\ ] : M_{m,n}(F) \mapsto M_{m,n}(F)$ и $(L \circ [\ ])(A) = [L(A)] = [\varphi_A] = A$.

2) Рассмотрим суперпозицию отображений $[\ ]$ и L. По определению $[\ ] \circ L : L(F_m, F_n) \mapsto L(F_m, F_n)$. Пусть $\varphi \in L(F_m, F_n)$ и $\varphi = \varphi_A$ для некоторой $A \in M_{m,n}(F)$. Тогда $([\ ] \circ L)(\varphi) = L([\varphi]) = L([\varphi_A]) = L(A) = \varphi_A = \varphi$.

Для любых $A \in M_{m,s}(F)$, $B \in M_{s,n}(F)$ положим

$$C = A \cdot B = \begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{ms} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{s1} & \cdots & a_{sn} \end{pmatrix} := \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \cdots & \cdots & \cdots \\ c_{m1} & \cdots & c_{mn} \end{pmatrix},$$

где $c_{ij} = \sum\limits_{k=1}^{s} a_{ik} b_{kj} = A_i B^{(j)}$, т. е.

$$A \cdot B = \begin{pmatrix} A_1 B^{(1)} & \cdots & A_1 B^{(n)} \\ \cdots & \cdots & \cdots \\ A_m B^{(1)} & & A_m B^{(n)} \end{pmatrix} = \begin{pmatrix} A_1 B \\ \vdots \\ A_m B \end{pmatrix}. \tag{1}$$

Теорема 1. *Для любых $\psi \in L(F_m, F_s)$ и $\varphi \in L(F_s, F_n)$ имеем $[\psi \circ \varphi] = [\psi] \cdot [\varphi]$.*

Доказательство. Из теоремы 1 §16 следует, что существуют $A \in M_{m,s}(F)$, $B \in M_{s,n}(F)$ такие, что $\psi = \varphi_A$, $\varphi = \varphi_B$.

Будем обозначать стандартный базис F_n через $\ell_1(n), \ldots, \ell_n(n)$. Тогда

$$[\psi \circ \varphi] = [\varphi_A \circ \varphi_B] = \begin{pmatrix} (\varphi_A \circ \varphi_B)(\ell_1(m)) \\ \cdots\cdots\cdots\cdots \\ (\varphi_A \circ \varphi_B)(\ell_m(m)) \end{pmatrix}.$$

Имеем, для $1 \le i \le m$, $(\varphi_A \circ \varphi_B)(\ell_i(m)) = \varphi_B(\varphi_A(\ell_i(m))) = \varphi_B(\ell_i(m)\, A) = (\ell_i(m) \cdot A) \cdot B = A_i \cdot B$. Поэтому, в силу (1) §16 и §17, $[\psi \circ \varphi] = \begin{pmatrix} A_1 B \\ \vdots \\ A_m B \end{pmatrix} = A \cdot B = [\varphi_A] \cdot [\varphi_B] = [\varphi_{A \cdot B}] = [\psi] \cdot [\varphi]$. □

Отметим, что из доказательства теоремы 1 для любых $A \in M_{m,s}(F)$, $B \in M_{s,n}(F)$ следует формула

$$\varphi_{A\cdot B} = \varphi_A \circ \varphi_B. \tag{2}$$

Следствие 1. *a) Для любых* $A \in M_{m,s}(F)$, $B \in M_{s,t}(F)$, $C \in M_{t,n}(F)$ *справедливо* $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ *— умножение матриц ассоциативно.*

b) Для любых $A \in M_{m,s}(F)$, $B \in M_{s,t}(F)$, $C \in M_{s,t}(F)$, $D \in M_{t,m}(F)$ *справедливо* $A \cdot (B + C) = AB + AC$, $(B + C)D = BD + CD$ *— умножение матриц дистрибутивно.*

Доказательство. a) По формуле (2) и лемме 1, имеем

$$\varphi_{(A\cdot B)\cdot C} = \varphi_{A\cdot B} \circ \varphi_C = (\varphi_A \circ \varphi_B) \circ \varphi_C = \varphi_A \circ (\varphi_B \circ \varphi_C) = \varphi_A \circ \varphi_{B\cdot C} = \varphi_{A\cdot(B\cdot C)}.$$

Тогда $\left[\varphi_{(A\cdot B)\cdot C}\right] = (A \cdot B) \cdot C = \left[\varphi_{A\cdot(B\cdot C)}\right] = A \cdot (B \cdot C)$.

b) По лемме 1 c), имеем $\varphi_{A\cdot(B+C)} = \varphi_A \circ \varphi_{B+C} = \varphi_A \circ (\varphi_B + \varphi_C) = \varphi_A \circ \varphi_B + \varphi_A \circ \varphi_C = \varphi_{AB} + \varphi_{AC} = \varphi_{AB+AC}$. Продолжая далее как и в пункте 1, получаем требуемое. Аналогично показывается второе равенство. □

§18. Обратимые преобразования и матрицы

Отображение $1_X : X \to X$ называется *единичным* (или тождественным), если $1_X(x) = x$ для любого $x \in X$. Отображение $g : Y \to X$ называется *обратным* к $f : X \to Y$ и обозначается $g = f^{-1}$, если $f \circ g = 1_X$, $g \circ f = 1_Y$. При этом f называется *обратимым*.

Лемма 1. *Для любого отображения* $f : X \to Y$ *имеем*:
a) $f \circ 1_Y = f$, $1_X \circ f = f$;
b) обратное отображение g *определяется однозначно*;
c) если $f \circ g = 1_X$, *то* f *инъективно, а* g *сюръективно*;
d) f *обратимо* $\Leftrightarrow$ f *биективно.*

Доказательство. a) Для любого $x \in X$ имеем: $f \circ 1_Y(x) = 1_Y(f(x)) = f(x)$, $1_X \circ f(x) = f(1_X(x)) = f(x)$.

b) Пусть $f \circ g_1 = f \circ g_2 = 1_X$, $g_1 \circ f = g_2 \circ f = 1_Y$. Тогда $g_1 = g_1 \circ 1_X = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = 1_Y \circ g_2 = g_2$.

c) Пусть $f(x_1) = f(x_2)$. Тогда $x_1 = 1_X(x_1) = (f \circ g)(x_1) = g(f(x_1)) = g(f(x_2)) = (f \circ g)(x_2) = 1_X(x_2) = x_2$, т. е. f инъективно. Для любого $x \in X$ имеем: $x = 1_X(x) = (f \circ g)(x) = g(f(x))$. Следовательно, g сюръективно.

d) Если $f \circ g = 1_X$, $g \circ f = 1_Y$, то f инъективно и сюръективно $\Rightarrow$ f биективно.

Обратно, для любого $y \in Y$ существует единственный $x \in X$ такой, что $f(x) = y$. Положим $g(y) = x$. Тогда $g : Y \to X$ и $f \circ g = 1_X$, $g \circ f = 1_Y$. $\square$

Следствие 1. *a) Если f биективно, то f^{-1} биективно и $(f^{-1})^{-1} = f$.*
b) Если $f : X \to Y$ и $h : Y \to Z$ — биективные отображения, то $f \circ h$ биективно и $(f \circ h)^{-1} = h^{-1} \circ f^{-1}$.

Доказательство. a) По лемме 1, f^{-1} существует и обратимо $\Rightarrow$ f^{-1} биективно и

$$f \circ f^{-1} = 1_X, f^{-1} \circ f = 1_Y \Rightarrow \left(f^{-1}\right)^{-1} = f.$$

b) По лемме 1, имеем $(f \circ h) \circ \left(h^{-1} \circ f^{-1}\right) = f \circ \left(\left(h \circ h^{-1}\right) \circ f^{-1}\right) = f \circ \left(1_Y \circ f^{-1}\right) = f \circ f^{-1} = 1_X$. Аналогично, $\left(h^{-1} \circ f^{-1}\right) \circ (f \circ h) = 1_Z$. $\square$

Множество матриц $M_{n,n}(F)$ обозначается через $M_n(F)$. Матрицы из $M_n(F)$ называются *квадратными*. Матрица $A \in M_n(F)$ называется *обратимой*, если существует $B \in M_n(F)$ такая, что $A \cdot B = B \cdot A = E$, где $E = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ — *единичная* матрица. Матрица B называется *обратной* к A и обозначается $B = A^{-1}$. Обратимая матрица называется также невырожденной. Как и в случае линейных отображений, легко доказать, что обратная матрица единственна.

Теорема 1. *Для любого преобразования $\varphi \in L(F_n, F_n)$ следующие условия эквивалентны:*

a) φ обратимо;

b) φ^{-1} обратимо и $\varphi^{-1} \in L(F_n, F_n)$;

c) $[\varphi]$ — обратимая матрица.

Доказательство. a) $\Leftrightarrow$ b) По лемме 1, φ^{-1} — биективное и, следовательно, обратимое отображение. Докажем линейность φ^{-1}. Для любых $\alpha, \beta \in F$ и $X, Y \in F_n$ обозначим

$$Z = \varphi^{-1}(\alpha X + \beta Y) - \alpha\varphi^{-1}(X) - \beta\varphi^{-1}(Y).$$

Тогда $\varphi(Z) = \varphi\left(\varphi^{-1}(\alpha X + \beta Y)\right) - \alpha\varphi\left(\varphi^{-1}(X)\right) - \beta\varphi\left(\varphi^{-1}(Y)\right) = \left(\varphi^{-1} \circ \varphi\right)(\alpha X + \beta Y) - \alpha\left(\varphi^{-1} \circ \varphi\right)(X) - \beta\left(\varphi^{-1} \circ \varphi\right)(Y) = \alpha X + \beta Y - \alpha X - \beta Y = 0$. Так как $\varphi(0) = 0$ и φ биективно, то $Z = 0$. Следовательно, $\varphi^{-1}(\alpha X + \beta Y) = \alpha\varphi^{-1}(X) + \beta\varphi^{-1}(Y)$.

a) $\Rightarrow$ c) Так как отображение φ обратимо, то, по пункту $b)$, φ^{-1} — обратимое линейное преобразование и $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = 1$, где $1 = 1_{F^n}$.

Имеем, по теореме 1 §17,

$$\left[\varphi \circ \varphi^{-1}\right] = [\varphi] \cdot \left[\varphi^{-1}\right] = \left[\varphi^{-1} \circ \varphi\right] = \left[\varphi^{-1}\right] \cdot [\varphi] = [1].$$

Но $[1] = \begin{pmatrix} 1(\ell_1(n)) \\ \vdots \\ 1(\ell_n(n)) \end{pmatrix} = \begin{pmatrix} \ell_1(n) \\ \vdots \\ \ell_n(n) \end{pmatrix} = E$. Поэтому $[\varphi] \cdot \left[\varphi^{-1}\right] = \left[\varphi^{-1}\right] \cdot [\varphi] = E$ и $[\varphi]$ — обратимая матрица, причем $[\varphi]^{-1} = [\varphi^{-1}]$.

c) $\Rightarrow$ *a)* $[\varphi] \cdot B = B \cdot [\varphi] = E$. Тогда, по формуле 1 §16, $[\varphi_B] = B$. Поэтому $[\varphi] \cdot [\varphi_B] = [\varphi \circ \varphi_B] = [\varphi_B] \cdot [\varphi] = [\varphi_B \circ \varphi] = [1]$. Так как $[\ ]$ инъективно, то $\varphi \circ \varphi_B = \varphi_B \circ \varphi = 1$, т. е. φ обратимо. □

Следствие 2. *Отображение* $[\ ]$ *является изоморфизмом* $L(F_m, F_n)$ *и* $M_{m,n}(F)$.

Доказательство. Из примеров §17 следует, что $[\ ]$ — это отображение обратное к L. Поэтому из Следствия 1 и Теоремы 1 следует, что $[\ ]$ является изоморфизмом. □

Следствие 3. *Для любых матриц* $A, B \in M_n(F)$ *имеем*

1) A *обратима* $\Leftrightarrow$ A^{-1} *обратима и* $(A^{-1})^{-1} = A$;

2) A, B *обратимы* $\Rightarrow$ $A \cdot B$ *обратима и* $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

Доказательство. Так как обратная матрица определена однозначно, то утверждение следует из равенств $AA^{-1} = A^{-1}A = E$, $(AB)(B^{-1} \cdot A^{-1}) = (B^{-1} \cdot A^{-1})(AB) = E$. □

§19. Образ и ядро линейного отображения, связь их размерностей. Характеризация обратимого преобразования в терминах ядра и образа

Рассмотрим линейное отображение $\varphi : V \to U$, где V, U — векторные пространства над F. *Ядром* линейного отображения φ называется множество

$$Ker\,\varphi = \{v \in V : \varphi(v) = 0\} \subseteq V,$$

образом линейного отображения φ называется множество

$$Im\,\varphi = \{\varphi(v) : v \in V\} \subseteq U.$$

Лемма 1. $Ker\,\varphi$ *— подпространство в* V, $Im\,\varphi$ *— подпространство в* U.

Доказательство. Так как $\varphi(0) = 0$, то $0 \in Ker\,\varphi \neq \varnothing$, $0 \in Im\,\varphi \neq \varnothing$. Далее, для любых $\alpha, \beta \in F$, $a, b \in Ker\,\varphi$ имеем $\varphi(\alpha a + \beta b) = \alpha\varphi(a) + \beta\varphi(b) = 0$. Следовательно, $\alpha a + \beta b \in Ker\,\varphi$, поэтому $Ker\,\varphi$ — подпространство в V.

Для любых $\alpha, \beta \in F$, $\varphi(a), \varphi(b) \in Im\,\varphi$ имеем $\alpha\varphi(a) + \beta\varphi(b) = \varphi(\alpha a + \beta b)$, т. е. $Im\,\varphi$ — подпространство в U. □

Теорема 1. $\dim V = \dim Ker\,\varphi + \dim Im\,\varphi$.

Доказательство. Пусть $e_1, \ldots, e_k$ — базис $Ker\,\varphi$, дополним его векторами $e_{k+1}, \ldots, e_n$ до базиса V. Тогда $Im\,\varphi = L(\varphi(e_1), \ldots, \varphi(e_n)) = L(\varphi(e_{k+1}), \ldots, \varphi(e_n))$. Пусть $\sum\limits_{i=k+1}^{n} \alpha_i\varphi(e_i) = 0$. Тогда $0 = \sum\limits_{i=k+1}^{n} \varphi(\alpha_i e_i) = \varphi\left(\sum\limits_{i=k+1}^{n} \alpha_i e_i\right)$. Поэтому $\sum\limits_{i=k+1}^{n} \alpha_i e_i \in Ker\,\varphi$ и существуют $\alpha_1, \ldots, \alpha_k \in F$ такие, что $\sum\limits_{i=k+1}^{n} \alpha_i e_i = -\sum\limits_{i=1}^{k} \alpha_i e_i$, откуда $\sum\limits_{i=1}^{n} \alpha_i e_i = 0$. Тогда $\alpha_1 = \ldots = \alpha_n = 0$ и $\varphi(e_{k+1}), \ldots, \varphi(e_n)$ линейно независимы. Следовательно, $\varphi(e_{k+1}), \ldots, \varphi(e_n)$ — базис $Im\,\varphi$ и $\dim V = n = k + (n-k) = \dim Ker\,\varphi + \dim Im\,\varphi$. □

Теорема 2. *Пусть $\varphi \in L(V, V)$, V — конечномерное пространство. Тогда следующие условия эквивалентны*: 1) *φ обратимо*; 2) $Ker\,\varphi = 0$; 3) $Im\,\varphi = V$.

Доказательство. По теореме 1, имеем $Ker\,\varphi = 0 \Leftrightarrow \dim Ker\,\varphi = 0 \Leftrightarrow \dim Im\,\varphi = \dim V \Leftrightarrow Im\,\varphi = V$, откуда следует эквивалентность 2) $\Leftrightarrow$ 3).

1) $\Rightarrow$ 2) Если φ обратимо, то φ биективно по лемме 1 §18 и $Ker\,\varphi = 0$.

Пусть $Ker\,\varphi = 0$, тогда $Im\,\varphi = V$, φ сюръективно и, более того, если $a, b \in V$ и $\varphi(a) = \varphi(b)$, то $0 = \varphi(a) - \varphi(b) = \varphi(a - b)$, т. е. $a - b \in Ker\,\varphi$, $a = b$. Поэтому φ инъективно и 1) $\Leftrightarrow$ 2). □

Отображение $\varphi \in L(V, V)$ называется *невырожденным*, если $Ker\,\varphi = 0$.

Следствие. *Пусть* $\dim_F V < \infty$. *Тогда φ невырождено $\Leftrightarrow$ φ обратимо.*

§20. Вертикальный и горизонтальный ранги матрицы, их равенство

Пусть $A \in M_{m,n}(F)$, $V_\Gamma = V_\Gamma(A)$ — подпространство в F_n, порожденное строками A, и $V_B = V_B(A)$ — подпространство в F^m, порожденное столбцами A. Тогда $\dim V_\Gamma := r_\Gamma$ называется *горизонтальным рангом* (ранг по строкам) матрицы A, $\dim V_B = r_B$ — *вертикальным рангом* (ранг по столбцам) матрицы A.

Лемма 1. *Если матрица A' получена из матрицы A элементарными преобразованиями строк, то $r_\Gamma(A) = r_\Gamma(A')$, $r_B(A) = r_B(A')$.*

Доказательство. Первое очевидно. Для доказательства второго надо заметить, что если A' получена из A элементарным преобразованием I и II типа, то всякая линейная зависимость между столбцами A перейдет в ту же зависимость (с теми же коэффициентами) между столбцами A'. Так как A также получается из A' элементарным преобразованием строк, то какие-то столбцы A линейно зависимы $\Leftrightarrow$ соответствующие столбцы A' линейно зависимы. Поэтому $r_B(A) = r_B(A')$. □

Пусть $A = (a_{ij}) \in M_{m,n}(F)$. Тогда матрица $A = (a_{ji}) \in M_{n,m}(F)$, у которой по определению элемент в i-ой строке и j-ом столбце равен a_{ji}, называется *транспонированной* матрицей к матрице A и обозначается A^τ.

Теорема 1. $r_\Gamma(A) = r_B(A)$ (*вертикальный и горизонтальные ранги совпадают*).

Доказательство. Достаточно доказать неравенство $r_B(A) \le r_\Gamma(A)$, тогда из аналогичного неравенства для транспонированной матрицы получим $r_\Gamma(A) = r_B(A^\tau) \le r_\Gamma(A^\tau) = r_B(A)$ и окончательно $r_\Gamma(A) = r_B(A)$.

Приведем A элементарными преобразованиями строк I и II типа к ступенчатому виду A'. По лемме достаточно доказать искомое неравенство для A'. Пусть A' имеет r ненулевых строк; тогда эти строки независимы, и $r_\Gamma(A') = r$. Так как в каждом столбце матрицы A' последние $m-r$ координат нулевые, то без ограничения общности можно считать, что $V_B(A') \subseteq F^r$, откуда $r_B(A') = \dim V_B(A') \le \dim F^r = r$. □

Число $r(A) = r_\Gamma(A) = r_B(A)$ называется *рангом* матрицы A.

Следствие. *Пусть* $A \in M_{m,n}(F)$. *Тогда* $r(A) = r(A^\tau)$.

§21. Ранг матрицы как размерность образа соответствующего линейного преобразования. Ранг произведения матриц

В §16 мы определили умножение строки на матрицу и в теореме 1 §16 было доказано, что отображение L является изоморфизмом линейных пространств $M_{m,n}(F)$ и $L(F_m, F_n)$. Аналогично, можно рассмотреть умножение столбца на матрицу. Для любых $X \in F^n$ и $A \in M_{m,n}(F)$ положим

$$A \cdot X = \begin{pmatrix} A_1 X \\ \vdots \\ A_m X \end{pmatrix}.$$

В точности повторяя рассуждения §16, мы получим, что отображение

$$L^\tau : A \to \psi_A, \text{ где } \psi_A(X) = A \cdot X,$$

является изоморфизмом линейных пространств $M_{m,n}(F)$ и $L(F^n, F^m)$. Причем, если $[\varphi]^\tau = (\varphi(e_1), \ldots, \varphi(e_n))$ — матрица φ в стандартном базисе $e_1, \ldots, e_n$ пространства F^n, то повторяя некоторые рассуждения предыдущих параграфов (меняя вектор-строки на вектор-столбцы), получим, что отображение

$$[\,]^\tau : L(F^n, F^m) \to M_{m,n}(F),$$

действующее по правилу $[\,]^\tau(\phi) = [\phi]^\tau$, является изоморфизмом линейных пространств.

Теорема 1. *Пусть $\varphi \in L(F_m, F_n)$. Тогда $r([\varphi]) = \dim(Im\,\varphi)$.*

Доказательство. Заметим, что $Im\,\varphi$ порождается векторами $\varphi(e_1), \ldots, \varphi(e_m)$. Тогда, по определению,

$$[\varphi] = \begin{pmatrix} \varphi(e_1) \\ \ldots \\ \varphi(e_m) \end{pmatrix}.$$

По определению, $r([\varphi])$ совпадает с максимальным числом линейно независимых векторов среди $\varphi(e_1), \ldots, \varphi(e_m)$, т. е. совпадает с размерностью пространства $Im\,\varphi$. □

Следствие 1. *Матрица $A \in M_n(F)$ обратима $\Leftrightarrow r(A) = n$.*

Доказательство. Рассмотрим $\varphi_A \in L(F_n, F_n)$, где $\varphi_A(X) = X \cdot A$ для $X \in F_n$. По теореме 1 §18 φ_A обратимо $\Leftrightarrow [\varphi_A] = A$ — обратимая матрица.

По теореме 2 §19 φ_A обратимо $\Leftrightarrow Im\,\varphi_A = F_n$, т. е. $\dim Im\,\varphi_A = \dim F_n = n$. По теореме 1 имеем $r(A) = \dim(Im\,\varphi_A) = n$. □

Пусть V, W — векторные пространства, U — подпространство в V и $\phi \in L(V, W)$. Обозначим через $\phi_{|_U}$ отображение из U в W, действующее по правилу $\phi_{|_U}(u) = \phi(u)$. Отображение $\phi_{|_U}$ называется *ограничением отображения ϕ* на подпространство U.

Теорема 2. *Пусть $A \in M_{m,n}(F)$, $B \in M_{n,k}(F)$. Тогда*

$$r(AB) \le \min\{r(A), r(B)\}.$$

Доказательство. Приведем два доказательства: первое — на языке линейных отображений, второе — на языке матриц.

1) Пусть $\varphi : F_m \to F_n$, $\psi : F_n \to F_k$ — такие линейные отображения, что в стандартных базисах $[\varphi] = A$, $[\psi] = B$. Тогда по теореме 1 §17 $AB = [\varphi \circ \psi] = [\varphi] \cdot [\psi]$. В частности, $r(A) = \dim Im\,\varphi$, $r(B) = \dim Im\ (\psi)$, $r(AB) = \dim Im\ (\varphi \circ \psi)$. Ясно, что $Im\,(\varphi \circ \psi) \subseteq Im\,\psi$, поэтому $r(AB) \leq r(B)$.

Для доказательства второго неравенства рассмотрим отображение $\bar{\psi} = \psi|_{Im\,\varphi}$ — ограничение отображения ψ на подпространстве $Im\,\varphi$. Тогда $Im\,\bar{\psi} = Im\ (\varphi \circ \psi)$, $Ker\,\bar{\psi} = Ker\,\psi \cap Im\,\varphi$. По теореме 1 §19, $\dim Im\,\varphi = \dim Im\,\bar{\psi} + \dim Ker\,\bar{\psi} \geq \dim Im\,\bar{\psi} = \dim Im\ (\varphi \circ \psi)$ и $r(A) \geq r(AB)$.

Заметим, что второе неравенство может быть выведено из первого:

$$r(AB) = r\left((AB)^\tau\right) = r\left(B^\tau A^\tau\right) \leq r\left(A^\tau\right) = r(A).$$

2) Пусть $AB = C$, тогда

$$C_i = \sum_{k=1}^{n} a_{ik} B_k,\ C^{(j)} = \sum_{k=1}^{n} b_{kj} A^{(k)},$$

где для матрицы $A \in M_{m,n}(F)$ через A_i обозначены ее строки, а через $A^{(j)}$ — столбцы. Поэтому

$$V_\Gamma(C) \subseteq V_\Gamma(B), V_B(C) \subseteq V_B(A).$$

Следовательно, $r(AB) \leq r(B)$, $r(AB) \leq r(A)$. □

Следствие 2. *Пусть $A \in M_{m,n}(F)$. Если матрицы $B \in M_m(F)$, $C \in M_n(F)$ обратимы, то $r(BAC) = r(A)$.*

Доказательство. Имеем $r(BAC) \leq r(AC) \leq r(A) = r\left(B^{-1}(BAC)C^{-1}\right) \leq r\left(BAC \cdot C^{-1}\right) \leq r(BAC)$. □

Следствие 3. *Матрица $A \in M_n(F)$ обратима $\Leftrightarrow$ A обратима справа или слева.*

Доказательство. Действительно, из равенства $AB = E$ следует, что $n = r(E) \leq r(A)$, поэтому $r(A) = n$ и A обратима. □

§22. Элементарные преобразования матриц, эквивалентность матриц одного ранга

Для матрицы $A \in M_{m,n}(F)$ назовем *элементарным преобразованием* строк III типа умножение некоторой строки на $\lambda \in F$, $\lambda \neq 0$. Аналогично определим

преобразование для столбцов. Элементарными преобразованиями матрицы $A \in M_{m,n}(F)$ назовем элементарные преобразования строк и столбцов типа I, II, III. Назовем две матрицы одинакового порядка *эквивалентными*, если одна получена из другой элементарными преобразованиями. Из леммы 1 §20 следует, что эквивалентные матрицы имеют равные ранги. Докажем теперь обратное.

Теорема 1. *Матрицы $A, B \in M_{m,n}(F)$ эквивалентны $\Leftrightarrow$ они имеют одинаковый ранг.*

Доказательство. Мы покажем, что всякая матрица A ранга r эквивалентна матрице $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$, где E_r — единичная матрица порядка r. Действительно, элементарными преобразованиями строк A приводится к ступенчатому виду с r ненулевыми строками. Переставив, если надо, столбцы, можно считать, что первый ненулевой элемент в i-й строке $(i = 1, \ldots, r)$ стоит на i-м месте. Следующим шагом можно превратить все эти элементы в 1, а затем легко занулить все остальные элементы. □

§23. Независимость числа главных неизвестных от способа приведения системы к ступенчатому виду. Теорема Кронекера-Капелли

Рассмотрим совместную с.л.у.

$$AX = B, \tag{1}$$

где $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(F), B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in F^m,\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$

Приведем ее методом Гаусса $A \rightsquigarrow \ldots \rightsquigarrow C$ к ступенчатому виду

$$CX = D,$$

где $C = \begin{pmatrix} 0 & \cdots & 0 & c_{1k_1} & \cdots & \cdots & \cdots & \cdots & \cdots & c_{1n} \\ 0 & \cdots & \cdots & \cdots & 0 & c_{2k_2} & \cdots & \cdots & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & c_{rk_r} & \cdots & c_{rn} \end{pmatrix} \in M_{r,n}(F),$

$1 \le k_1 < \ldots < k_r \le n;\ c_{1k_1} \cdot c_{2k_2} \cdot \ldots \cdot c_{rk_r} \neq 0,\ D = \begin{pmatrix} d_1 \\ \vdots \\ d_r \end{pmatrix} \in F^r.$

В §8 были определены главные переменные $x_{k_1}, \ldots, x_{k_r}$ и свободные переменные x_i, $i \neq k_1, \ldots, k_r$, $1 \leq i \leq n$. Ввиду того, что в общем случае выбор главных переменных зависит от способа приведения $A \rightsquigarrow \ldots \rightsquigarrow C$ системы к ступенчатому виду, $x_{k_1}, \ldots, x_{k_r}$ будем называть главными переменными метода Гаусса $A \rightsquigarrow \ldots \rightsquigarrow C$. Формулы (4) из §8 определяют основное свойство переменных $x_{k_1}, \ldots, x_{k_r}$. А именно, придадим свободным переменным x_i, $1 \leq i \leq n$, $i \neq k_1, \ldots, k_r$, произвольные значения $\beta_1, \ldots, \beta_{n-r} \in F$, тогда по формулам (4) из §8, однозначно найдем единственное решение с.л.у. (1).

Переменные $x_{i_1}, \ldots, x_{i_s}$, $s \leq n$, называются *главными* в системе (1), если для любых $\beta_i \in F$, $1 \leq i \leq n$, $i \neq i_1, \ldots, i_s$, существует единственный набор $(\alpha_{i_1}, \ldots, \alpha_{i_s}) \in F_s$ такой, что

$$x_i = \begin{cases} \beta_i, \ i \neq i_1, \ldots, i_s \\ \alpha_i, \ i = i_1, \ldots, i_s \end{cases} \text{ — решение системы (1)}$$

и s максимально с этим свойством. Оставшиеся переменные назовем *свободными*.

В силу сказанного, любые главные переменные метода Гаусса являются главными. Возникают два вопроса:

— от чего зависит число главных переменных?

— какие переменные могут быть главными?

Ответы на них дает следующая теорема:

Теорема 1. *Пусть $AX = B$ — совместная система линейных уравнений и $r(A) = r$. Тогда $x_{i_1}, \ldots, x_{i_r}$ — главные переменные $\Leftrightarrow$ $A^{(i_1)}, \ldots, A^{(i_r)}$ линейно независимы. В частности, число главных переменных равно рангу системы.*

Доказательство. Перепишем с.л.у. (1) в виде

$$x_1 \cdot A^{(1)} + x_2 \cdot A^{(2)} + \ldots + x_n \cdot A^{(n)} = B.$$

Предположим, что $A^{(i_1)}, \ldots, A^{(i_r)}$ линейно зависимы. Тогда, так как $r(A) = r \leq n$, то существует j, $1 \leq j \leq n$, $j \neq i_1, \ldots, i_r$, такое, что $A^{(j)} \notin L\left(A^{(i_1)}, \ldots, A^{(i_r)}\right)$. Придадим свободным переменным следующие значения:

$x_j = 1$, а остальные свободные переменные приравняем к нулю;

$x_j = 2$, а остальные свободные переменные приравняем к нулю.

Тогда существуют $(\alpha_{i_1}, \ldots, \alpha_{i_r}) \in F^r$, $(\beta_{i_1}, \ldots, \beta_{i_r}) \in F^r$ такие, что

$$\begin{cases} \sum\limits_{k=1}^{r} \alpha_{i_k} A^{(i_k)} + A^{(j)} = B, \\ \sum\limits_{k=1}^{r} \beta_{i_k} A^{(i_k)} + 2A^{(j)} = B. \end{cases}$$

Вычитая одно равенство из другого, получим $A^{(j)} = \sum\limits_{k=1}^{r} (\beta_{i_k} - \alpha_{i_k}) A^{(i_k)}$, т. е. $A^{(j)} \in L\left(A^{(i_1)}, \ldots, A^{(i_r)}\right)$. Получено противоречие, и, следовательно, $A^{(i_1)}, \ldots, A^{(i_r)}$ линейно независимы.

Обратно, так как с.л.у. (1) совместна, то $B \in L\left(A^{(1)}, \ldots, A^{(n)}\right)$. Так как, $r(A) = r$, а $A^{(i_1)}, \ldots, A^{(i_r)}$ линейно независимы, то $A^{(i_1)}, \ldots, A^{(i_r)}$ — базис $L\left(A^{(1)}, \ldots, A^{(n)}\right)$. Следовательно, для любых $\alpha_i \in F$, $1 \leq i \leq n$, $i \neq i_1, \ldots, i_r$, вектор $(B - \sum\limits_{\substack{i \neq i_1, \ldots, i_r \\ 1 \leq i \leq n}} \alpha_i A^{(i)})$ однозначно раскладывается по базису $A^{(i_1)}, \ldots, A^{(i_r)}$. □

Теорема 2 (*Кронекера-Капелли*). *С.л.у. $AX = B$ совместна $\Leftrightarrow r(A) = r(A|B)$.*

Доказательство. Имеем $r(A) = r(A|B) \Leftrightarrow \dim L\left(A^{(1)}, \ldots, A^{(n)}\right) = \dim L\left(A^{(1)}, \ldots, A^{(n)}, B\right) \Leftrightarrow L\left(A^{(1)}, \ldots, A^{(n)}\right) = L\left(A^{(1)}, \ldots, A^{(n)}, B\right) \Leftrightarrow B \in L\left(A^{(1)}, \ldots, A^{(n)}\right) \Leftrightarrow$ существуют $\alpha_1, \ldots, \alpha_n \in F$ такие, что $\sum\limits_{i=1}^{n} \alpha_i A^{(i)} = B \Leftrightarrow (\alpha_1, \ldots, \alpha_n)$ — решение с.л.у. $AX = B$. □

§24. Однородные системы, размерность пространства решений, фундаментальная система решений

Рассмотрим однородную с.л.у.

$$AX = 0, \tag{1}$$

где $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(F)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ — столбец неизвестных.

В §9 было доказано, что $V_{\text{реш.}}$ (множество решений системы (1)) является подпространством F^n. Как найти его размерность и базис? Рассмотрим отображение $\varphi : F^n \to F^m$

$$\varphi(x) = A \cdot X.$$

Лемма 1. 1) $\varphi \in L(F^n, F^m)$. 2) $V_{\text{реш.}} = Ker\,\varphi$.

Доказательство. 1) Для любых $\alpha, \beta \in F$; $X, Y \in F^n$ имеем $\varphi(\alpha X + \beta Y) = A(\alpha X + \beta Y) = \alpha AX + \beta AY = \alpha\varphi(X) + \beta\varphi(Y)$. Следовательно, $\varphi \in L(F^n, F^m)$.

2) $Ker\,\varphi = \{X \in F^n : \varphi(X) = 0\} = \{X \in F^n : AX = 0\} = V_{\text{реш.}}$. □

Теорема 1. $\dim V_{\text{реш.}} = n - r(A)$.

Доказательство. Вычислим матрицу $[\varphi]$ в стандартном базисе $e_1, \ldots, e_n$ пространства F^n. Имеем $[\varphi]_{e_1,\ldots,e_n} = (\varphi(e_1), \ldots, \varphi(e_n)) = (A \cdot e_1, \ldots, A \cdot e_n) = \left(A^{(1)}, \ldots, A^{(n)}\right) = A$. Далее, по теореме 1 §21, $r(A) = \dim(Im\,\varphi)$. По теореме 1 §19, $n = \dim F^n = \dim Ker\,\varphi + \dim Im\,\varphi$. Поэтому $\dim V_{\text{реш.}} = n - r(A)$. □

Произвольный базис пространства $V_{\text{реш.}}$ для системы $AX = 0$ называется *фундаментальной системой* решений.

Алгоритм построения фундаментальной системы.

Пусть $r(A) = r$. Выберем произвольные главные переменные $x_{i_1}, \ldots, x_{i_r}$ для системы (1). Для простоты изложения будем обозначать главные переменные через $y_1, \ldots, y_r$, свободные переменные — через $y_{r+1}, \ldots, y_n$. Через $\bar{a} = (\alpha_1, \ldots, \alpha_n)$ будем обозначать следующее решение системы (1): $y_1 = \alpha_1, \ldots, y_r = \alpha_r, y_{r+1} = \alpha_{r+1}, \ldots, y_n = \alpha_n$. В силу формулы (4) из §8, найдем решения

$$\begin{aligned} &\bar{a}_1 = (\alpha_{11}, \ldots, \alpha_{1r}, 1, 0, \ldots, 0), \\ &- - - - - - - - - - - - - - - \\ &\bar{a}_{n-r} = (\alpha_{n-r,1}, \ldots, \alpha_{n-r,r}, 0, 0, \ldots, 1). \end{aligned}$$

По построению они линейно независимы, а так как их число равно $(n-r)$, то это базис $V_{\text{реш.}}$, и, следовательно, это фундаментальная система решений.

Теорема 2. *Всякое подпространство $V \subseteq F^n$ размерности s является пространством решений некоторой однородной системы ранга $(n-s)$.*

Доказательство. Выберем $a_1, \ldots, a_s$ — некоторый базис V, дополним его векторами $a_{s+1}, \ldots, a_n$ до базиса F^n. Пусть $U = L(a_{s+1}, \ldots, a_n)$. Тогда $F^n = V \oplus U$. Рассмотрим проекцию ψ пространства F^n на U: если $x = v + u \in F^n$, где $v \in V$, $u \in U$, то $\psi(x) := u$. Пусть $A = [\psi]$. Рассмотрим отображение $\varphi : X \mapsto AX$. Тогда $[\varphi] = A$. Следовательно, $\varphi = \psi$, и $V = Ker\,\psi = V_{\text{реш.}}$ □

§25. Линейные многообразия и решения неоднородной системы линейных уравнений

Пусть V — линейное пространство, U — подпространство в V, $a \in V$. Множество $a + U = \{a + x : x \in U\}$ называется *линейным многообразием* типа U и размерности $\dim U$. Нетрудно заметить, что $a + U$ является линейным подпространством $\Leftrightarrow a \in U$. Действительно, $0 \in a + U \Leftrightarrow a \in U \Leftrightarrow a + U = U$.

Лемма 1. *Пусть $a_1 + U_1$, $a_2 + U_2$ — линейные многообразия, тогда $a_1 + U_1 = a_2 + U_2 \Leftrightarrow U_1 = U_2$, $a_1 - a_2 \in U_1$. В частности, для любого $c \in a_1 + U_1$ верно $c + U_1 = a_1 + U_1$.*

Доказательство. "$\Rightarrow$" Существует $u_1 \in U_1$ такой, что $a_1 + u_1 = a_2 + 0 = a_2$, т. е. $a_1 - a_2 = -u_1 \in U_1$. Существует $u_2 \in U_2$, что $a_1 + 0 = a_1 = a_2 + u_2$, т. е. $a_1 - a_2 = u_2 \in U_2$. Тогда для любого $v_2 \in U_2$ существует $v_1 \in U_1$ такой, что $a_1 + v_1 = a_2 + v_2$. Следовательно, $v_2 = (a_1 - a_2) + v_1 \in U_1$ и $U_2 \subseteq U_1$. Аналогично, $U_1 \subseteq U_2$ и $U_1 = U_2$.

"$\Leftarrow$" $a_1 + U_1 = a_2 + (a_1 - a_2) + U_2 \subseteq a_2 + U_2 = a_1 + (a_2 - a_1) + U_1 \subseteq a_1 + U_1$. Следовательно, $a_1 + U_1 = a_2 + U_2$. □

Вернемся к неоднородным системам линейных уравнений. Пусть эта система имеет вид

$$AX = B. \tag{1}$$

Допустим, что система совместна, и $X_0 \in F^n$ — какое-то ее решение. Тогда $X_1 \in F^n$ — решение (1) $\Leftrightarrow (X_1 - X_0)$ — решение однородной системы $AX = 0$. Действительно, $A \cdot (X_1 - X_0) = AX_1 - AX_0 = B - B = 0$ и $0 = A \cdot (X_1 - X_0) = AX_1 - AX_0 = AX_1 - B \Rightarrow AX_1 = B$.

Теорема 1. *Множество решений системы линейных уравнений* (1) *совпадает с линейным многообразием $X_0 + V_{\text{реш.}}$, где X_0 — частное решение* (1), *$V_{\text{реш.}}$ — пространство решений системы $AX = 0$. Обратно, всякое линейное многообразие в F^n является множеством решений некоторой системы линейных уравнений от n неизвестных.*

Доказательство. Пусть Y — решение (1). Тогда $(Y - X_0) \in V_{\text{реш.}}$ и $Y \in X_0 + V_{\text{реш.}}$. С другой стороны, для любого $u \in V_{\text{реш.}}$ имеем $A(X_0 + u) = AX_0 + Au = B \Rightarrow X_0 + u$ решение (1).

Докажем обратное. Пусть подпространство V задается некоторой однородной системой $AX = 0$. Тогда многообразие $(X_0 + V)$ задается системой $AX = AX_0$. □

§26. Фактор-пространство, его базис и размерность

Пусть V — векторное пространство, $U \subseteq V$ — некоторое подпространство. Обозначим через V/U — множество всех линейных многообразий типа U в V, т. е.

$$V = \{x + U : x \in V\}.$$

Лемма 1. *Для любых $x, y \in V$ либо $x+U = y+U$ либо $(x+U)\cap(y+U) = \varnothing$.*

Доказательство. Пусть $(x+U) \cap (y+U) \neq \varnothing$ и $z \in (x+U) \cap (y+U)$. По лемме 1 §25, $z+U = x+U$ и $z+U = y+U$. Поэтому $x+U = y+U$. □

Превратим V/U в линейное пространство над F, для любых $a, b \in V$ и $\alpha \in F$ полагая

$$\begin{cases} (a+U)+(b+U) = (a+b)+U, \\ \alpha\,(a+U) = \alpha a + U. \end{cases}$$

Необходимо проверить корректность определенных операций.

Пусть $(a+U) = (a_1+U)$, тогда $(a-a_1) \in U$. Если $(b+U) = (b_1+U)$, то $(b-b_1) \in U$.

Поэтому $(a+b)-(a_1+b_1) = (a-a_1)+(b-b_1) \in U$ и, по лемме 1 §25, $(a+b)+U = (a_1+b_1)+U$. Далее, $(a-a_1) \in U \Rightarrow \alpha(a-a_1) \in U \Rightarrow \alpha a + U = \alpha a_1 + U$.

Аксиомы векторного пространства в V/U справедливы ввиду того, что они справедливы в V и операции в V/U сводятся к соответствующим операциям над элементами из V.

Теорема 1. *Отображение $\varphi : V \to V/U$, определенное по правилу $\varphi(x) = x+U$, является линейным отображением, т. е. $\varphi \in L(V, V/U)$. При этом $Ker\,\varphi = U$, $Im\,\varphi = V/U$. В частности, для конечномерных пространств $\dim V/U = \dim V - \dim U$. Пусть $v_1, \ldots, v_k$ — дополнение базиса U до базиса V. Тогда $v_1+U, \ldots, v_k+U$ — базис V/U.*

Доказательство. Для любых $\alpha, \beta \in F$, $x, y \in V$ имеем $\varphi(\alpha x + \beta y) = (\alpha x + \beta y) + U = \alpha\,(x+U) + \beta\,(y+U) = \alpha\varphi(x) + \beta\varphi(y) \Rightarrow \varphi \in L(V, V/U)$. Далее, для любого $x \in Ker\,\varphi$ имеем $\varphi(x) = x+U = 0+U \Leftrightarrow x \in U$. Следовательно, $Ker\,\varphi = U$. Докажем, что для конечномерных пространств

$$\dim V/U = \dim V - \dim U.$$

(Заметим, что это следует из теоремы 1 §19, но мы приведем явное доказательство.)

Пусть $a_1, \ldots, a_m$ — базис U. Дополним его векторами $a_{m+1}, \ldots, a_n$ до базиса V. Тогда $a_{m+1} + U, \ldots, a_n + U$ — базис V/U. Действительно,

$$\sum_{i=m+1}^{n} \alpha_i \left(a_i + U\right) = 0 + U \Rightarrow \sum_{i=m+1}^{n} \alpha_i a_i + U = 0 + U \Rightarrow \sum_{i=m+1}^{n} \alpha_i a_i \in U.$$

Поэтому $\alpha_{m+1} = \ldots = \alpha_n = 0$, т. е. $a_{m+1} + U, \ldots, a_n + U$ линейно независимы. Далее, для любого $x \in V$ существуют $\alpha_1, \ldots, \alpha_n \in F$ такие, что $x = \sum\limits_{i=1}^{n} \alpha_i a_i$. Тогда $\varphi\left(x\right) = \sum\limits_{i=m+1}^{n} \alpha_i \left(a_i + U\right)$ и $Im\, \varphi = V/U \in L\left(a_{m+1} + U, \ldots, a_n + U\right)$. Следовательно, $a_{m+1} + U, \ldots, a_n + U$ — базис V/U и $\dim V/U = n - m = \dim V - \dim U$. $\square$

§27. Определитель квадратной матрицы, его основные свойства

Индукцией по размерности n квадратной матрицы $A \in M_n(F)$ определим отображение $\det : M_n\left(F\right) \to F$, которое будем называть *детерминантом* или *определителем* A, по следующему правилу:

$$\begin{aligned} n = 1: &\quad \det\left(a\right) = a, \\ n = 2: &\quad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc. \end{aligned}$$

Предположим, что для всех квадратных матриц размера меньше n функция det определена. Рассмотрим матрицу $A \in M_n(F)$. По предположению индукции, определены числа

$$M_{ij}\left(A\right) = \det \left(\begin{array}{cc|c|cc} a_{11} & \cdots & & \cdots & a_{1n} \\ \cdots & \cdots & & \cdots & \cdots \\ \hline & & & & \\ \hline \cdots & \cdots & & \cdots & \cdots \\ a_{n1} & \cdots & & \cdots & a_{nn} \end{array}\right) \begin{array}{c} \\ \\ i\text{-строка} \\ \\ \\ \end{array}$$
$$j\text{-столбец}$$

детерминанты матриц размера $(n-1)$, полученных вычёркиванием i-строки и j-столбца матрицы A. Эти числа называются *минорами* матрицы A. Числа

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

называются *алгебраическими дополнениями.* Далее, полагаем по определению

$$\det(A) = \sum_{i=1}^{n} a_{i1} A_{i1}(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} M_{i1}(A). \qquad (1)$$

Формула (1) называется *разложением определителя* по 1-му *столбцу.*

Если ясно о какой матрице идет речь, то для краткости записывают: $M_{ij} = M_{ij}(A)$, $A_{ij} = A_{ij}(A)$, тогда

$$\det(A) = \sum_{i=1}^{n} a_{i1} A_{i1} = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} M_{i1}.$$

Функция $\det(A)$ часто обозначается через $|A|$. Аналогично определяются миноры $M_{i_1,\ldots,i_k;j_1,\ldots,j_k}(A) = M_{i_1,\ldots,i_k;j_1,\ldots,j_k}$ — определители матриц, полученных из A вычёркиванием строк с номерами $i_1, \ldots, i_k$ и столбцов с номерами $j_1, \ldots, j_k$.

Найдем по определению

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

$$= a_{11} \cdot (a_{22} \cdot a_{33} - a_{32} \cdot a_{23}) - a_{21} \cdot (a_{12} \cdot a_{33} - a_{13} \cdot a_{32}) + a_{31} \cdot (a_{12} \cdot a_{23} - a_{22} \cdot a_{13}) =$$

$$= a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{32} \cdot a_{21}$$

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

Теорема 1. *Определитель обладает следующими свойствами:*

$(D1)$ *при перестановке строк определитель меняет знак;*

$(D2)$ *при умножении какой-то строки на скаляр* $\lambda \in F$ *определитель также умножается на* λ;

$(D3)$ *определитель является линейной функцией строк матрицы* A;

$(D4)$ $|E| = 1$.

Доказательство всех этих свойств по индукции; вначале расписываем определитель по определению, затем применяем предположение индукции, и вновь сворачиваем сумму в определитель. Нужно только проследить, что происходит со слагаемыми, соответствующими тем строкам, с которыми совершается преобразование.

$(D1)$ Легко проверить, что $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = - \begin{vmatrix} c & d \\ a & b \end{vmatrix}$. Предположим, что $(D1)$ верно для матриц размера $(n-1)$. Пусть матрица B получена из $A \in M_n(F)$ перестановкой строк с номерами i и j. Тогда

$$\det(B) = \sum_{k=1}^{n} b_{k1} B_{k1} = \sum_{k=1}^{n} (-1)^{k+1} b_{k1} M_{k1}(B).$$

Для произвольной матрицы $C \in M_n(F)$ обозначим: $\hat{C}_i$ — отсутствие i-строки; $\bar{C}_i = (c_{i2}, c_{i3}, \ldots, c_{in})$ — i-строка без первого элемента. Тогда, по предложению индукции, имеем: при $k \neq i, j$

$$(-1)^{k+1} b_{k1} M_{k1}(B) = (-1)^{k+1} a_{k1} \cdot (-1) M_{k1}(A);$$

при $k = i$

$$(-1)^{i+1} b_{i1} M_{i1}(B) = (-1)^{i+1} a_{j1} \det \begin{pmatrix} \vdots \\ \widehat{\overline{A}}_j \\ \overline{A}_{i+1} \\ \vdots \\ \overline{A}_{j-1} \\ \overline{A}_i \\ \vdots \end{pmatrix} \begin{matrix} \\ \leftarrow i\text{-строка} \\ \\ \\ \\ \leftarrow j\text{-строка} \\ \\ \end{matrix}$$

$$= \left\{ \begin{array}{l} \text{последовательно переставляя строки, вернем} \\ \text{строку } \bar{A}_i \text{ с } j \text{ на } i \text{ место} \end{array} \right\} =$$

$$= (-1)^{i+1} a_{j1} \cdot (-1)^{j-i-1} \det \begin{pmatrix} \vdots \\ \widehat{\overline{A}}_j \\ \vdots \end{pmatrix} \leftarrow j\text{-строка} = -(-1)^{j+1} a_{j1} M_{j1}(A);$$

при $k = j$, аналогично,

$$(-1)^{j+1} b_{j1} \cdot M_{j1}(B) = -(-1)^{i+1} a_{i1} M_{i1}(A).$$

Следовательно, $\det(B) = -\sum\limits_{k=1}^{n} (-1)^{k+1} a_{k1} M_{k1}(A) = -\det(A)$.

$(D2)$ Легко проверить, что $\det(\lambda a) = \lambda \det(a)$, $\det \begin{pmatrix} \lambda a & \lambda b \\ c & d \end{pmatrix} = \lambda \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Предположим, что $(D2)$ верно для всех матриц размера

$(n-1)$. Пусть матрица B получена из $A \in M_n(F)$ умножением i-строки на λ. По предположению индукции, имеем: при $k \neq i$

$$(-1)^{k+1} b_{k1} M_{k1}(B) = (-1)^{k+1} a_{k1} \cdot \lambda \cdot M_{k1}(A);$$

при $k = i$

$$(-1)^{i+1} b_{i1} M_{i1}(B) = (-1)^{i+1} \lambda a_{i1} \cdot M_{i1}(A).$$

Следовательно, $\det(B) = \lambda \sum\limits_{k=1}^{n} (-1)^{k+1} a_{k1} M_{k1}(A) = \lambda \det(A)$.

$(D3)$ Докажем в начале, что

$$\det \begin{pmatrix} \vdots \\ A_i + B_i \\ \vdots \end{pmatrix} = \det \begin{pmatrix} \vdots \\ A_i \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ B_i \\ \vdots \end{pmatrix}.$$

Легко проверить, что $\det(a+b) = (a+b) = \det(a) + \det(b)$,

$$\det \begin{pmatrix} a+x & b+y \\ c & d \end{pmatrix} = (a+x) \cdot d - (b+y) \cdot c = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \det \begin{pmatrix} x & y \\ c & d \end{pmatrix}.$$

Пусть $C = \begin{pmatrix} A_1 \\ \vdots \\ A_i + B_i \\ \vdots \\ A_n \end{pmatrix}$, $D = \begin{pmatrix} A_1 \\ \vdots \\ B_i \\ \vdots \\ A_n \end{pmatrix}$, $B_i = (b_{i1}, \ldots, b_{in})$. Тогда для матрицы $C = (c_{ij})$ имеем по предположению индукции: при $k \neq i$

$$(-1)^{k+1} c_{k1} M_{k1}(C) = (-1)^{k+1} a_{k1} \det \begin{pmatrix} \vdots \\ \widehat{\overline{A_k}} \\ \vdots \\ \overline{A}_i + \overline{B}_i \\ \vdots \end{pmatrix} =$$

$$= (-1)^{k+1} a_{k1} M_{k1}(A) + (-1)^{k+1} d_{k1} M_{k1}(D);$$

при $k = i$

$$(-1)^{k+1} c_{i+1} M_{i1}(C) = (-1)^{i+1} (a_{i1} + b_{i1}) \det \begin{pmatrix} \vdots \\ \widehat{\overline{A}}_i + \widehat{\overline{B}}_i \\ \vdots \end{pmatrix} =$$

$$= (-1)^{i+1} a_{i1} M_{i1}(A) + (-1)^{i+1} d_{i1} M_{i1}(D).$$

Следовательно,

$$\det(C) = \sum_{k=1}^{n} (-1)^{k+1} c_{k1} M_{k1}(C) =$$

$$= \sum_{k=1}^{n} (-1)^{k+1} a_{k1} M_{k1}(A) + \sum_{k=1}^{n} (-1)^{k+1} d_{k1} M_{k1}(D) = \det(A) + \det(D).$$

В силу доказанного и свойства $(D2)$, имеем

$$\det \begin{pmatrix} A_1 \\ \vdots \\ \alpha A_i + \beta B_i \\ \vdots \\ A_n \end{pmatrix} = \alpha \det \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \beta \det \begin{pmatrix} A_1 \\ \vdots \\ B_i \\ \vdots \\ A_n \end{pmatrix}.$$

$(D4)$ Имеем $\det(1) = 1$, $\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$. Далее, $\det(E_n) = (-1)^{1+1} \cdot 1 \cdot \det(E_{n-1})$, где E_k — единичная матрица в $M_k(F)$. □

Следствие 1. 1) *Пусть* $1 + 1 \neq 0$ *в поле* F, *если* $A \in M_n(F)$ *содержит две одинаковые строки, то* $|A| = 0$. 2) *Если* A *содержит нулевую строку, то* $|A| = 0$. 3) $|\lambda A| = \lambda^n |A|$.

Доказательство. 1) Поменяем местами одинаковые строки. Тогда из $(D1)$ следует $\det(A) = -\det(A)$ и $\det(A) = 0$. Свойство 2) вытекает из $(D2)$ при $\lambda = 0$. Свойство 3) также следует из $(D2)$. □

§28. Определитель матрицы как полилинейная кососимметрическая нормированная функция строк матрицы

Пусть V, U — векторные пространства над полем F и $f : V^{\times n} \mapsto U$. Отображение f называется *полилинейным*, если оно линейно по каждому аргументу, т. е. для любого $i = 1, \ldots, n$ и любых $\alpha, \beta \in F$, $v_i, v_i' \in V$ имеем $f(v_1, \ldots, \alpha v_i + \beta v_i', \ldots, v_n) = \alpha f(v_1, \ldots, v_i, \ldots, v_n) + \beta f(v_1, \ldots, v_i', \ldots, v_n)$. Отображение f называется *кососимметричным*, если для любых $i, j = 1, \ldots, n$ $(i \neq j)$ имеем $f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n)$.

Лемма 1. *Пусть* $\Phi : M_n(F) \to F$ *удовлетворяет свойствам* $(D1)-(D4)$. *Тогда*

a) если матрица B *получена из* A *элементарными преобразованиями строк II типа (прибавление к одной строке другой, умноженной на скаляр), то* $\Phi(B) = \Phi(A)$;

b) если A *— верхнетреугольная, т. е.* $A = \begin{pmatrix} a_{11} & \cdots & a_n \\ & \ddots & \vdots \\ 0 & & a_{nn} \end{pmatrix}$, *то* $\Phi(A) = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}$.

Доказательство. Свойство a) вытекает из $(D3)$, $(D2)$ и следствия. Для доказательства b) заметим, что если $a_{nn} = 0$, то $\Phi(A) = 0$ в силу $(D2)$. Если же $a_{nn} \neq 0$, то можно занулить все элементы n-го столбца, стоящие над a_{nn}. После этого перейдем к a_{n-1n-1}, и т. д. Если все $a_{ii} \neq 0$, мы в итоге получим $\Phi(A) = \Phi(diag\{a_{11}, a_{22}, \ldots, a_{nn}\}) = (\text{по } (D2)) = a_{11}a_{22}\ldots a_{nn}\Phi(E) = a_{11}a_{22}\ldots a_{nn}$. □

Теорема 1. *Пусть функция* $\Phi : M_n(F) \to F$ *удовлетворяет свойствам* $(D1) - (D4)$. *Тогда* $\Phi(A) = |A|$ *для любой* $A \in M_n(F)$.

Доказательство. Приведем A к ступенчатому виду A' элементарными преобразованиями I и II типа (без умножений строк на скаляры). Пусть при этом мы совершили k перестановок строк. Тогда

$$\Phi(A) = (-1)^k \Phi(A'), |A| = (-1)^k |A'|.$$

Если в A' есть нулевая строка, то $\Phi(A') = |A'| = 0$. Иначе же A' является верхнетреугольной и снова $\Phi(A') = |A'|$ по лемме 1. □

§29. Теорема об определителе транспонированной матрицы

Теорема 1. *Для любой* $A \in M_n(F)$ *имеем* $|A| = |A^\tau|$.

Доказательство по индукции. При $n = 1, 2$ имеем $|a| = |a^\tau|$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = \begin{vmatrix} a & c \\ b & d \end{vmatrix}$. Предположим, что для любой матрицы $B \in M_k(F)$, при $k < n$, $|B| = |B^\tau|$. Обозначим элементы матрицы A^τ через a^τ_{ij}, т. е. $a^\tau_{ij} = a_{ji}$.

Пусть $A \in M_n(F)$, тогда $|A| = a_{11}A_{11} + \sum\limits_{i=2}^{n} a_{i1}A_{i1}$. Далее,

$$S := \sum_{i=2}^{n} a_{i1}A_{i1} = \sum_{i=2}^{n} (-1)^{i+1} a_{i1} M_{i1}(A) = \sum_{i=2}^{n} (-1)^{i+1} a_{i1} M_{1i}(A^\tau).$$

Теперь разложим определитель $M_{1i}(A^\tau)$ по 1-му столбцу:

$$M_{1i}(A^\tau) = \sum_{j=2}^{n} a_{1j} \cdot (-1)^j M_{1,j;i,1}(A^\tau) = \sum_{j=2}^{n} (-1)^j a_{1j} M_{1,i;1,j}(A). \qquad (*)$$

Подставив это в S, получим

$$S = \sum_{i=2}^{n}\sum_{j=2}^{n} (-1)^{i+j+1} a_{i1}a_{1j} M_{1,i;1,j}(A) =$$

$$= \sum_{j=2}^{n} (-1)^{j+1} a_{1j} \left(\sum_{i=2}^{n} (-1)^i a_{i1} M_{1,i;1,j}(A) \right) =$$

$$\overset{(*)}{=} \sum_{j=2}^{n} (-1)^{j+1} a_{1j} \left(\sum_{i=2}^{n} (-1)^i a^\tau_{1i} M_{1,j;1,i}(A^\tau) \right) = \sum_{j=2}^{n} (-1)^{j+1} a_{1j} M_{1j}(A).$$

Тогда

$$a_{11}A_{11} = (-1)^{1+1} a^\tau_{11} M_{11}(A^\tau),$$

$$S = \sum_{j=2}^{n} (-1)^{j+1} a_{1j} M_{1j}(A) = \sum_{j=2}^{n} (-1)^{j+1} a^\tau_{j1} M_{j1}(A^\tau).$$

Поэтому $|A| = \sum\limits_{j=1}^{n} (-1)^{j+1} a^\tau_{j1} M_{j1}(A^\tau) = |A^\tau|$. □

Следствие 1. *Свойства $(D1) - (D4)$ верны не только для строк, но и для столбцов матрицы A.*

Следствие 2. $|A| = \sum\limits_{i=1}^{n} a_{1i}A_{1i}$ — *разложение по первой строке.*

§30. Разложение определителя по любому столбцу. Присоединенная матрица и ее применение к нахождению обратной матрицы

Теорема 1 (*о разложении определителя по любому столбцу (строке)*).

$$|A| = \sum_{i=1}^{n} a_{ij}A_{ij} \left(= \sum_{j=1}^{n} a_{ij}A_{ij} \right).$$

Доказательство. Пусть B получена из A перестановкой 1-го и j-го столбцов. Тогда

$$|A| = -|B| = -\sum_{i=1}^{n} a_{ij} B_{i1} = -\sum_{i=1}^{n} a_{ij} (-1)^{i+1} M_{i1}(B) =$$

$$= -\sum_{i=1}^{n} a_{ij} (-1)^{i+1} (-1)^{j-2} M_{ij}(A) = -\sum_{i=1}^{n} a_{ij} (-1)^{i+j+1} M_{ij}(A) = \sum_{i=1}^{n} a_{ij} A_{ij}.$$

Аналогично для строк. □

Следствие 1.

$$\sum_{k=1}^{n} a_{ik} A_{jk} = \begin{cases} |A|, & \text{при } i = j; \\ 0, & \text{при } i \neq j. \end{cases}$$

$$\sum_{k=1}^{n} a_{ki} A_{kj} = \begin{cases} |A|, & \text{при } i = j; \\ 0, & \text{при } i \neq j. \end{cases}$$

Доказательство. Достаточно заметить, что сумма $\sum\limits_{k=1}^{n} x_{jk} A_{jk}$ равна определителю матрицы, полученной из A заменой j-ой строки строкой $X_j = (x_{j1}, \ldots, x_{jn})$. Поэтому, при $i \neq j$, $\sum\limits_{k=1}^{n} a_{ik} A_{jk} = 0$. Аналогично для столбцов.□

Матрица $A^* = (A_{ij})^\tau$ называется *присоединённой матрицей* к матрице A.

Теорема 2. *Пусть $A \in M_n(F)$. Тогда $A \cdot A^* = A^* \cdot A = \det(A) \cdot E$. В частности, если $\det(A) \neq 0$, то $A^{-1} = \frac{1}{\det(A)} \cdot A^*$.*

Доказательство. Пусть $C = A \cdot A^*$. Тогда $c_{ij} = \sum_{k=1}^{n} a_{ik} A_{jk}$ и по следствию 1 имеем

$$C = \begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} = \det(A) \cdot E.$$

Аналогично, $A^* \cdot A = \det(A) \cdot E$. □

Следствие 2. *Следующие условия для квадратной матрицы A эквивалентны:*

(i) A обратима;

(ii) строки A линейно независимы;

(iii) столбцы A линейно независимы;

(iv) $|A| \neq 0$, т. е. A невырождена.

Доказательство. Эквивалентность $(i) \sim (ii) \sim (iii)$ — это следствие 1 §21. Если строки A линейно независимы, то, как и в §28, A эквивалентна диагональной матрице без нулевых строк, т. е. $|A| \neq 0$. Из (iv) следует (i) по теореме 2. □

§31. Определитель произведения матриц

Лемма 1. *Пусть* $A = diag\{d_1, \ldots, d_n\}$, $B \in M_n(F)$. *Тогда*

$$|AB| = d_1 \cdot \ldots \cdot d_n \cdot |B| = |A|\,|B|.$$

Доказательство. Имеем $A \cdot B = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \cdot B = \begin{pmatrix} d_1 B_1 \\ \vdots \\ d_n B_n \end{pmatrix}$. Поэтому

$$|AB| = \begin{vmatrix} d_1 B_1 \\ \vdots \\ d_n B_n \end{vmatrix} \underset{(D2)}{=} d_1 \ldots d_n |B| = d_1 \ldots d_n |E|\,|B| = \begin{vmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{vmatrix} |B| = |A|\,|B|.$$ □

Лемма 2. *Пусть* $C = AB$. *Если* A' *получена из* A *каким-то элементарным преобразованием строк I и II типа, то* $C' = A'B$ *получается из* C *тем же самым элементарным преобразованием строк.*

Доказательство. $C_i = \left(A_i B^{(1)}, A_i B^{(2)}, \ldots, A_i B^{(n)}\right) = A_i \cdot B.$ □

Теорема 1. $|A \cdot B| = |A| \cdot |B|$.

Доказательство. Пусть $C = A \cdot B$. Если $r(A) < n$, то $r(AB) \leq r(A) < n$, поэтому $|A| = |A \cdot B| = 0$. Пусть $r(A) = n$, тогда A невырождена и элементарными преобразованиями строк I и II типа приводится к диагональному виду $D = diag\{d_1, \ldots, d_n\}$. Пусть при этом совершено k перестановок строк, тогда $|A| = (-1)^k |D|$. Применяя те же элементарные преобразования строк к матрице C, по лемме 2 получим матрицу $C' = DB$; при этом $|C'| = (-1)^k |C|$. По лемме 1, $|C'| = |D| \cdot |B| = (-1)^k |A| \cdot |B|$, откуда $|C| = |A| \cdot |B|$. □

§32. Формулы Крамера

Теорема 1 (*Формулы Крамера*). *Если система* n *линейных уравнений от* n *неизвестных* $A \cdot X = B$ *имеет ненулевой определитель* (*т. е.* $|A| \neq 0$), *то она определена и ее единственное решение задается формулами* $x_i = \frac{\Delta_i}{\Delta}$,

$i = 1, 2, \ldots, n$, где $\Delta = |A|$, а Δ_i получается из Δ заменой i-го столбца столбцом свободных членов.

Доказательство. Пусть $A \cdot X = B$, где

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \quad \det(A) \neq 0 \quad \text{и} \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Так как строки матрицы A линейно независимы, то по теореме 1 §4, система имеет единственное решение. Найдём его:

$$A \cdot X = B \Rightarrow X = A^{-1} \cdot B = \frac{1}{\det(A)} \cdot A^* \cdot B.$$

Имеем $A^* \cdot B = Y$, где $y_i = \sum\limits_{k=1}^{n} b_k A_{ki} = \det\left(A^{(1)} \ldots A^{(i-1)} B\, A^{(i+1)} \ldots A^{(n)}\right) = \Delta_i$.

Следовательно, $X = \left(\frac{\Delta_1}{\Delta}, \ldots, \frac{\Delta_n}{\Delta}\right)^\tau$ — решение системы. □

§33. Ранг матрицы как наибольший порядок ненулевых миноров. Теорема об окаймляющем миноре

Рангом матрицы по минорам назовем наибольший порядок ее ненулевых миноров.

Теорема 1. *Ранг матрицы равен ее рангу по минорам.*

Доказательство. Пусть r_m — ранг по минорам матрицы A, $r = r(A)$. Ясно, что $r_m \leq r$, так как строки, входящие в любой ненулевой минор, линейно независимы.

Обратно, пусть строки $A_{i_1}, \ldots, A_{i_r}$ линейно независимы. Рассмотрим матрицу A', составленную из этих r строк, тогда $r(A') = r$. Значит, существуют r линейно независимых столбцов в этой матрице: $A'^{(j_1)}, \ldots, A'^{(j_r)}$. Матрица A'', составленная из этих столбцов, принадлежит $M_r(F)$, столбцы ее линейно независимы, поэтому $|A''| \neq 0$. Но $|A''|$ — это минор r-го порядка матрицы A, стоящий на пересечении строк $A_{i_1}, \ldots, A_{i_r}$ и столбцов $A^{(j_1)}, \ldots, A^{(j_r)}$. Значит, $r_m \geq r$. □

Теорема 2 (*об окаймляющем миноре*). *Пусть все миноры порядка $k+1$, содержащие данный ненулевой минор порядка k, равны нулю. Тогда $r(A) = k$.*

Доказательство. Пусть данный минор расположен в строках $A_{i_1}, \ldots, A_{i_k}$ и столбцах $A^{(j_1)}, \ldots, A^{(j_k)}$. Столбцы $A^{(j_1)}, \ldots, A^{(j_k)}$ линейно независимы (т. к. линейно независимы "укороченные" столбцы). Пусть B — произвольный столбец матрицы A. Рассмотрим матрицу A' со столбцами $A^{(j_1)}, \ldots, A^{(j_k)}, B$. Ее строки $A'_{i_1}, \ldots, A'_{i_k}$ тоже линейно независимы. Предположим, что $r(A') = k+1$; тогда найдется строка $A'_{i_{k+1}}$ матрицы A', образующая вместе со строками $A'_{i_1}, \ldots, A'_{i_k}$ линейно независимую систему. Значит, определитель матрицы порядка $k+1$, составленной из этих строк, отличен от нуля. Но этот определитель является окаймляющим минором для исходного минора, поэтому обязан быть нулевым. Следовательно, $r(A') = k$, и столбец B линейно выражается через столбцы $A^{(j_1)}, \ldots, A^{(j_k)}$. Значит, $r(A) = k$. □

§34. Задачи

1. Найти сумму всех корней n-й степени из 1.

2. Доказать, что любой элемент из $\mathbb{C}$ является корнем квадратного или линейного уравнения с коэффициентами из $\mathbb{R}$.

3. Найти число всех упорядоченных троек (A, B, C) подмножеств множества $\bar{10} = \{1, \ldots, 10\}$ таких, что $A \cup B \cup C = \bar{10}$ и $A \cap B \cap C = \varnothing$.

4. Доказать, что для перемножения матриц 2×2 достаточно 7 умножений. (Для матриц $n \times n$ — это т.н. проблема Штрассена.)

5. Пусть $A_n \in M_{2n+1}(F)$ — кососимметрическая матрица ($A_n = -(A_n)^\tau$), у которой элементы первых n поддиагоналей равны 1, а элементы оставшихся поддиагоналей равны -1. Найти ранг A_n.

6. Пусть A — квадратная матрица порядка n. Доказать, что если $A^2 = E$, то сумма рангов матриц $A + E$ и $A - E$ равна n.

7. Доказать, что если размерность суммы двух линейных подпространств в $\mathbb{R}^n$ на единицу больше размерности их пересечения, что сумма совпадает с одним из них, а пересечение — с другим.

8. Обосновать следующий алгоритм построения *базиса суммы и пересечения* подпространств: Пусть $V = F_n$ — пространство n-строк над полем F, $L_1 = \langle a_1, \ldots, a_k \rangle$, $L_2 = \langle b_1, \ldots, b_m \rangle$. Из строк $a_1, \ldots, a_k, b_1, \ldots, b_m$ составляем матрицу A, а из строк $a_1, \ldots, a_k, 0, \ldots, 0$ составляем матрицу B. Расширенную матрицу $(A|B)$ элементарными

преобразованиями строк приводим к ступенчатому виду. Тогда ненулевые строки в левой части расширенной матрицы дают базу суммы $L_1 + L_2$, а ненулевые строки в правой части, стоящие напротив нулевых строк из левой части, дают базу $L_1 \cap L_2$.

9. Проверить, что поле вещественных чисел $\mathbb{R}$ является векторным пространством над полем рациональных чисел $\mathbb{Q}$. Доказать, что квадратные корни $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$ из простых чисел линейно независимы над $\mathbb{Q}$.

10. Проверить, что поле $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ является векторным пространством над полем рациональных чисел $\mathbb{Q}$. Найти его базис и размерность.

11. Найти максимальное значение определителя третьего порядка, у которого два элемента равны 4, а остальные 1 или -1.

12. Найти сумму всех определителей порядка n, в каждом из которых в каждой строке и в каждом столбце один элемент равен 1, а остальные нулю. Сколько всего таких определителей?

13. Пусть $A_1, \ldots, A_{n+1}$ — матрицы размера $n \times n$. Доказать, что найдутся $n+1$ чисел $x_1, \ldots, x_{n+1}$, не равные нулю одновременно, такие, что матрица $x_1A_1 + \ldots + x_{n+1}A_{n+1}$ вырождена.

14. Какую наибольшую размерность может иметь подпространство линейного пространства матриц n-го порядка, целиком состоящее из вырожденных матриц.

15. Пусть $x_1, \ldots, x_n$ — ненулевые векторы векторного пространства V, A — линейное преобразование в V такое, что $Ax_1 = x_1, Ax_k = x_k + x_{k-1},\ k = 2, \ldots, n$. Доказать, что $x_1, \ldots, x_n$ линейно независимы.

16. *Элементарными преобразованиями строк* назовем следующие: умножение строки на ненулевое число; перестановку строк; прибавление к одной строке другой. Обосновать следующий алгоритм нахождения *обратной матрицы* к матрице $A \in M_n(F)$: Расширенную матрицу $(A|E)$ элементарными преобразованиями строк приводим к виду $(E|B)$, где E — единичная матрица. Тогда $A^{-1} = B$.

17. Пусть $|AB| \neq 0$. Доказать, что если $E + AB$ обратима, то $E + BA$ обратима. Можно ли утверждать то же самое, если $|AB| = 0$?

Глава 2

Группы, кольца, поля

В этой главе мы познакомимся с такими основными алгебраическими системами как группы, кольца и поля, и докажем первые важные теоремы об этих системах.

§1. Алгебраическая операция. Алгебраическая система, подсистема, изоморфизм

Пусть X — некоторое множество, X^n — n-ая декартова степень X.

Отображение $f : X^n \to X$ называется n-арной (n-местной) *операцией* на X, т. е. f — n-арная операция, если для любых $x_1, \ldots, x_n \in X$ однозначно определен элемент $f(x_1, \ldots, x_n) \in X$. Пусть на X определены операции $f_i, i \in I$, имеющие арности $n_i, i \in I$. Обозначим через $\Omega = \{f_i, i \in I\}$ множество заданных на X операций. Система $A = \{X; \Omega\}$ называется *алгебраической системой* типа $\langle n_i, i \in I\rangle$, где X — основное множество системы, $\Omega = \{f_i, i \in I\}$ — операции на X.

Примеры. 1) $\langle \mathbb{Q}; +, \cdot\rangle$ — система типа $\langle 2, 2\rangle$.
2) $\langle \mathbb{Z}; +, \cdot, \text{Н.О.Д}(a, b, c); a, b, c \in \mathbb{Z}\rangle$ — система типа $\langle 2, 2, 3\rangle$.

Подмножество B алгебраической системы $A = \{X; f_i, i \in I\}$ типа $\langle n_i, i \in I\rangle$ называется алгебраической *подсистемой* системы A, если $f_i(b_1, \ldots, b_{n_i}) \in B$ для любого $i \in I$ и для всех $b_j \in B, j = 1, \ldots, n_i$.

Алгебраические системы $A = \{X; f_i, i \in I\}$ типа $\langle n_i, i \in I\rangle$ и $B = \{Y; g_i, i \in I\}$ такого же типа $\langle n_i, i \in I\rangle$ называются изоморфными, если существует такое взаимно однозначное соответствие $\phi : X \mapsto Y$, что для любого $i \in I$ и любых $x_1, \ldots, x_{n_i} \in X$ справедливо равенство $\phi(f_i(x_1, \ldots, x_{n_i})) = g_i(\phi(x_1), \ldots, \phi(x_{n_i}))$.

Алгебраическая система $\langle G; * \rangle$ типа $\langle 2 \rangle$ называется *группой* если выполнены следующие аксиомы:

$(G1)$ $(a * b) * c = a * (b * c)$ для любых $a, b, c \in G$;

$(G2)$ существует $e \in G$ такой, что $a * e = e * a = a$ для всех $a \in G$;

$(G3)$ для любого $a \in G$ существует $b \in G$ такой, что $a * b = b * a = e$.

Если при этом также выполняется следующая аксиома:

$(G4)$ $a * b = b * a$ для всех $a, b \in G$,

то группа называется *абелевой*.

§2. Определение и примеры полугрупп. Теорема об обобщенной ассоциативности

Пусть X — некоторое множество и f — бинарная операция на X. Напомним, что операция f называется *ассоциативной*, если $f(f(x, y), z) = f(x, f(y, z))$ для любых $x, y, z \in X$.

Аддитивная запись: $(x + y) + z = x + (y + z)$.

Мультипликативная запись: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Алгебраическая система $\langle X, f \rangle$ в этом случае называется *ассоциативной* по f.

Бинарная операция называется *коммутативной*, если $f(x, y) = f(y, x)$ для любых $x, y \in X$ ($x + y = y + x$ либо $x \cdot y = y \cdot x$, в зависимости от формы записи операции). Система $\langle X, f \rangle$ в этом случае называется *коммутативной* (или абелевой) по f.

Элемент $e \in X$ ($0 \in X$) называется *единичным* (нулевым) относительно операции $*$ (соответственно $+$), если $e * x = x * e = x$ ($0 + x = x + 0 = x$) для любого $x \in X$. Нетрудно доказать, что единичный элемент единственен: если e_1 — другая единица, то $e = e * e_1 = e_1$. Далее бинарные операции будем записывать, не дублируя форму записи.

Примеры:

- $\langle \mathbb{Z}; - \rangle$ не абелева, не ассоциативная система, так как $2 - 3 \neq 3 - 2$, $(1 - 1) - 1 \neq 1 - (1 - 1)$.
- $\langle M_n(F); + \rangle$ — ассоциативно-коммутативная система;
- $\langle M_n(F); \cdot \rangle$ — ассоциативная, но не коммутативная система:

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Пусть G — некоторое множество, $*$ — бинарная операция на G. Система $\langle G; * \rangle$ называется *группоидом*. Ассоциативный группоид называется

полугруппой, т. е. $\langle G, * \rangle$ — полугруппа, если $(a * b) * c = a * (b * c)$ для любых $a, b, c \in G$. Полугруппа с единицей называется *моноидом*, т. е. $\langle G; \cdot \rangle$ — моноид, если $(a * b) * c = a * (b * c)$ для любых $a, b, c \in G$ и существует $e \in G$ такой, что $a * e = e * a = a$ для любого $a \in G$.

Моноид, состоящий только из обратимых элементов, является *группой*.

Если $a * b = b * a = e$, то элемент b называется *обратным* к a и обозначается a^{-1} (в аддитивной записи: $-a$). Ясно, что $(a^{-1})^{-1} = a$. Нетрудно заметить, что обратный элемент определяется однозначно:

$$\begin{cases} a * b = b * a = e \\ a * b' = b' * a = e \end{cases} \Rightarrow b = e * b = (b' * a) * b = b' * (a * b) = b' * e = b'.$$

Примеры:

• $\langle \mathbb{Z}, + \rangle$ — абелева группа.

• Пусть $M(X)$ — множество всех отображений из X в X, $\circ$ — суперпозиция отображений. В силу доказанного в §17, $\langle M(X); \circ \rangle$ — моноид.

• Пусть $S(X)$ — множество всех биективных отображений X на X. Тогда $\langle S(X); \circ \rangle$ — группа (§17).

• Пусть $P(X) = \{Y : Y \subseteq X\}$ — множество всех подмножеств X. Нетрудно проверить, что $\langle P(X); \cap \rangle$, $\langle P(X); \cup \rangle$ — коммутативные полугруппы.

• $GL(n, F) = \langle A : A \in M_n(F), |A| \neq 0; \cdot \rangle$ — *полная линейная группа* степени n над F. Аксиома $(G1)$ доказана в §17; $(G2)$: $A \cdot E = E \cdot A = A$ для всех $A \in M_n(F)$, $\det(E) = 1 \neq 0$; $(G3)$: $\det(A) \neq 0 \Rightarrow A^{-1} = \frac{1}{\det(A)} \cdot A^* \in GL(n, F)$.

• $SL(n, F) = \langle \{A : A \in M_n(F), \det(A) = 1\}, \cdot \rangle$ — *специальная линейная группа* степени n над F. $(G3)$: $\det(A) = 1 \Rightarrow \det\left(A \cdot A^{-1}\right) = \det(A) \cdot \det\left(A^{-1}\right) = \det(E) \Rightarrow A^{-1} \in SL(n, F)$.

• $SL(n, \mathbb{Z}) \subseteq SL(n, \mathbb{Q}) \subseteq SL(n, \mathbb{R})$, $GL(n, \mathbb{Q}) \subseteq GL(n, \mathbb{R})$ — цепочка включений групп.

Пусть $\langle X; \cdot \rangle$ — группоид и $x_1, \ldots, x_n$ — упорядоченная последовательность элементов из X. Обозначим через e_n число всех возможных элементов X, полученных из $x_1 \cdot \ldots \cdot x_n$ различной естественной расстановкой скобок, не меняя порядка самих элементов. Например,

$e_1 = 1 : x_1$; $\quad e_2 = 1 : x_1 \cdot x_2$;

$e_3 = 2 : (x_1 \cdot x_2) \cdot x_3$, $x_1 \cdot (x_2 \cdot x_3)$, если эти элементы различны;

$e_4 = 5 : ((x_1 \cdot x_2) \cdot x_3) \cdot x_4, (x_1 \cdot (x_2 \cdot x_3)) \cdot x_4, x_1 \cdot (x_2 \cdot (x_3 \cdot x_4)), x_1 \cdot ((x_2 \cdot x_3) \cdot x_4)$, $(x_1 \cdot x_2) \cdot (x_3 \cdot x_4)$, если все эти элементы различны.

Теорема 1 (*об обобщенной ассоциативности*). *Если бинарная операция на X ассоциативна, то $e_n = 1$, т. е. результат ее последовательного применения к n элементам множества X не зависит от способа расстановки скобок.*

Доказательство. Обозначим $\prod\limits_{i=1}^{n} x_i = ((\ldots(x_1 \cdot x_2) \cdot x_3) \cdot \ldots \cdot x_{n-1}) \cdot x_n$. Докажем индукцией по n, что для любой расстановки скобок τ на $x_1, \ldots, x_n$, имеем

$$\tau(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i.$$

При $n = 1, 2$ доказывать нечего. При $n = 3$

$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3) = \prod_{i=1}^{3} x_i,$$

что следует из аксиомы ассоциативности. Пусть для любых k, $3 \le k < n$ утверждение справедливо. Тогда по предложению индукции

$$\tau(x_1, \ldots, x_n) = \tau_1(x_1, \ldots, x_i) \cdot \tau_2(x_{i+1}, \ldots, x_n) = \left(\prod_{k=1}^{i} x_k\right) \cdot \left(\prod_{k=i+1}^{n} x_k\right).$$

Если $i = n-1$, то $\tau(x_1, \ldots, x_n) = \left(\prod\limits_{k=1}^{n-1} x_k\right) \cdot x_n = \left(\prod\limits_{k=1}^{n} x_k\right)$.

Если $i < n-1$, то $\tau(x_1, \ldots, x_n) = \left(\prod\limits_{k=1}^{i} x_k\right) \cdot \left(\left(\prod\limits_{k=i+1}^{n-1} x_k\right) \cdot x_n\right) =$

$$\underset{(G1)}{=} \left(\left(\prod_{k=1}^{i} x_k\right) \cdot \left(\prod_{k=i+1}^{n-1} x_k\right)\right) \cdot x_n \underset{\text{индукция}}{=} \left(\prod_{k=1}^{n-1} x_k\right) \cdot x_n = \prod_{k=1}^{n} x_k. \qquad \square$$

§3. Подгруппы, циклические группы. Порядок элемента и порядок порождённой им циклической группы

Непустое подмножество H группы G называется *подгруппой* в G, если H — группа относительно операции группы G. Обозначается $H \le G$.

Предложение 1. *Пусть G — группа, $H \subseteq G, H \ne \varnothing$. Тогда H — подгруппа $\iff$ для любых $a, b \in H$ верно $a \cdot b^{-1} \in H$.*

Доказательство. Необходимость следует из определения подгруппы. Обратно, пусть $a \in H$. Тогда $a \cdot a^{-1} = e \in H$. Поэтому $e \cdot b^{-1} = b^{-1} \in H$

и $a \cdot \left(b^{-1}\right)^{-1} = a \cdot b \in H$ для любых $a, b \in H$. Следовательно, H — подгруппа в G. $\square$

Определим целую *степень* произвольного элемента $a \in G$, где G — группа:

$$a^n = \begin{cases} \underbrace{a \cdot \ldots \cdot a}_{n \text{ раз}}, & n \in \mathbb{N}, n > 0; \\ e, & n = 0; \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-n \text{ раз}}, & n \in \mathbb{Z}, n < 0. \end{cases} \tag{1}$$

Лемма 1. *Пусть G — группа, $a \in G$. Тогда для любых $n, m \in \mathbb{Z}$ выполняется*:

1) $a^{n+m} = a^n \cdot a^m$; 2) $(a^n)^m = a^{n \cdot m}$.

Доказательство. 1) При $n, m > 0$ либо $n = 0$, $m \in \mathbb{Z}$, $m = 0$, $n \in \mathbb{Z}$, пункт 1) следует из (1). При $n, m < 0$

$$a^{n+m} = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-(n+m) \text{ раз}} = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-n \text{ раз}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-m \text{ раз}} = a^n \cdot a^m.$$

При $n > 0$, $m < 0$

$$a^n \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{n \text{ раз}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-m \text{ раз}} = \begin{cases} a^{n-(-m)} = a^{n+m}, & \text{при } n > -m; \\ e = a^{n+m}, & \text{при } n = -m; \\ \left(a^{-1}\right)^{-m-n} = a^{n+m}, & \text{при } n < -m. \end{cases}$$

Аналогично рассматривается случай $n < 0$, $m > 0$.

2. При $m > 0$ имеем $(a^n)^m = \underbrace{a^n \cdot \ldots \cdot a^n}_{m \text{ раз}} = a^{n \cdot m}$; $(a^n)^m = e = a^{n \cdot 0} = a^{n \cdot m}$ при $m = 0$, а при $m < 0$ получаем

$$(a^n)^m = \underbrace{(a^n)^{-1} \cdot \ldots \cdot (a^n)^{-1}}_{-m \text{ раз}} = \underbrace{a^{-n} \cdot \ldots \cdot a^{-n}}_{-m \text{ раз}} = a^{-n \cdot (-m)} = a^{n \cdot m}.$$

Предложение 2. *Пусть G — группа, $a \in G$. Тогда $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$ — подгруппа в G.*

Доказательство. Элемент $a \in \langle a \rangle$, поэтому $\langle a \rangle \neq \varnothing$. Для любых $n, m \in \mathbb{Z}$ имеем $a^n \cdot a^{-m} = a^{n-m} \in \langle a \rangle$. По предложению 1, $\langle a \rangle$ — подгруппа в G. $\square$

Группа $\langle a \rangle$ называется подгруппой в G, *порождённой элементом a*. Группа G называется *циклической*, если существует $a \in G$ такой, что $G = \langle a \rangle$. Элемент a в этом случае называется *порождающим* группы G. Если группа содержит бесконечное число элементов, то она называется

бесконечной; в противном случае группа называется *конечной*, а число её элементов называется *порядком группы*.

Примеры: 1) $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle$. 2) $Z_2 = \langle \{+1, -1\}, \cdot \rangle = \langle -1 \rangle$.

Рассмотрим произвольную группу G и $a \in G$. Для элемента a возможны 2 случая:

1) $a^n \neq a^m$ для любых $n \neq m \in \mathbb{N}$. В этом случае элемент a называют элементом *бесконечного порядка* и обозначают $|a| := +\infty$.

2) $\exists n, m \in \mathbb{N},\ n \neq m : a^m = a^n \Rightarrow \exists k \in \mathbb{N} : a^k = e \Rightarrow \exists s = \min \{n \in \mathbb{N} : a^n = e\}$. В этом случае элемент a называют элементом *порядка* s и обозначают $|a| := s$.

Теорема 1. *Пусть G — группа. Тогда*

1) *для любого $a \in G$ имеем $|a| = |\langle a \rangle|$;*

2) *если $|a| = k < \infty$, то $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$;*

3) *если $m \in \mathbb{Z}$, то $a^m = e \Leftrightarrow k$ делит m.*

Доказательство. Если $|a| = +\infty$, то очевидно, что $|\langle a \rangle| = +\infty$. Пусть $|a| = k$, тогда по определению все элементы $e, a, \ldots, a^{k-1}$ различны. Далее, для любого $m \in \mathbb{Z}$ имеем $m = k \cdot p + q$, где $0 \leq q < k$. Поэтому

$$a^m = a^{(k \cdot p + q)} = \left(a^k\right)^p \cdot a^q = e^p \cdot a^q = a^q \in \left\{e, a, \ldots, a^{k-1}\right\}.$$

Следовательно, $\langle a \rangle = \left\{e, a, \ldots, a^{k-1}\right\}$. Причем, $a^m = a^q = e \Leftrightarrow q = 0$, т. е. k/m. □

§4. Симметрическая группа. Разложение подстановки на независимые циклы

Пусть X — множество из n элементов. Множество $\mathbb{S}(X)$ всех взаимно однозначных отображений множества X на X относительно операции суперпозиции отображений называется *симметрической группой* степени n и обозначается через $\mathbb{S}_n$, т. е. $\mathbb{S}_n = \langle S(X); \circ \rangle$. Для простоты изложения часто полагают $X = \{1, 2, \ldots, n\}$. Элементы $\mathbb{S}_n$ называются *подстановками*. Их принято обозначать строчными греческими буквами, тождественное отображение (или единицу в $\mathbb{S}_n$) обозначают через id.

Пусть $\tau \in \mathbb{S}_n$; $\tau(1) = i_1, \ldots, \tau(n) = i_n$. Тогда данную подстановку обозначают через $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$. Такая запись в две строки

позволяет легко перемножать подстановки:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \tau = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}, \quad \text{тогда}$$

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \cdot \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix},$$

$\sigma \cdot \tau(s) = \tau(\sigma(s)) = \tau(i_s) = j_s$; а также находить обратный элемент: если $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$, то $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

Группа $\mathbb{S}_n$ не является коммутативной:

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

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

Легко подсчитать, что $|\mathbb{S}_n| = n!$

Подстановка $\tau = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$ называется *транспозицией* и обозначается через $\tau = (ij)$. Символ i называется *действительно перемещаемым* для $\sigma \in \mathbb{S}_n$, если $\sigma(i) \neq i$. Обозначим через $D(\sigma)$ множество всех действительно перемещаемых символов для σ, т. е. $D(\sigma) = \{i : \sigma(i) \neq i, 1 \leq i \leq n\}$.

Подстановка σ называется *циклом* длины k, если

$$D(\sigma) = \left\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\right\},$$

где $\sigma^k(i) = i$ и обозначается $\sigma = (i_1 i_2 \ldots i_k)$, где $i_1 = i$, $i_2 = \sigma(i), \ldots, i_k = \sigma^{k-1}(i)$, т. е.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & i_1 & \cdots & i_2 & \cdots & i_k & \cdots & n \\ 1 & 2 & \cdots & i_2 & \cdots & i_3 & \cdots & i_1 & \cdots & n \end{pmatrix}.$$

Очевидно, что $\sigma^k = id$ и $(i_1, \ldots, i_k) = (i_s, \ldots, i_k, i_1, \ldots, i_{s-1})$ для любого $s = 2, \ldots, k$.

Предложение 1. *Для любой подстановки $\sigma \in \mathbb{S}_n$ справедливо*:
1) $D(\sigma) = \varnothing \Leftrightarrow \sigma = id$;
2) $i \notin D(\sigma) \Leftrightarrow \sigma(i) \notin D(\sigma) \Leftrightarrow \sigma^{-1}(i) \notin D(\sigma)$;
3) $i \in D(\sigma) \Leftrightarrow \sigma(i) \in D(\sigma) \Leftrightarrow \sigma^{-1}(i) \in D(\sigma)$;

4) *если* $i \in D(\sigma)$, *то существует* $k \in \mathbb{N}$ *такое, что* $i, \sigma(i), \ldots, \sigma^{k-1}(i)$ *различные,* $\sigma^k(i) = i$; *если* $j \in \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$, *то* $\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\} = \{j, \sigma(j), \ldots, \sigma^{k-1}(j)\}$ *и* $\sigma^k(j) = j$.

Доказательство. 1) Очевидно. 2) Действительно, если $i \notin D(\sigma)$, то $\sigma(i) = i$ и $\sigma^{-1}(i) = i$. 3) Следует из 2). 4) В силу свойства 3), существуют $s > t > 0 : \sigma^s(i) = \sigma^t(i) \Rightarrow \sigma^{s-t}(i) = i$. Пусть $k = \min\{s \in \mathbb{N} : \sigma^s(i) = i\}$. Тогда очевидно, что $\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ — различные и $\sigma^k(i) = i$. Так как σ — взаимно однозначное отображение, то для любого $j \in \{i, \ldots, \sigma^{k-1}(i)\}$ имеем: $\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\} = \{j, \sigma(j), \ldots, \sigma^{k-1}(j)\}$ и $\sigma^k(j) = j$. □

Подстановки σ и τ называются *независимыми*, если $D(\sigma) \cap D(\tau) = \varnothing$.

Лемма 1. *Если* σ *и* τ *— независимые подстановки, то* $\sigma \cdot \tau = \tau \cdot \sigma$.

Доказательство. Пусть $i \notin D(\sigma) \cup D(\tau)$. Тогда $\sigma \cdot \tau(i) = \tau(\sigma(i)) = i = \tau \cdot \sigma(i)$. Если $i \in D(\sigma)$, то $i \notin D(\tau)$. Тогда $\sigma(i) \in D(\sigma)$, $\sigma(i) \notin D(\tau)$ и $\tau(i) = i$. Поэтому $\sigma \cdot \tau(i) = \tau(\sigma(i)) = \sigma(i)$, $\tau \cdot \sigma(i) = \sigma(\tau(i)) = \sigma(i)$. Аналогично рассматривается случай $i \notin D(\sigma)$ и $i \in D(\tau)$. Поэтому для любого i, $1 \le i \le n$, $\sigma \cdot \tau(i) = \tau \cdot \sigma(i) \Rightarrow \tau \cdot \sigma = \sigma \cdot \tau$. □

Теорема 1. *Каждая не единичная подстановка есть произведение попарно независимых циклов. Это разложение однозначно с точностью до перестановки.*

Доказательство. Докажем существование такого разложения. Так как $D(\tau) \neq \varnothing$, то, в силу 4) Предложения 1, множество $D(\tau)$ можно представить в виде

$$D(\tau) = \bigcup_{p=1}^{k} \{i_p, \tau(i_p), \ldots, \tau^{s_p-1}(i_p)\},$$

где для любого p, $1 \le p \le k$, $i_p, \tau(i_p), \ldots, \tau^{s_p-1}(i_p)$ различны, $\tau^{s_p}(i_p) = i_p$ и, при $p \neq q$,

$$\{i_p, \tau(i_p), \ldots, \tau^{s_p-1}(i_p)\} \cap \{i_q, \tau(i_q), \ldots, \tau^{s_q-1}(i_q)\} = \varnothing.$$

Обозначим $\sigma_p = \left(i_p \tau(i_p) \ldots \tau^{s_p-1}(i_p)\right)$, $p = 1, \ldots, k$. Тогда $\tau = \sigma_1 \cdot \ldots \cdot \sigma_k$ — искомое разложение. Действительно, $D(\tau) = \bigcup\limits_{p=1}^{k} D(\sigma_p)$ и для любого $i \in D(\tau)$ существует единственное p, $1 \le p \le k$, такое, что $i \in D(\sigma_p)$. Поэтому $\tau(i) = \sigma_1 \cdot \ldots \cdot \sigma_k(i) = \sigma_p(i)$. Докажем единственность разложения. Пусть $\tau = \sigma_1 \cdot \ldots \cdot \sigma_k = \tau_1 \cdot \ldots \cdot \tau_m$ — два разложения в произведение попарно независимых циклов. Тогда для любого $i \in D(\tau)$ существуют единственные σ_p и τ_s такие, что $i \in D(\sigma_p)$ и $i \in D(\tau_s)$. Поэтому $\tau(i) = \sigma_p(i) = \tau_s(i)$ и,

в силу свойства 2) Предложения 1, $\sigma_p(i) \in D(\sigma_p)$ и $\tau_s(i) \in D(\tau_s)$. Поэтому $\tau^2(i) = \sigma_p^2(i) = \tau_s^2(i)$, где $\sigma_p^2(i) \in D(\sigma_p)$ и $\tau_s^2(i) \in D(\tau_s)$. Продолжая так далее, для любого $k \in \mathbb{N}$ имеем $\tau^k(i) = \sigma_p^k(i) = \tau_s^k(i)$. Следовательно, $\sigma_p = \tau_s$ и $\sigma_1 \cdot \ldots \cdot \hat{\sigma}_p \cdot \ldots \cdot \sigma_k = \tau_1 \cdot \ldots \cdot \hat{\tau}_s \cdot \ldots \cdot \tau_m$. Продолжая этот процесс, за конечное число шагов получим $k = m$ и $\sigma_i = \tau_i$ с точностью до перестановки циклов. □

§5. Разложение подстановки в произведение транспозиций, независимость чётности числа сомножителей от способа разложения. Знакопеременная группа, ее порядок

Докажем, что любую подстановку можно представить в виде произведения транспозиций.

Лемма 1. *Для любой подстановки $\sigma \in \mathbb{S}_n$ существуют транспозиции $\tau_1, \ldots, \tau_k$ такие, что $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$.*

Доказательство. Если $\sigma = id$, то $\sigma = (12)^2$. Если $\sigma \neq id$, то, по теореме 1 §4, представим $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m$, где σ_i — попарно независимые циклы. Далее, любой цикл $(i_1 i_2 \ldots i_s)$ легко представить в виде произведения транспозиций $(i_1 i_2 \ldots i_s) = (i_1 i_2) \cdot (i_1 i_3) \cdot \ldots \cdot (i_1 i_s)$. □

Нетрудно заметить, что представление в виде произведения транспозиций неоднозначно: если $\sigma \in S_n$, то $\sigma = (12) \cdot (12) \cdot \sigma$.

Пусть $id \neq \sigma \in S_n$ и $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_k$ — разложение в произведение попарно независимых циклов. Число

$$N(\sigma) = |D(\sigma)| - k = \sum_{i=1}^{k} \left(\begin{array}{c} \text{длина } i\text{-цикла} \\ \text{в разложении} \end{array} \right) - k$$

называется *декрементом* подстановки $\sigma \in S_n$. Декремент тождественной подстановки по определению полагают равным нулю, то есть $N(id) = 0$.

Лемма 2. *Пусть $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$, где τ_i — транспозиции, тогда $k \equiv N(\sigma) \pmod 2$, то есть чётность числа транспозиций в разложении любой подстановки совпадает с чётностью ее декремента.*

Доказательство. Найдём, как меняется декремент подстановки σ при умножении её на транспозицию. Если $\sigma = id$, то $(ij)\sigma = (ij)id = (ij)$ и $N((ij)\sigma) = 2 - 1 = N(\sigma) + 1$. Пусть $\sigma \neq id$. Разложим σ в произведение

независимых циклов $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_\ell$. Подсчитаем $N((ij)\sigma)$. Рассмотрим все возможные случаи:

1) $i, j \notin D(\sigma)$. Тогда $(ij)\sigma_1 \cdot \ldots \cdot \sigma_\ell$ — произведение независимых циклов и

$$N((ij)\sigma) = D(\sigma) + 2 - (\ell + 1) = D(\sigma) - \ell + 1 = N(\sigma) + 1.$$

2) $i \in D(\sigma)$ и $j \notin D(\sigma)$. Пусть i входит в цикл $(ii_1 \ldots i_k)$, тогда $(ij)(ii_1 \ldots i_k) = (iji_1 \ldots i_k)$. Так как независимые циклы перестановочны, считаем, что $i \in D(\sigma_1)$. Поэтому $N((ij)\sigma) = N((iji_1 \ldots i_k) \cdot \sigma_2 \cdot \ldots \cdot \sigma_\ell) = D(\sigma) + 1 - \ell = D(\sigma) - \ell + 1 = N(\sigma) + 1$.

3) Аналогично рассматривается случай $i \notin D(\sigma)$ и $j \in D(\sigma)$.

4) $i, j \in D(\sigma)$ и входят в один цикл. С точностью до перестановки независимых циклов считаем, что $i, j \in D(\sigma_1)$. Тогда, если $\sigma_1 = (ii_1 \ldots i_k j j_1 \ldots j_s)$ и $\{i_1 \ldots i_k\} \neq \varnothing$, то

$$(ij)(ii_1 \ldots i_k j j_1 \ldots j_s) = (ij_1 j_2 \ldots j_s) \cdot (ji_1 \ldots i_k).$$

Поэтому $N((ij)\sigma) = N((ij_1 \ldots j_s) \cdot (ji_1 \ldots i_k) \cdot \sigma_2 \cdot \ldots \cdot \sigma_\ell) =$

$$= D(\sigma) - (\ell + 1) = D(\sigma) - \ell - 1 = N(\sigma) - 1.$$

Случай, когда $\{i_1 \ldots i_k\} = \varnothing$, разбирается аналогично.

5) $i, j \in D(\sigma)$ и входят в два различных цикла. С точностью до перестановки, считаем, что $i \in D(\sigma_1)$ и $j \in D(\sigma_2)$. Тогда

$$(ij)(ii_1 \ldots i_k)(jj_1 \ldots j_s) = (ij_1 \ldots j_s j i_1 \ldots i_k).$$

Поэтому $N((ij)\sigma) = N((ij_1 \ldots j_s j i_1 \ldots i_k) \cdot \sigma_3 \cdot \ldots \cdot \sigma_\ell) =$

$$= D(\sigma) - (\ell - 1) = D(\sigma) - \ell + 1 = N(\sigma) + 1.$$

Таким образом, для любой $\sigma \in S_n$ и транспозиции τ имеем $N(\tau \cdot \sigma) = N(\sigma) \pm 1$ и $N(\tau \cdot \sigma) \equiv 1 + N(\sigma)\ (mod\, 2)$. Пусть $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$ — разложение σ в произведение транспозиций, тогда

$$N(\sigma) = N(\tau_1 \cdot \ldots \cdot \tau_k) \equiv 1 + N(\tau_2 \cdot \ldots \cdot \tau_k)\,(\mathrm{mod}2) \equiv$$

$$\equiv 2 + N(\tau_3 \cdot \ldots \cdot \tau_k)\,(\mathrm{mod}2) \equiv \ldots \equiv (k-1) + N(\tau_k)\,(\mathrm{mod}2) \equiv k(\mathrm{mod}2). \quad \square$$

Для подстановки $\pi \in \mathbb{S}_n$ число $Sg(\pi) = (-1)^{N(\pi)}$ называется *знаком* подстановки π.

Теорема 1. *Пусть $\pi \in \mathbb{S}_n$ и $\pi = \pi_1 \cdot \ldots \cdot \pi_k$ — разложение в произведение транспозиций, тогда*

1) *чётность числа k не зависит от способа разложения π в произведение транспозиций*;

2) $Sg(\pi) = (-1)^k$;

3) $Sg(\sigma \cdot \pi) = Sg(\sigma) \cdot Sg(\pi)$ *для любых* $\sigma, \pi \in S_n$.

Доказательство. 1) В силу леммы 1, чётность числа k совпадает с чётностью декремента. 2) В силу леммы 1, $k \equiv N(\pi) \pmod 2 \Rightarrow Sg(\pi) = (-1)^{N(\pi)} = (-1)^k$.

3) Пусть $\sigma = \tau_1 \cdot \ldots \cdot \tau_\ell$ — разложение в произведение транспозиций, тогда $Sg(\sigma \cdot \pi) = (-1)^{\ell+k} = (-1)^\ell \cdot (-1)^k = Sg(\sigma) \cdot Sg(\pi)$. □

Подстановка $\sigma \in \mathbb{S}_n$ называется *чётной*, если $Sg(\sigma) = +1$ и *нечётной*, если $Sg(\sigma) = -1$.

Теорема 2. $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n : Sg(\sigma) = +1\}$ *является подгруппой в* $\mathbb{S}_n$ *и* $|\mathbb{A}_n| = \frac{n!}{2}$.

Доказательство. Подстановка $id \in \mathbb{A}_n$, так как $Sg(id) = +1$. Пусть $\sigma, \tau \in \mathbb{A}_n$, тогда $Sg(\sigma \cdot \tau) = Sg(\sigma) \cdot Sg(\tau) = +1$ и $\sigma \cdot \tau \in \mathbb{A}_n$. Пусть $\sigma \in \mathbb{A}_n$ и $\sigma = \tau_1 \cdot \ldots \cdot \tau_{2k}$ — разложение в произведение транспозиций. Нетрудно заметить, что $\sigma^{-1} = \tau_{2k} \cdot \ldots \cdot \tau_1$ и $\sigma^{-1} \in \mathbb{A}_n$. По предложению 1 из §3, $\mathbb{A}_n$ — подгруппа $\mathbb{S}_n$.

Пусть B_n — множество всех нечётных подстановок из $\mathbb{S}_n$. Тогда $(12)\mathbb{A}_n := \{(12)\sigma : \sigma \in \mathbb{A}_n\}$ — множество, состоящее из различных нечётных подставок, $(12)B_n := \{(12)\sigma : \sigma \in B_n\}$ — множество, состоящее из различных чётных подстановок. Поэтому $|\mathbb{A}_n| \le |B_n| \le |\mathbb{A}_n|$. Следовательно, $|\mathbb{A}_n| = |B_n| = \frac{1}{2}|\mathbb{S}_n|$. □

Группа $\mathbb{A}_n$ называется *знакопеременной группой.*

§6. Теорема о полном развертывании определителя

Теорема 1. *Для любой* $A \in M_n(F)$ *справедливо равенство*

$$\det(A) = \sum_{\sigma \in \mathbb{S}_n} Sg(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}.$$

Доказательство. В силу теоремы 1 из §1.25, определитель $|A|$ есть полилинейная кососимметрическая нормированная функция D строк матрицы A, т. е. $|A| = D(A_1, \ldots, A_n)$, где A_i — i-строка матрицы A.

Разложим $A_1, \ldots, A_n$ по стандартному базису $\{e_1, \ldots, e_n\}$ пространства F_n:

$$A_i = \sum_{j=1}^{n} a_{ij} e_j, \quad i = 1, \ldots, n.$$

Тогда $\det(A) = D\left(\sum\limits_{i_1=1}^{n} a_{1i_1} e_{i_1}, A_2, \ldots, A_n\right) = \sum\limits_{i_1=1}^{n} a_{1i_1} D(e_{i_1}, A_2, \ldots, A_n) = \ldots$

$$= \sum_{i_1=1}^{n} \ldots \sum_{i_n=1}^{n} a_{1i_1} a_{2i_2} \ldots a_{ni_n} D(e_{i_1}, e_{i_2}, \ldots, e_{i_n}) =$$

$$= \sum_{i_1=1, i_2=1, \ldots, i_n=1}^{n} a_{1i_1} a_{2i_2} \ldots a_{ni_n} D(e_{i_1}, e_{i_2}, \ldots, e_{i_n}).$$

В силу кососимметричности функции D, имеем $D(\ldots, e_i, \ldots, e_i, \ldots) = 0$. Поэтому

$$\det(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} D\left(e_{\sigma(1)}, \ldots, e_{\sigma(n)}\right).$$

Найдём число $D\left(e_{\sigma(1)}, \ldots, e_{\sigma(n)}\right)$. Заметим, что, в силу кососимметричности D, для любой транспозиции $\tau \in \mathbb{S}_n$ и для любых различных $i_1, \ldots, i_n$ имеем

$$D\left(e_{\tau(i_1)}, \ldots, e_{\tau(i_n)}\right) = -D(e_{i_1}, \ldots, e_{i_n}).$$

Разложим σ в произведение транспозиций: $\sigma = \tau_1 \cdot \ldots \cdot \tau_k$. Тогда

$$D\left(e_{\sigma(1)}, \ldots, e_{\sigma(n)}\right) = D\left(e_{\tau_k(\tau_{k-1}(\ldots\tau_1(1)\ldots))}, \ldots, e_{\tau_k(\tau_{k-1}(\ldots\tau_1(n)\ldots))}\right) =$$

$$-D\left(e_{\tau_1\cdot\ldots\cdot\tau_{k-1}(1)}, \ldots, e_{\tau_1\cdot\ldots\cdot\tau_{k-1}(n)}\right) = (-1)^2 D\left(e_{\tau_1\cdot\ldots\cdot\tau_{k-2}(1)}, \ldots, e_{\tau_1\cdot\ldots\cdot\tau_{k-2}(n)}\right) =$$

$$= \ldots = (-1)^k D(e_1, \ldots, e_n) = Sg(\sigma).$$

Следовательно, $\det(A) = \sum\limits_{\sigma \in \mathbb{S}_n} Sg(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$. □

§7. Изоморфизм групп, теорема Кэли

Рассмотрим две группы G и G' с операциями $*$ и $\circ$. Отображение $f : G \to G'$ называется *гомоморфизмом*, если f сохраняет операцию, то есть для любых $a, b \in G$

$$f(a * b) = f(a) \circ f(b).$$

Гомоморфизм f называется *эпиморфизмом*, если отображение f сюръективное (отображение на), гомоморфизм f называется *изоморфизмом*, если отображение f биективно. В этом случае группы G и G' называются *изоморфными* и это обозначается $G \simeq G'$.

Простейшие свойства гомоморфизмов. Пусть $f : G \to G'$ гомоморфизм, тогда

1) $f(e) = e'$ (e' — единица в G').

Действительно, $a*e = e*a = a$. Следовательно, $f(a) \circ f(e) = f(e) \circ f(a) = f(a)$, и потому $f(e) = e'$.

2) $(f(g))^{-1} = f\left(g^{-1}\right)$ для любого $g \in G$.

Действительно,

$$f(g) \circ f\left(g^{-1}\right) = f\left(g * g^{-1}\right) = f(e) = f\left(g^{-1} * g\right) = f\left(g^{-1}\right) \circ f(g) = e' \Rightarrow$$

$$f^{-1}(g) = f\left(g^{-1}\right);$$

3) Пусть f — изоморфизм, тогда f^{-1} — изоморфизм G' и G.

Действительно, f^{-1} существует, так как f биективно. Далее, пусть $f^{-1}(a') = a, f^{-1}(b') = b$ для любых $a', b' \in G'$. Тогда $a' = f(a)$, $b' = f(b)$. Следовательно,

$$a' \circ b' = f(a) \circ f(b) = f(a * b) \Rightarrow f^{-1}(a' \circ b') = a * b = f^{-1}(a') * f^{-1}(b').$$

Множество $Ker\, f = \{g \in G : f(g) = e'\}$ называется *ядром* гомоморфизма $f : G \to G'$.

Лемма 1. $Ker\, f \leq G$, $Im\, f \leq G'$.

Доказательство. По свойству 1) $e \in Ker\, f$, следовательно, $Ker\, f \neq \varnothing$. Далее, для любых $a, b \in Ker\, f$ имеем $f\left(a * b^{-1}\right) = f(a) \circ f\left(b^{-1}\right) = e' \circ (f(b))^{-1} = e'$, откуда $a * b^{-1} \in Ker\, f$. По предложению 1 из §3, $Ker\, f \leq G$.

По свойству 1) $e' \in Im\, f$, следовательно, $Im\, f \neq \varnothing$. Для любых $a', b' \in Imf$ существуют $a, b \in G$ такие, что $f(a) = a'$, $f(b) = b'$. Тогда

$$f\left(a * b^{-1}\right) = f(a) \circ f\left(b^{-1}\right) = a' \circ (b')^{-1} \Rightarrow a' \circ (b')^{-1} \in Imf \Rightarrow Imf \leq G'. \quad \square$$

Докажем, что изоморфизм определяет отношение эквивалентности на множестве всех групп.

1. Для любой группы G имеем $G \approx G$.

Тождественное отображение $id : G \to G$, очевидно, является изоморфизмом.

2. Для любых групп G, G' имеем $G \simeq G' \Leftrightarrow G' \simeq G$.

Если $f : G \to G'$ — изоморфизм, то, по свойству 3), $f^{-1} : G'$ — изоморфизм.

3. Для любых групп G_1, G_2, G_3 имеем $G_1 \simeq G_2$, $G_2 \simeq G_3 \Rightarrow G_1 \simeq G_3$.

Если $f : G_1 \to G_2$, $f_2 : G_2 \to G_3$ — изоморфизмы, то $f_1 \circ f_2 : G_1 \to G_3$ — биективное отображение и для любых $a, b \in G_1$ имеем

$$(f_1 \circ f_2)(a *_1 b) = f_2(f_1(a *_1 b)) = f_2(f_1(a) *_2 f_1(b)) =$$

$$= f_2(f_1(a)) *_3 f_2(f_1(b)) = (f_1 \circ f_2)(a) *_3 (f_1 \circ f_2)(b),$$

где $*_i$ — операция в группе G_i. Таким образом, $f_1 \circ f_2 : G_1 \to G_3$ — гомоморфизм и $G_1 \simeq G_3$.

В силу теоремы 1 из §5, множество всех групп распадается на классы изоморфных групп. С точки зрения алгебры естественно изучать неизоморфные объекты.

Лемма 2. *Все циклические группы одного порядка изоморфны.*

Доказательство. Пусть G — циклическая группа.

1) Пусть G — бесконечная группа. Тогда $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. Рассмотрим бесконечную циклическую группу $\mathbb{Z} = \langle \mathbb{Z}; + \rangle$ и отображение $\varphi : G \to \mathbb{Z}$ определённое правилом: $\varphi(a^n) = n$ для любого $n \in \mathbb{Z}$. Очевидно, что φ биективно и для любых $n, m \in \mathbb{Z}$ имеем

$$\varphi(a^n \cdot a^m) = \varphi\left(a^{n+m}\right) = n + m = \varphi(a^n) + \varphi(a^m).$$

Следовательно, φ — изоморфизм и $G \simeq \mathbb{Z}$.

2) Пусть $G = \left\{e, a, \ldots, a^{n-1}\right\}$ и $G' = \left\{e', b, \ldots, b^{n-1}\right\}$ — циклические группы порядка n, т. е. $G = \langle a \rangle$, $|a| = n$; $G' = \langle b \rangle$, $|b| = n$. Пусть $\varphi : G \to G'$ такое, что $\varphi(a^k) = b^k$ для всех $0 \leq k \leq n-1$. Тогда φ биективно и для любых $a^m, a^k \in G$ имеем $\varphi\left(a^m \cdot a^k\right) = \varphi(a^r)$, где r — остаток от деления $m + k$ на n, т. е. $(m + k) = n \cdot q + r$. Тогда $\varphi\left(a^m \cdot a^k\right) = \varphi\left(a^{m+k}\right) = \varphi(a^r) = b^r = e' \cdot b^r = (b^n)^q \cdot b^r = b^{nq+r} = b^{m+k} = b^m \cdot b^k = \varphi(a^m) \cdot \varphi\left(a^k\right)$. Следовательно, $G \simeq G'$. □

Следующая теорема показывает, что все конечные группы с точностью до изоморфизма являются подгруппами в $\mathbb{S}_n$.

Теорема 1 (*Кэли*). *Любая конечная группа порядка n изоморфна некоторой подгруппе группы $\mathbb{S}_n$.*

Доказательство. Пусть G — группа порядка n и $\mathbb{S}_n$ — группа биективных отображений G на G относительно суперпозиции, т. е. $\mathbb{S}_n = \langle S(G); \circ \rangle$. Для любого $g \in G$ определим отображение $T_g : G \to G$ по правилу $T_g(a) = a \cdot g$ для любого $a \in G$.

Докажем, что $T_g \in S(G)$, т. е. T_g является биективным.

Для любого $b \in G$ имеем $T_g\left(b \cdot g^{-1}\right) = b \cdot g^{-1} \cdot g = b \Rightarrow T_g$ сюръективно.

Для любых $a, b \in G$ имеем $T_g(a) = T_g(b) \Rightarrow a \cdot g = b \cdot g \Rightarrow a = b \Rightarrow T_g$ инъективно и $T_g \in S(G)$.

Так как $a \cdot e = a$ для любого $a \in G$, то $T_e = id$. Поэтому $T_g \circ T_{g^{-1}}(a) = T_{g^{-1}}(T_g(a)) = (a \cdot g) \cdot g^{-1} = a \cdot e = a = T_e(a)$ для любого $g \in G$. Следовательно, $T_g^{-1} = T_{g^{-1}}$ для любого $g \in G$.

Рассмотрим множество H всех отображений T_g, $g \in G$. Докажем, что $H = \{T_g : g \in G\} \leq \mathbb{S}_n$. Действительно, $id = T_e \in H \Rightarrow H \neq \varnothing$. Далее, для любых $T_a, T_b \in H$ и $c \in G$ имеем

$$\left(T_a \circ T_b^{-1}\right)(c) = T_{b^{-1}}(T_a(c)) = (c \cdot a) \cdot b^{-1} = c \cdot \left(a \cdot b^{-1}\right) = T_{a \cdot b^{-1}}(c).$$

Следовательно, $T_a \circ T_b^{-1} = T_{a \cdot b^{-1}} \in H$ и по предложению 1 из §3 имеем $H \leq S_n$.

Рассмотрим отображение $\varphi : G \to H$, определённое по правилу $\varphi(g) = T_g$. Докажем, что φ — изоморфизм. По определению, φ сюръективно. Пусть $\varphi(a) = \varphi(b) \Rightarrow T_a = T_b$. Тогда для любого $x \in G$ справедливо

$$T_a(x) = x \cdot a = T_b(x) = x \cdot b \Rightarrow a = b \Rightarrow T_a = T_b.$$

Таким образом, φ инъективно. Далее, для любых $g_1, g_2 \in G$ имеем $\varphi(g_1 \cdot g_2) = T_{g_1 \cdot g_2}$. Для любого $x \in G$ имеем $T_{g_1 \cdot g_2}(x) = x \cdot (g_1 \cdot g_2) = (x \cdot g_1) \cdot g_2 = (T_{g_1} \circ T_{g_2})(x) \Rightarrow T_{g_1 \cdot g_2} = T_{g_1} \circ T_{g_2}$. Поэтому $\varphi(g_1 \cdot g_2) = T_{g_1 \cdot g_2} = T_{g_1} \circ T_{g_2} = \varphi(g_1) \circ \varphi(g_2)$. Следовательно, φ — изоморфизм и $G \simeq H$. □

§8. Смежные классы по подгруппе. Теорема Лагранжа

Рассмотрим подгруппу H группы G.

Определение. Множество $gH = \{gh : h \in H\}$, где $g \in G$, называется *левым смежным классом* группы G по подгруппе H, элемент g называют *представителем* этого класса.

Лемма 1. *$H, K \leq G$. Тогда $gH = g_1K \Leftrightarrow H = K$, $g^{-1} \cdot g_1 \in H$.*

Доказательство. “$\Rightarrow$” Существует $k \in K$ такой, что $g \cdot e = g = g_1 \cdot k \Rightarrow g_1^{-1} \cdot g = k \in K$ и аналогично $g^{-1} \cdot g_1 \in H$. Тогда для любого $h \in H$ существует $k \in K$ такой, что $g \cdot h = g_1 \cdot k \Rightarrow h = g^{-1} \cdot g_1 \cdot k = \left(g_1^{-1} \cdot g\right)^{-1} \cdot k \in K$. Поэтому $H \subseteq K$. Аналогично доказываем, что $K \subseteq H$. Следовательно, $K = H$.

“$\Leftarrow$” $gH = g_1 \cdot \left(g_1^{-1} \cdot g\right) \cdot H = g_1 \cdot \left(g \cdot g_1^{-1}\right)^{-1} \cdot H \subseteq g_1H$, аналогично $g_1H \subseteq gH$. Поэтому $g_1H = gH$. □

Следствие 1. *Два левых смежных класса G по H либо совпадают, либо не пересекаются.*

Доказательство. Если $gH \cap g_1H \neq \varnothing$, то $\exists a \in gH \cap g_1H \Rightarrow \exists h, h_1 \in H : g \cdot h = g_1 \cdot h_1 \Rightarrow g^{-1} \cdot g_1 = h \cdot h_1^{-1} \in H \Rightarrow gH = g_1H$. □

Теорема 1 (*Лагранж*). *Порядок конечной группы G делится на порядок любой её подгруппы H.*

Доказательство. Очевидно, что $g \in gH$ для любого $g \in G$. Поэтому $G = \bigcup\limits_{g \in G} gH$. В силу следствия 1, можно выбрать все различные смежные классы $g_1H, \ldots, g_kH$, где $g_iH \cap g_jH = \varnothing$ при $i \neq j$ и $G = \bigcup\limits_{i=1}^{k} g_iH$. Докажем, что $|g_iH| = |H|$. Действительно, если $g_i \cdot h_1 = g_i \cdot h_2$, то $h_1 = h_2$. Следовательно, $|G| = \sum\limits_{i=1}^{k} |g_i \cdot H| = k \cdot |H|$. □

Множество всех различных левых смежных классов обозначается через $(G/H)_l$. Их число называется (*левым*) *индексом* H в G и обозначается через $(G : H)_l$.

Таким образом, теорему Лагранжа можно записать следующим образом:

$$|G| = |H| \cdot (G : H)_l .$$

Аналогично определяются *правые* смежные классы и $(G : H)_r$ — их правый индекс в G, и доказывается, что

$$|G| = |H| \cdot (G : H)_r .$$

Следствие 2. *Порядок любого элемента конечной группы делит порядок группы. Группа простого порядка p всегда циклическая.*

Доказательство. По теореме 1 §3, имеем $|g| = |\langle g \rangle|$ для любого $g \in G$. По теореме Лагранжа $|g|$ делит $|G|$. Пусть $|G| = p$ и $a \in G$, $a \neq e$. Тогда $|a|$ делит p, т. е. $|a| = |\langle a \rangle| = p \Rightarrow \langle a \rangle = G$. □

Обратное утверждение теоремы Лагранжа в общем случае не верно. В группе $\mathbb{A}_4$ нет подгрупп порядка 6 (см. задачи). Но для циклических групп это утверждение верно.

Теорема 2. *Всякая подгруппа циклической группы является циклической. В циклической группе порядка n для любого делителя d числа n существует единственная подгруппа порядка d.*

Доказательство. Пусть $H \leq \mathbb{Z} = \langle \mathbb{Z}; + \rangle$ и $k = \min\limits_{m>0} \{m \in H\}$. Тогда $\ell = k \cdot q + r$ для любого $\ell \in H$, при этом $0 \leq r < k$. Следовательно, $r = \ell - q \cdot k \in H$, $r = 0$, и $H = \{s \cdot k : s \in \mathbb{Z}\} = \langle k \rangle$ — бесконечная циклическая группа. Более того, по лемме 2 §7, $H \simeq \mathbb{Z}$.

Рассмотрим случай конечной циклической группы

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

Пусть $H \leq G$ и $k = \min\limits_{m>0} \{a^m \in H\}$. Как и в случае бесконечной циклической группы для любого $a^m \in H$ имеем $m = k \cdot q + r$, где $0 \leq r < k$. Тогда

$$a^r = a^{m-kq} = a^m \cdot \left(a^k\right)^{-q} \in H \Rightarrow r = 0,$$

т. е. $H = \left\langle a^k \right\rangle$ — конечная циклическая группа.

Далее, пусть $n = d \cdot m$ и $H = \langle a^m \rangle$. Найдем порядок элемента a^m. Если $|a^m| = s$, то $a^{m \cdot s} = e$ и n делит $m \cdot s$, следовательно, $s \geq d$ и $|a^m| = d = |H|$.

Рассмотрим произвольную подгруппу $K \leq G$ порядка d. По доказанному $K = \langle a^s \rangle$, где $|a^s| = d$. Имеем $a^{s \cdot d} = e$, т. е. n делит $s \cdot d$. Таким образом, $d \cdot m \cdot l = s \cdot d \Rightarrow m \cdot l = s$ и m делит s. Следовательно, $a^s \in \langle a^m \rangle = H \Rightarrow K \subseteq H$. Так как $|K| = |H| = d$, то $K = H$. □

§9. Нормальные подгруппы и фактор-группы

Подгруппа H группы G называется *нормальной*, если $gH = Hg$ для любого $g \in G$. Нормальная подгруппа обозначается $H \trianglelefteq G$.

Лемма 1. *$H \trianglelefteq G \iff g^{-1}Hg \subseteq H$ для любого $g \in G$.*

Доказательство. Пусть $H \trianglelefteq G$. Тогда для любых $h \in H$, $g \in G$ существует $h_1 \in H$ такой, что $gh_1 = hg \Rightarrow g^{-1}hg = h_1 \in H \Rightarrow g^{-1}Hg \subseteq H$ для любого $g \in G$.

Обратно, для любых $h \in H$, $g \in G$ существуют $h_1, h_2 \in H : g^{-1}hg = h_1 \Rightarrow h \cdot g = g \cdot h_1 \subseteq g \cdot H \Rightarrow Hg \subseteq gH$ и $ghg^{-1} = h_2 \Rightarrow g \cdot h = h_2 \cdot g \in Hg \Rightarrow gH \subseteq Hg$. Поэтому $gH = Hg$ для любого $g \in G$. □

Отметим, что для любой $H \leq G$ справедливо

$$\forall g \in G \vDash g^{-1}Hg \subseteq H \Leftrightarrow \forall g \in G \vDash g^{-1}Hg = H;$$

Действительно, если $g^{-1}Hg \subseteq H$ для всех $g \in G$, то

$$g^{-1}Hg \subseteq H \subseteq g^{-1}\left(gHg^{-1}\right)g \subseteq g^{-1}Hg \Rightarrow g^{-1}Hg = H.$$

Определение фактор-группы. Пусть $H \trianglelefteq G$. Рассмотрим множество смежных классов

$$G/H = \{gH : g \in G\} .$$

Определим операцию на G/H по следующему правилу:

$$g_1H \cdot g_2H = (g_1 \cdot g_2)\, H.$$

Проверим корректность определения операции. Выберем другие представители в смежных классах g_1H и g_2H. Пусть $aH = g_1H$, $bH = g_2H$. Необходимо доказать, что $(a \cdot b)\, H = (g_1 \cdot g_2)\, H$.

По лемме 1 §8 имеем

$$g_1H = aH \Rightarrow a^{-1} \cdot g_1 = h_1 \in H,$$

$$g_2H = bH \Rightarrow b^{-1} \cdot g_2 = h_2 \in H.$$

Так как $H \trianglelefteq G$, то $b^{-1} \cdot h_1 = h_3 \cdot b^{-1}$ для некоторого $h_3 \in H$. Поэтому

$$(a \cdot b)^{-1} \cdot (g_1 \cdot g_2) = b^{-1} \cdot a^{-1} \cdot g_1 \cdot g_2 = b^{-1} \cdot h_1 \cdot g_2 = h_3 \cdot b^{-1} \cdot g_2 = h_3 \cdot h_2 \in H.$$

Следовательно, по лемме 1 §8, $(a \cdot b)\, H = (g_1 \cdot g_2)\, H$.

Теорема 1. *$\langle G/H; \cdot \rangle$ является группой.*

Доказательство. Для $a \in G$ обозначим смежный класс aH через $\bar{a}$. Тогда, по определению умножения, $\forall \bar{a}, \bar{b} \in G/H$ имеем $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$. Проверим аксиомы группы.

1) $\forall \bar{a}, \bar{b}, \bar{c} \in G/H : \left(\bar{a} \cdot \bar{b}\right) \cdot \bar{c} = \overline{a \cdot b} \cdot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)} = \bar{a} \cdot \left(\bar{b} \cdot \bar{c}\right)$.

2) $\forall \bar{a} \in G/H : \bar{e} \cdot \bar{a} = \overline{e \cdot a} = \bar{a} = \overline{a \cdot e} = \bar{a} \cdot \bar{e}$, т. е. $\bar{e}$ — единица G/H.

3) $\forall \bar{a} \in G/H : \bar{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \bar{e} = \overline{a^{-1} \cdot a} = \overline{a^{-1}} \cdot \bar{a}$. Следовательно, $\bar{a}^{-1} = \overline{a^{-1}}$. □

Рассмотрим произвольную подгруппу $H \leq \mathbb{Z}$. Так как $\mathbb{Z}$ — абелева группа, то $H \trianglelefteq \mathbb{Z}$. По теореме 2 из §8, H является циклической группой и имеет вид $H = n\mathbb{Z}$, где $n \geq 0$. Пусть $H \neq 0$. Докажем, что $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ при $n > 0$ является циклической группой порядка n.

Теорема 2. *$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ — циклическая группа порядка n.*

Доказательство. Для любого $a \in \mathbb{Z}$ имеем $a = n \cdot q + r$, где $0 \leq r < n$. Поэтому $\bar{a} = \bar{r}$. Причем $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \,(\mathrm{mod}\, n)$. Поэтому $\mathbb{Z}/n\mathbb{Z}$ состоит из следующих смежных классов: $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Очевидно, что $|\bar{1}| = n$. Следовательно, $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ — циклическая группа порядка n. □

В силу леммы 2 из §7 и доказанной теоремы имеем

Следствие 1. *Все циклические группы порядка n изоморфны $\mathbb{Z}_n$.*

§10. Основная теорема о гомоморфизмах групп

Пусть G, G' — группы и $\varphi : G \to G'$ — эпиморфизм. Найдём некоторое описание группы G'.

Теорема 1. Пусть $\varphi : G \to G'$ — эпиморфизм групп. Тогда $Ker\,\varphi \trianglelefteq G$ и $G' \simeq G/Ker\,\varphi$.

Обратно, если $H \trianglelefteq G$, то $\psi(g) = \bar{g}$ есть эпиморфизм G на G/H и $Ker\,\psi = H$.

Доказательство. Обозначим $Ker\,\varphi = H$. По лемме 1 §7, $H \leq G$. Легко видеть, что $g^{-1}Hg \subseteq H$.

Определим отображение $\tilde{\varphi} : G/H \to G'$ по правилу $\tilde{\varphi}(\bar{g}) = \varphi(g)$ для $\bar{g} \in G/H$.

Проверим корректность определения этого отображения. Пусть $\bar{g} = gH$, $\bar{a} = aH$ и $\bar{g} = \bar{a}$. Докажем, что $\varphi(g) = \varphi(a)$. По лемме 1 §8, $\bar{g} = \bar{a} \Leftrightarrow a^{-1} \cdot g \in Ker\,\varphi \Leftrightarrow \varphi\left(a^{-1} \cdot g\right) = e' = \varphi(a)^{-1} \cdot \varphi(g) \Leftrightarrow \varphi(a) = \varphi(g)$, где e' — единица G'. Докажем, что $\tilde{\varphi}$ — изоморфизм групп G/H и G'. Для любого $a' \in G'$ существует такой $a \in G$, что $\varphi(a) = a'$. Тогда $\tilde{\varphi}(\bar{a}) = a'$, поэтому $\tilde{\varphi}$ сюръективно. Далее, $\tilde{\varphi}(\bar{a}) = \tilde{\varphi}\left(\bar{b}\right) \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1} \cdot \varphi(b) = e' \Leftrightarrow \varphi\left(a^{-1} \cdot b\right) = e' \Leftrightarrow a^{-1} \cdot b \in H \Leftrightarrow \bar{a} = \bar{b}$. Следовательно, $\tilde{\varphi}$ — биективное отображение G/H на G'.

Для любых $\bar{a}, \bar{b} \in G/H$ имеем $\tilde{\varphi}\left(\bar{a} \cdot \bar{b}\right) = \tilde{\varphi}\left(\overline{a \cdot b}\right) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \tilde{\varphi}(\bar{a}) \cdot \tilde{\varphi}\left(\bar{b}\right)$. Таким образом, $G/H \simeq G'$.

Обратно, отображение $\psi : G \to G/H$, где $\psi(g) = \bar{g}$, сюръективно и, так как
$\psi(g_1 \cdot g_2) = \overline{g_1 \cdot g_2} = \bar{g}_1 \cdot \bar{g}_2 = \psi(g_1) \cdot \psi(g_2)$, то ψ — эпиморфизм. Далее,

$$a \in Ker\,\psi \Leftrightarrow \psi(a) = \bar{a} = \bar{e} \Leftrightarrow a \in H \Rightarrow Ker\,\psi = H. \quad \square$$

§11. Примеры и свойства колец. Кольца многочленов и формальных степенных рядов

Алгебраическая система $\mathbb{K} = \langle K; +, \cdot \rangle$, $K \neq \varnothing$, с двумя бинарными операциями $+$ (сложение) и $\cdot$ (умножение) называется *кольцом*, если $\langle K; + \rangle$ — абелева группа и $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$ для любых $a, b, c \in K$.

Алгебраическую систему $\langle K; + \rangle$ называют *аддитивной* группой кольца $\mathbb{K}$.

Если $\langle K; \cdot \rangle$ — полугруппа, то кольцо называется ассоциативным, а алгебраическую систему $\langle K; \cdot \rangle$ называют *мультипликативной* полугруппой

кольца $\mathbb{K}$.

Если $\langle K;\cdot\rangle$ — моноид, то K — кольцо с единицей.

Если $a\cdot b = b\cdot a$ для любых $a,b\in K$, то кольцо $\mathbb{K}$ называют *коммутативным.*

Подмножество $H\subseteq K$ называют *подкольцом*, если H — кольцо относительно операций кольца K.

Примеры: 1) $\langle\mathbb{Z};+,\cdot\rangle\subseteq\langle\mathbb{Q};+,\cdot\rangle\subseteq\langle\mathbb{R};+,\cdot\rangle$;

2) $\langle M_n(\mathbb{Z});+,\cdot\rangle\subseteq\langle M_n(\mathbb{Q});+,\cdot\rangle\subseteq\langle M_n(\mathbb{R});+,\cdot\rangle$;

3) Кольца функций относительно обычного сложения и умножения вещественных функций: $C^1[0,1]$ (кольцо дифференцируемых функций на $[0,1]$) $\subseteq C[0,1]$ (непрерывных) $\subseteq R^{\text{огр}}[0,1]$ (ограниченных) $\subseteq R[0,1]$ (всех);

4) Пусть $\langle A;+\rangle$ — произвольная абелева группа. Её легко превратить в кольцо $\langle A;+,\cdot\rangle$, определив умножение по правилу: $a\cdot b=0$ для любых $a,b\in A$.

Общие свойства. 1) Для любого $a\in K$ имеем $a\cdot 0 = 0\cdot a = 0$. Действительно, $a\cdot(0+0) = a\cdot 0 + a\cdot 0 = a\cdot 0 \Rightarrow a\cdot 0 = 0$. Аналогично $0\cdot a = 0$.

2) Если $0=1$, то $K=\{0\}$. Значит, в нетривиальном кольце $0\neq 1$.

3) Для любых $a,b\in K$: $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$. Действительно, $0 = a\cdot 0 = a\cdot(b+(-b)) = a\cdot b + a\cdot(-b)$, т. е. $a\cdot(-b) = -(a\cdot b)$. Аналогично, $(-a)\cdot b = -(a\cdot b)$.

4) Для любых $a_1,\ldots,a_n,b_1,\ldots,b_m\in K$: $\left(\sum\limits_{i=1}^{n} a_i\right)\left(\sum\limits_{i=1}^{m} b_i\right) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} a_i b_j$.

Доказательство индукцией по n и m. В частности, из 3) и 4) следует, что для любого $n\in\mathbb{Z}$ справедливо $(na)\cdot b = a\cdot(nb) = n\,(a\cdot b)$.

5) Если K — коммутативное кольцо, то, для любых $a,b\in K, n\in\mathbb{N}$,

$$(a+b)^n = \sum_{i=0}^{n} C_n^i a^i\cdot b^{n-i}.$$

Кольцо многочленов. Пусть K — некоторое кольцо и x — символ, не принадлежащий K (x называют *неизвестной, переменной*). Выражение вида

$$a = a_0 + a_1 x + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

где $a_i\in K$ и $n\in\mathbb{N}$, называют *многочленом* от x с коэффициентами $a_i\in K$.

Множество всех многочленов от x обозначают через

$$K[x] = \{a = \sum_{i=0}^{n} a_i x^i : a_i \in K, n \in \mathbb{N}\}.$$

Два многочлена $a = \sum\limits_{i=0}^{n} a_i x^i$ и $b = \sum\limits_{i=0}^{m} b_i x^i$ равны, если бесконечные векторы, составленные из коэффициентов a и b, совпадают покоординатно:

$$(a_0, a_1, \ldots, a_n, 0, \ldots) = (b_0, b_1, \ldots, b_m, 0, \ldots).$$

Пример: $a = 1 + 2x^2 = b = 1 + 0 \cdot x + 2x^2 + 0 \cdot x^7$.

Поэтому всегда можно считать, что два многочлена a и b имеют одинаковые границы суммирования. Для этого можно добавить необходимое число нулевых коэффициентов.

Определим операции на $K[x]$ по правилу:

$$\begin{cases} \sum\limits_{i=0}^{n} a_i x^i + \sum\limits_{i=0}^{n} b_i x^i = \sum\limits_{i=0}^{n} (a_i + b_i) x^i, \\ \sum\limits_{i=0}^{n} a_i x^i \cdot \sum\limits_{i=0}^{m} b_i x^i = \sum\limits_{i=0}^{n+m} c_i x^i, \text{ где } c_i = \sum\limits_{i_1+i_2=i} a_{i_1} \cdot b_{i_2}. \end{cases}$$

Докажем, что $\langle K[x]; +, \cdot \rangle$ является кольцом. Для простоты изложения будем записывать многочлены в виде бесконечных векторов:

$$a = \sum_{i=0}^{n} a_i x^i = (a_0, a_1, \ldots, a_n, 0, \ldots, 0, \ldots) = (a_i).$$

Тогда $K[x] = \{(a_i) : a_i \in K, n \in \mathbb{N}\}$ — алгебраическая система с операциями:

$$\begin{cases} a + b = (a_i + b_i), \\ a \cdot b = (c_i), \text{где } c_i = \sum\limits_{i_1+i_2=i} a_{i_1} \cdot b_{i_2}. \end{cases}$$

Теорема 1. $\langle K[x]; +, \cdot \rangle$ — *кольцо.*

Доказательство. Ясно, что $\langle K[x]; + \rangle$ — абелева группа, так как сложение векторов покоординатно. Докажем дистрибутивность умножения. Для любых $a, b, c \in K[x]$ имеем

$$a \cdot (b + c) = a \cdot (b_i + c_i) = (\sum_{i_1+i_2=i} a_{i_1} \cdot (b_{i_2} + c_{i_3})) =$$

$$= (\sum_{i_1+i_2=i} a_{i_1} \cdot b_{i_2} + \sum_{i_1+i_2=i} a_{i_1} \cdot c_{i_2}) = a \cdot b + a \cdot c.$$

Аналогично получаем $(b+c)\cdot a = b\cdot a + c\cdot a$. □

Элементы $a, b \in K$ называют *делителями нуля*, если $a, b \neq 0$, но $a\cdot b = 0$. Коммутативное ассоциативное кольцо без делителей нуля называют *областью целостности.*

Число $\deg(a) = \max\limits_i \{i : a_i \neq 0\}$ называют *степенью* многочлена $a = \sum\limits_{i=0}^{n} a_i x^i$, обычно полагают $\deg(0) = -\infty$. Отметим свойства степени многочленов:

$$\deg(a+b) \leq \max\{\deg(a), \deg(b)\},$$

$$\deg(a\cdot b) \leq \deg(a) + \deg(b).$$

Лемма 1. 1) *K ассоциативно $\Rightarrow$ $K[x]$ ассоциативно.* 2) *K коммутативно $\Rightarrow$ $K[x]$ коммутативно.* 3) *K — область целостности $\Rightarrow$ $K[x]$ — область целостности, причём* $\deg(a\cdot b) = \deg(a) + \deg(b)$ *для любых* $a, b \in K[x]$.

Доказательство. 1) Докажем ассоциативность умножения. Для любых $a, b, c \in K[x]$ имеем

$$(a\cdot b)\cdot c = (\sum_{i_1+i_2=i} a_{i_1}\cdot b_{i_2})\cdot c = (\sum_{k+i_3=i}\ (\sum_{i_1+i_2=k} a_{i_1}\cdot b_{i_2})\cdot c_{i_3}) =$$

$$= (\sum_{k+i_3=i}\ \sum_{i_1+i_2=k} a_{i_1}\cdot b_{i_2}\cdot c_{i_3}) = (\sum_{i_1+i_2+i_3=i} a_{i_1}\cdot b_{i_2}\cdot c_{i_3}).$$

Аналогично вычисляем $a\cdot(b\cdot c) = (\sum\limits_{i_1+i_2+i_3=i} a_{i_1}\cdot b_{i_2}\cdot c_{i_3})$.

Следовательно, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$.

2) Для любых $a, b \in K[x]$ имеем

$$a\cdot b = (\sum_{i_1+i_2=i} a_{i_1}\cdot b_{i_2}) = (\sum_{i_1+i_2=i} b_{i_2}\cdot a_{i_1}) = b\cdot a.$$

3) Если $a, b \neq 0$, $\deg(a) = n$ и $\deg(b) = m$, то $a_n, b_m \neq 0$ и поэтому $c_{n+m} = a_n\cdot b_m \neq 0$, то есть $c = a\cdot b \neq 0$. При этом $\deg(c) = n+m = \deg(a) + \deg(b)$. Если $a = 0$, то $a\cdot b = 0$ и $\deg(a\cdot b) = -\infty$ и $\deg(a) + \deg(b) = -\infty$. □

Переход от кольца K к $K[x]$ называют кольцевым присоединением x. Присоединяя к $K[x]$ переменную y, получим кольцо многочленов $K[x, y]$ от двух переменных. Этот процесс можно продолжать:

$$K \subset K[x] \subset K[x, y] \subset K[x, y, z] \subset \dots .$$

Замечание. По правилу умножения в кольце $K[x]$, многочлены $\sum\limits_{i=0}^{n} a_i x^i$ и $\sum\limits_{i=0}^{n} b_i x^i$ можно перемножать и складывать как обычные функции, используя правило: $x^k \cdot x^s = x^{k+s}$, $a_k x^k + b_k x^k = (a_k + b_k) x^k$. Но при этом следует различать, что многочлены — это не функции на кольце K. Например, превратим группу $\mathbb{Z}_2$ в кольцо, полагая $\bar{0} \cdot \bar{1} = \bar{1} \cdot \bar{0} = \bar{0}$, $\bar{1} \cdot \bar{1} = \bar{1}$. Тогда многочлены $f = \bar{1} + \bar{1} \cdot x^2, g = \bar{1} + \bar{1} \cdot x^4 \in \mathbb{Z}_2[x]$ различны, но как функции из $\mathbb{Z}_2$ в $\mathbb{Z}_2$ совпадают: $f(\bar{0}) = g(\bar{0}) = \bar{1}$, $f(\bar{1}) = g(\bar{1}) = \bar{0}$.

Кольцо формальных степенных рядов. Рассмотрим множество бесконечных векторов с координатами из K:

$$K[[x]] = \{a = (a_0, a_1, \ldots, a_n, \ldots) = (a_i) : a_i \in K\}.$$

Заметим, что $K[x] \subsetneq K[[x]]$. В отличие от множества $K[x]$, в $K[[x]]$ векторы могут иметь бесконечное число ненулевых координат. Определим операции на $K[[x]]$ по правилу:

$$\begin{cases} a + b = (a_i + b_i), \\ a \cdot b = (c_i), \text{ где } \; c_i = \sum\limits_{i_1 + i_2 = i} a_{i_1} \cdot b_{i_2}. \end{cases}$$

Так как число операций сложения и умножения при определении координат суммы и произведения векторов из $K[[x]]$ является конечным, то операции в $K[[x]]$ определены корректно.

Теорема 2. $\langle K[[x]]; +, \cdot \rangle$ — *кольцо.*

Доказательство без изменений повторяет доказательство теоремы 1, так как мы никогда не использовали конечность числа ненулевых координат бесконечных векторов. □

Кольцо $K[[x]]$ называют *кольцом формальных степенных рядов*. Векторы $a = (a_i) \in K[[x]]$ обозначают как бесконечные формальные суммы:

$$a = (a_0, a_1, \ldots, a_n, \ldots) = \sum_{i=0}^{\infty} a_i x^i, \quad a_i \in K.$$

Операции на этих суммах определены по правилу:

$$\begin{cases} \sum\limits_{i=0}^{\infty} a_i x^i + \sum\limits_{i=0}^{\infty} b_i x^i = \sum\limits_{i=0}^{\infty} (a_i + b_i) x^i, \\ \sum\limits_{i=0}^{\infty} a_i x^i \cdot \sum\limits_{i=0}^{\infty} b_i x^i = \sum\limits_{i=0}^{\infty} \left(\sum\limits_{s+t=i} a_s \cdot b_t \right) x^i. \end{cases}$$

Как видно из определения, формальные степенные ряды довольно просты в обращении. Используя известные тождества из математического анализа, можно получить ряд красивых формул для $K[[x]]$. Единственным условием такого переноса является конечность числа операций сложения и умножения элементов из K при вычислении коэффициентов рядов.

Примеры: $e^{2x} \cdot e^{1+x^2} = e^{(x+1)^2}$ тогда и только тогда, когда

$$\left(1 + \frac{2x}{1!} + \frac{2^2 \cdot x^2}{2!} + \dots\right)\left(1 + \frac{x^2+1}{1!} + \frac{\left(x^2+1\right)^2}{2!} + \dots\right) =$$

$$= 1 + \frac{(x+1)^2}{1!} + \frac{(x+1)^4}{2!} + \dots;$$

$\sin^2 x + \cos^2 x = 1$ тогда и только тогда, когда

$$\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots\right)^2 + \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots\right)^2 = 1.$$

§12. Гомоморфизмы и идеалы колец. Фактор-кольцо и основная теорема о гомоморфизмах колец. Кольцо вычетов $\mathbb{Z}_n$

Пусть $\langle K; +, \cdot\rangle$, $\langle K'; \oplus, \odot\rangle$ — кольца. Отображение $\varphi : K \to K'$ называется *гомоморфизмом*, если оно сохраняет операции, т. е. для любых $a, b \in K$:

$$\varphi(a+b) = \varphi(a) \oplus \varphi(b),$$
$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b).$$

Так как φ является гомоморфизмом групп $\langle K; +\rangle$ и $\langle K'; \oplus\rangle$, то, в силу доказанного в §7, имеем $\varphi(0) = 0'$ ($0'$ — ноль кольца K') и $\varphi(na) = n\varphi(a)$ для любых $a \in K$, $n \in \mathbb{Z}$ (в частности, $\varphi(-a) = -\varphi(a)$).

Множество $Ker\,\varphi = \{x \in K : \varphi(x) = 0'\}$ называется *ядром* гомоморфизма φ. Подкольцо I кольца K называют *идеалом*, если $ai \subseteq I$, $ia \subseteq I$ для любых $a \in K, i \in I$ (это обозначают также так: $KI \subseteq I$, $IK \subseteq I$). Идеал I кольца K обозначают следующим образом: $I \trianglelefteq K$.

Лемма 1. *Если $\varphi : K \to K'$ — гомоморфизм колец, то $Ker\,\varphi \trianglelefteq K$, $Im\varphi$ — подкольцо K'.*

Доказательство. Обозначим $Ker\,\varphi$ через I. В силу леммы 1 §7, достаточно доказать, что $ab \in I$, $ba \in I$ для любых $a \in K$, $b \in I$ и $a' \cdot b' \in Im\varphi$ для любых $a', b' \in Im\varphi$.

Для любых $a \in K$, $b \in I$ имеем $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) = \varphi(a) \odot 0' = 0'$. Следовательно, $a \cdot b \in I$ и $KI \subseteq I$. Аналогично доказывается, что $IK \subseteq I$.

Далее, для любых $a', b' \in Im\varphi$ существуют $a, b \in K$ такие, что $a' = \varphi(a)$, $b' = \varphi(b)$. Поэтому $a' \odot b' = \varphi(a) \odot \varphi(b) = \varphi(a \cdot b) \Rightarrow a' \odot b' \in Im\varphi$. □

Определение фактор-кольца. Пусть $I \trianglelefteq K$. Рассмотрим K/I — множество смежных классов $\langle K; + \rangle$ по $\langle I; + \rangle$ и определим операции на K/I по правилу:

$$\begin{aligned} (a + I) \oplus (b + I) &= (a + b) + I, \\ (a + I) \odot (b + I) &= a \cdot b + I. \end{aligned}$$

Будем для краткости записывать $a + I = \bar{a}$. Итак, $K/I = \{\bar{a} : a \in K\}$ с операциями

$$\bar{a} \oplus \bar{b} = \overline{a + b},$$
$$\bar{a} \odot \bar{b} = \overline{a \cdot b}.$$

Докажем, что операции определены корректно. По лемме 1 §8, $\bar{a} = \bar{b} \Leftrightarrow a - b \in I$. Пусть $\bar{a} = \bar{b}$, $\bar{c} = \bar{d}$, тогда

$$\overline{a + c} - \overline{b + d} = \overline{a + c - b - d} = \overline{a - b + c - d} = \overline{a - b} + \overline{c - d} = \bar{0} + \bar{0} = \bar{0},$$

$$\overline{a \cdot c} - \overline{b \cdot d} = \overline{a \cdot c - b \cdot d} = \overline{a \cdot c - b \cdot c + b \cdot c - b \cdot d} = \overline{(a - b) \cdot c} + \overline{b \cdot (c - d)} = \bar{0}.$$

Следовательно, $\overline{a + c} = \overline{b + d}$, и $\overline{a \cdot c} = \overline{b \cdot d}$.

Лемма 2. *$\langle K/I; \oplus, \odot \rangle$ — кольцо; если K ассоциативно, то K/I ассоциативно.*

Доказательство. Проверим все аксиомы кольца. Во-первых, $\langle K/I; \oplus \rangle$ — группа по теореме 1 из §8.

Далее, для любых $\bar{a}, \bar{b}, \bar{c} \in K/I$ имеем

$$\bar{a} \odot \left(\bar{b} \oplus \bar{c}\right) = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \bar{a} \odot \bar{b} \oplus \bar{a} \odot \bar{c}.$$

Аналогично, $\left(\bar{b} \oplus \bar{c}\right) \cdot \bar{a} = \bar{b} \odot \bar{a} \oplus \bar{c} \odot \bar{a}$.

Наконец, $\langle K/I; \odot \rangle$ — полугруппа, так как для любых $\bar{a}, \bar{b}, \bar{c} \in K/I$ имеем $\left(\bar{a} \odot \bar{b}\right) \odot \bar{c} = \overline{a \cdot b} \odot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)} = \bar{a} \odot \overline{(b \cdot c)} = \bar{a} \odot \left(\bar{b} \odot \bar{c}\right)$. □

Кольцо $\langle K/I; \oplus, \odot \rangle$ называется *фактор-кольцом* K по идеалу I.

Пусть $\varphi : K \to K'$. Тогда φ — *изоморфизм*, если φ — гомоморфизм и φ — взаимно однозначное отображение. Если φ — изоморфизм, то кольца K и K' называют *изоморфными* и обозначают $K \simeq K'$. Отображение φ — *эпиморфизм*, если φ — гомоморфизм и $Im\varphi = K'$. Отображение φ — *мономорфизм*, если φ — гомоморфизм и $Ker\,\varphi = 0$.

Теорема 1 (*основная теорема о гомоморфизмах колец*). *Пусть* $\varphi : K \to K'$ *— эпиморфизм, тогда* $Ker\,\varphi \trianglelefteq K$ *и* $K' \simeq K/Ker\,\varphi$. *Обратно, пусть* $I \trianglelefteq K$ *и* $\pi : K \to K/I$ *определено правилом* $\pi(a) = \bar{a}$ *для* $a \in K$. *Тогда* π *— эпиморфизм и* $Ker\,\pi = I$.

Доказательство. Обозначим $Ker\,\varphi = I$. По лемме 1, $I \trianglelefteq K$. Положим $\tilde{\varphi} : K/I \to K'$, где $\tilde{\varphi}(\bar{a}) = \varphi(a)$ для $\bar{a} \in K/I$. Проверим корректность определения $\tilde{\varphi}$.

Пусть $\bar{a} = \bar{b}$, тогда $a - b \in Ker\,\varphi$, поэтому $\varphi(a-b) = 0'$ и $\varphi(a) = \varphi(b)$.

Докажем, что $\tilde{\varphi}$ — изоморфизм колец K/I и K'.

1) Покажем, что $\tilde{\varphi}$ взаимно однозначно.

Для любого $a' \in K'$ существует такой $a \in K$, что $\varphi(a) = a'$, тогда $\tilde{\varphi}(\bar{a}) = a'$ по определению. Далее, $\tilde{\varphi}(\bar{a}) = \tilde{\varphi}\left(\bar{b}\right)$ для любых $a, b \in K \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \varphi(a-b) = 0' \Leftrightarrow a - b \in Ker\,\varphi \Leftrightarrow \bar{a} = \bar{b}$.

2) Покажем, что $\tilde{\varphi}$ — гомоморфизм.

Для любых $a, b \in K$ имеем

$$\tilde{\varphi}\left(\bar{a} \oplus \bar{b}\right) = \tilde{\varphi}\left(\overline{a+b}\right) = \varphi(a+b) = \varphi(a) \oplus \varphi(b) = \tilde{\varphi}(\bar{a}) \oplus \tilde{\varphi}\left(\bar{b}\right),$$

$$\tilde{\varphi}\left(\bar{a} \odot \bar{b}\right) = \tilde{\varphi}\left(\overline{a \cdot b}\right) = \varphi(a \cdot b) = \varphi(a) \odot \varphi(b) = \tilde{\varphi}(\bar{a}) \cdot \tilde{\varphi}\left(\bar{b}\right).$$

Таким образом, $K/I \simeq K'$.

Обратно, пусть $\pi : K \to K/I$, где $\pi(a) = \bar{a}$ для любого $a \in K$. Тогда, очевидно, что π — эпиморфизм и $Ker\,\pi = \{a \in K : \pi(a) = \bar{a} = \bar{0}\} = \{a \in K : a \in I\} = I$. □

Лемма 3. *Всякое подкольцо кольца* $\langle \mathbb{Z}; +, \cdot \rangle$ *имеет вид* $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$, *где* $n \in \mathbb{N}$.

Доказательство. Пусть K — подкольцо в $\langle \mathbb{Z}; +, \cdot \rangle$, тогда K — подгруппа в $\mathbb{Z}$. По теореме 2 из §7, $K = n\mathbb{Z}$. Легко проверить, что $n\mathbb{Z}$ замкнуто относительно умножения. □

Очевидно, что $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, так как $m(n\mathbb{Z}) = n(m\mathbb{Z}) \subseteq n\mathbb{Z}$ для любого $m \in \mathbb{Z}$.

Кольцо $\mathbb{Z}/n\mathbb{Z}$ называют *кольцом вычетов* по модулю n и обозначают через $\mathbb{Z}_n$. По определению $\mathbb{Z}_n = \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$ с операциями

$$\bar{a} + \bar{b} = \overline{a+b},$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b},$$

где через $\bar{a}$ обозначен остаток от деления a на n.

§13. Поле, подполе, расширение поля. Поле F_p. Теорема о простом подполе. Характеристика поля

Алгебраическая система $\langle F; +, \cdot\rangle$ типа $\langle 2, 2\rangle$ называется *полем* если:

$(F1)$ $\langle F; +\rangle$ — абелева группа;

$(F2)$ $\langle F \setminus \{0\}; \cdot\rangle$ — абелева группа;

$(F3)$ $(x + y)z = xz + yz$ для всех $x, y, z \in F$.

По определению считаем, что в поле $0 \neq 1$. Если в аксиоме $(F2)$ не требовать, чтобы группа была абелевой, то такая алгебраическая система называется *телом*, т. е. тело — это некоммутативное поле.

Другими словами, $\langle F; +, \cdot\rangle$ является *полем*, если $\langle F; +, \cdot\rangle$ — ассоциативное коммутативное кольцо с 1, а $\langle F^* = F \setminus \{0\}; \cdot\rangle$ — коммутативная группа.

Теорема 1. *$\mathbb{Z}_m$ — поле $\Leftrightarrow$ $m = p$ — простое число.*

Доказательство. Если $\mathbb{Z}_m$ — поле и $m = n_1 \cdot n_2$, то $\bar{n}_1 \cdot \bar{n}_2 = \bar{m} = \bar{0}$. Следовательно, $\bar{n}_1 = 0$ или $\bar{n}_2 = 0$, т. е. $n_1 = m$ или $n_2 = m$.

Обратно, если $m = p$ — простое, то для любого $1 \leq k \leq p - 1$ имеем $(k, p) = 1 \Rightarrow \exists s, t \in \mathbb{Z}$ такие, что $s \cdot k + t \cdot p = 1 \Rightarrow \bar{s} \cdot \bar{k} + \bar{t} \cdot \bar{p} = \overline{s \cdot k + t \cdot p} = \bar{1} = \bar{s} \cdot \bar{k}$. Таким образом, элемент $\bar{k}$ является обратимым и $\langle \mathbb{Z}_p^*, \cdot\rangle$ — группа. □

Заметим, что вместо $\mathbb{Z}_p$ пишут часто F_p (или $GF(p)$) и называют это поле *полем Галуа*. Подкольцо $F \subseteq P$ поля P, само являющееся полем, называется *подполем*, а P называется *расширением* поля F. (Заметим, что пересечение любого числа подполей поля P является подполем (как и групп, колец).) Поле F называется *простым*, если в нем нет собственных подполей.

Примеры. 1) F_p — простое поле. Пусть P подполе в F_p. Тогда $\bar{1} \in P$ и, следовательно, $\bar{2}, \ldots, \overline{p-1} \in P$, т. е. $P = F_p$.

2) $\mathbb{Q}$ — простое поле. Пусть P — подполе в $\mathbb{Q}$. Тогда $1 \in P$ и $n, m \in P$ для любых $n, m \in \mathbb{Z}$. Поэтому $\frac{n}{m} \in P$ $(m \neq 0)$ и $P = \mathbb{Q}$.

Теорема 2. *В любом поле P существует единственное простое подполе P_0. При этом $P_0 \simeq \mathbb{Q}$ или $P_0 \simeq F_p$.*

Доказательство. Пусть P_1, P_2 — простые подполя в P. Тогда $P_1 \cap P_2$ — подполе в P_1 и P_2 и $P_1 \cap P_2 = P_1 = P_2$.

Пусть e — единица поля P. Возможны два случая: либо $ne \neq 0$ для любого $n \in \mathbb{N}$, либо существует $n \in \mathbb{N}$ такое, что $ne = 0$. Рассмотрим отдельно эти случаи.

1) Пусть $P_0 = \left\{n\,(me)^{-1} : n \in \mathbb{Z}, m \in \mathbb{N}\right\}$. Докажем, что P_0 — простое подполе в P. Заметим что $na = ne \cdot a$, $na \cdot mb = nm(ab)$. Далее, имеем $0 \in P_0, e = 1(1e)^{-1} \in P_0$. Пусть $n_1\,(m_1e)^{-1} + n_2\,(m_2e)^{-1} = a$. Тогда

$$a \cdot (m_1m_2e) = (n_1m_2 + n_2m_1) \cdot e \Rightarrow a = (n_1m_2 + n_2m_1)\,(m_1m_2e)^{-1} \in P_0,$$

$$n_1\,(m_1e)^{-1} \cdot n_2\,(m_2e)^{-1} = n_1n_2\,(m_1m_2e)^{-1} \in P_0,$$

$$-\left(n\,(me)^{-1}\right) = (-n)\,(me)^{-1} \in P_0.$$

Если $n \neq 0$, то $n\,(me)^{-1} \cdot m\,(ne)^{-1} = nm\,(nme)^{-1} = (nme)\,(nme)^{-1} = e$, поэтому $\left(n\,(me)^{-1}\right)^{-1} = m\,(ne)^{-1}$ и P_0 — подполе в P.

Докажем, что $P_0 \simeq \mathbb{Q}$. Пусть $\varphi\left(n\,(me)^{-1}\right) = \frac{n}{m}$. Покажем корректность:

$$n_1\,(m_1e)^{-1} = n_2\,(m_2e)^{-1} \Leftrightarrow n_1m_2e = n_2m_1e \Leftrightarrow$$

$$(n_1m_2 - n_2m_1)\,e = 0 \Leftrightarrow n_1m_2 - n_2m_1 = 0 \Leftrightarrow \frac{n_1}{m_1} = \frac{n_2}{m_2}.$$

Покажем, что φ — гомоморфизм:

$$\varphi\left(n_1\,(m_1e)^{-1} + n_2\,(m_2e)^{-1}\right) = \varphi\left((n_1m_2 + n_2m_1)\,(m_1m_2e)^{-1}\right) =$$

$$= \frac{n_1m_2 + n_2m_1}{m_1m_2} = \frac{n_1}{m_1} + \frac{n_2}{m_2} = \varphi\left(n_1\,(m_1e)^{-1}\right) + \varphi\left(n_2\,(m_2e)^{-1}\right),$$

$$\varphi\left(n_1\,(m_1e)^{-1} \cdot n_2\,(m_2e)^{-1}\right) = \varphi\left(n_1n_2\,(m_1m_2e)^{-1}\right) =$$

$$= \frac{n_1n_2}{m_1m_2} = \frac{n_1}{m_1} \cdot \frac{n_2}{m_2} = \varphi\left(n_1\,(m_1e)^{-1}\right) \cdot \varphi\left(n_2\,(m_2e)^{-1}\right).$$

Покажем, что φ — эпиморфизм: $\varphi\left(n \cdot (me)^{-1}\right) = \frac{n}{m}$ для любого $\frac{n}{m} \in \mathbb{Q}$.

Проверим, что φ — мономорфизм:

$$Ker\,\varphi = \left\{n \cdot (me)^{-1} : \varphi\left(n \cdot (me)^{-1}\right) = \frac{n}{m} = 0 \Leftrightarrow n = 0\right\} = \{0\}.$$

По основной теореме о гомоморфизмах колец $P/Ker\,\varphi = P_0/\{0\} \simeq P_0 \simeq \mathbb{Q}$. Следовательно, $P_0 \simeq \mathbb{Q}$ — простое поле в P.

2). Существует $n \in \mathbb{N}$ такое, что $ne = 0$. Выберем $m = \min\{n \in \mathbb{N} : ne = 0\}$. Тогда $m = p$ простое, так как если $m = m_1 \cdot m_2$, то $me = (m_1 \cdot m_2)e = (m_1e) \cdot (m_2e) = 0$. Следовательно, либо $m_1e = 0$, либо

$m_2 e = 0$, т. е. либо $m_1 = m$, либо $m_2 = m$. Пусть $P_0 = \{0, e, \ldots, (p-1)\,e\}$. Тогда для любых $k, s \in P_0$ имеем

$$\begin{aligned} ke + se &= (k+s)\,e = (\overline{k+s})e, \\ (ke)\cdot(se) &= (k\cdot s)\,e = (\overline{k\cdot s})e, \end{aligned}$$

где $\bar{n}$ обозначает остаток от деления n на p. Легко видеть, что $P_0 \simeq F_p$ — простое подполе в P. □

Следствие. *Любое поле является расширением F_p или $\mathbb{Q}$.*

Если $P_0 \simeq \mathbb{Q}$, то говорят, что поле P имеет *характеристику* 0 (обозначение: $char\, P = 0$). Если $P_0 \simeq F_p$, то говорят, что поле P имеет характеристику p (обозначение: $char\, P = p$).

Очевидно, что если $char\, P = 0$, то $na \neq 0$ для любого ненулевого $a \in P$ и любого $n \in \mathbb{N}$. Если же $char\, P = p$, то $pa = 0$ для любого $a \in P$.

§14. Поле комплексных чисел: матричная конструкция, изоморфизм с конструкцией в виде пар действительных чисел. Групповые свойства корней из единицы

Теорема 1. $P = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ — *подкольцо в $M_2(\mathbb{R})$, являющееся полем.*

Доказательство. Заметим, что $0, E \in P$. Кроме того,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} a+x & (b+y) \\ -(b+y) & a+x \end{pmatrix} \in P,$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} ax-by & (bx+ay) \\ -(bx+ay) & ax-by \end{pmatrix} \in P,$$

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in P.$$

Далее, $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2$ и $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ — обратимая матрица, если она ненулевая, с обратной из P. Таким образом, P — поле. □

Замечание. $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = aE + bJ$, где $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Тогда $\{a \cdot E : a \in \mathbb{R}\} \simeq \mathbb{R}$, $J^2 = (-J)^2 = -E$, т. е. J, $-J$ — решения уравнения $x^2 + 1 = 0$.

Вспомним определение поля $\mathbb{C}$: $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$.

Теорема 2. *$\langle \mathbb{C}; +, \cdot \rangle$ является полем изоморфным P.*

Доказательство. Определим $\varphi : P \to \mathbb{C}$ правилом $\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = (a, b)$. Тогда φ — эпиморфизм, т. е. $\mathbb{C}$ — кольцо. $Ker\,\varphi = \{0\} \Rightarrow P/Ker\,\varphi = P/\{0\} = P \simeq \mathbb{C}$. □

Обозначим через P_n множество $\left\{\varepsilon_k = \cos\frac{2\pi k}{n} + \mathbf{i}\sin\frac{2\pi k}{n} : 0 \leq k \leq n-1\right\}$.

Теорема 3. $\langle P_n; \cdot \rangle \simeq \mathbb{Z}_n$.

Доказательство. Имеем

$$\varepsilon_k \cdot \varepsilon_j = \cos\frac{2\pi\,(k+j)}{n} + \mathbf{i}\sin\frac{2\pi\,(k+j)}{n} = \varepsilon_r = \cos\frac{2\pi r}{n} + \mathbf{i}\sin\frac{2\pi r}{n},$$

где $r = r(k, j)$ — остаток от деления $(k + j)$ на n.

Определим отображение $\varphi : P_n \to \mathbb{Z}_n$ правилом $\varphi(\varepsilon_k) = \bar{k}$.

Покажем, что φ — гомоморфизм. Пусть r определено как и раньше, тогда

$$\varphi(\varepsilon_k \cdot \varepsilon_j) = \varphi(\varepsilon_r) = \bar{r} = \overline{k+j} = \bar{k} + \bar{j} = \varphi(\varepsilon_k) + \varphi(\varepsilon_j).$$

Поскольку $\varphi(\varepsilon_i) = \bar{0} \iff \bar{i} = \bar{0}$, то $i = 0$ и $Ker\,\varphi = \{1\}$. Очевидно, что φ сюръективно. Следовательно, $P_n \simeq \mathbb{Z}_n$. □

§15. Максимальные идеалы колец и поля вычетов

Идеал I кольца K называется *максимальным*, если $I \neq K$ и для любого $J \lhd K$ такого, что $I \subseteq J \subseteq K$, либо $J = I$, либо $J = K$. Обозначение: $I \lhd_{\max} K$.

Теорема 1. *Пусть K — ассоциативное коммутативное кольцо с 1, I — идеал в K. Тогда K/I — поле $\Leftrightarrow I \lhd_{\max} K$.*

Доказательство. Пусть K/I — поле, $I \subseteq J \trianglelefteq K$ и $I \neq J$. Тогда существует $j \in J \setminus I$. Так как K/I — поле, то существует $\bar{x} \in K/I$ такой, что $\bar{j} \cdot \bar{x} = \bar{1}$. Следовательно, $j \cdot x + I = 1 + I$ и $1 - j \cdot x \in I$. Тогда $j \cdot x \in J, I \subseteq J$ и $1 \in J$. Поэтому $1 \cdot k = k \in J$ для любого $k \in K$, т. е. $K = J$.

Обратно, пусть $I \lhd_{\max} K$. Рассмотрим $a \in K \setminus I$ и $J := a \cdot K + I := \{ak + i : k \in K, i \in I\}$. Тогда $J \lhd K$, $a \in J$, и $I \subseteq J$. Следовательно, $a \cdot K + I = K$. Поэтому $1 = a \cdot x + i$, где $i \in I$ и $\bar{1} = \bar{a} \cdot \bar{x}$ в K/I $(1 \notin I \Rightarrow \bar{1} \in K/I)$. Таким образом, K/I — поле. □

Поле K/I, где $I \lhd_{\max} K$, а K — ассоциативное коммутативное кольцо с 1, называется *полем вычетов*.

Пример. Как мы видели ранее, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, где p — простое число, является полем. Следовательно, $p\mathbb{Z} \lhd_{\max} \mathbb{Z}$. Более того, все максимальные идеалы в $\mathbb{Z}$ имеют вид $p\mathbb{Z}$, где p — простое число.

§16. Целостные кольца и поля частных. Поле рядов Лорана

Кольцо A называется *целостным*, если A — ассоциативное коммутативное кольцо с 1 и без делителей нуля.

Пример. $\mathbb{Z} \subseteq \mathbb{Q}$.

Наша цель — вложить целостное кольцо A в поле, т. е. построить такое поле F, что A можно рассматривать как подкольцо в F.

Построение поля частных. Рассмотрим множество

$$A \times A^* = \{(a, b) : a \in A, b \in A^* = A \setminus \{0\}\}.$$

Разобьём $A \times A^*$ на классы эквивалентности:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Предложение 1. *"$\sim$" — отношение эквивалентности на $A \times A^*$.*

Доказательство. Очевидно, что $(a, b) \sim (a, b)$ и $(a, b) \sim (c, d) \Leftrightarrow (c, d) \sim (a, b)$. Пусть $(a, b) \sim (c, d), (c, d) \sim (e, f)$, т. е. $ad = bc$, $cf = ed$. Тогда $adf = bcf$, $bcf = bed$. Следовательно, $af = be$. □

В силу теоремы 1 из § 1.5, $A \times A^*$ разбивается на классы эквивалентности: $Q(A) = \{a/b : a, b \in A, b \neq 0\}$, где $a/b = \{(x, y) \in A \times A^* : (x, y) \sim (a, b)\}$, причем $a/b = c/d \Leftrightarrow ad = b$. Определим операции (корректность легко проверяется) на $Q(A)$:

$$a/b + c/d = (ad + bc)/bd,$$
$$a/b \cdot c/d = ac/bd.$$

Теорема 1. *Для любого целостного кольца A алгебраическая система $\langle Q(A); +, \cdot\rangle$ является полем, которое называется полем частных кольца A. При этом вложение $f : A \to Q(A)$, где $f(a) = a/1$, является изоморфизмом между A и $f(A)$.*

Доказательство. Легко видеть, что

$$(a/b + c/d) + e/f = a/b + (c/d + e/f),$$

$$-a/b + a/b = 0,\ a/b + 0/b = a/b,\ a/b + c/d = c/d + a/b,$$

$$(a/b \cdot c/d) \cdot e/f = a/b \cdot (c/d \cdot e/f),\quad a/b \cdot 1/1 = a/b,$$

$$a/b \cdot b/a = 1/1, a, b \neq 0, a/b \cdot c/d = c/d \cdot a/b.$$

Таким образом, $Q(A)$ — поле.

Пусть $\bar{A} = f(A)$. Тогда $f(a+b) = (a+b)/1 = a/1 + b/1 = f(a) + f(b)$ и $f(a \cdot b) = (a \cdot b)/1 = a/1 \cdot b/1 = f(a) \cdot f(b)$. Далее, $f(a) = f(b) \Leftrightarrow a/1 = b/1 \Leftrightarrow a = b$. Таким образом, f — изоморфизм A на $\bar{A}$. □

Пример: $Q(\mathbb{Z}) = \mathbb{Q}$, $\mathbb{Z} \subseteq \mathbb{Q}$.

Рассмотрим кольцо многочленов $F[x]$ и кольцо формальных степенных рядов $F[[x]]$. Выясним, что из себя представляют $Q(F[x])$, $Q(F[[x]])$.

Пусть $f = a_0 + a_k x^k + a_{k+1}x^{k+1} + \ldots \in F[[x]]$ и $a_k \neq 0$. Назовем *нижней степенью элемента* f число $v(f) = k = \min\limits_{k \geq 1}\{k : a_k \neq 0\}$. Положим $v\left(a_0 + 0 \cdot x + 0 \cdot x^2 + \ldots\right) = \infty$.

Лемма 1. *Пусть F — целостное кольцо. Тогда $F[[x]]$ — целостное кольцо.*

Доказательство. Пусть

$$\begin{aligned} f &= a_k x^k + a_{k+1}x^{k+1} + \ldots \in F[[x]],\ a_k \neq 0, \\ g &= b_m x^m + b_{m+1}x^{m+1} + \ldots \in F[[x]],\ b_m \neq 0, \end{aligned}$$

тогда $f \cdot g = a_k b_m x^{k+m} + \ldots \neq 0$. □

Лемма 2. *Пусть $f = 1 + h$, где $h = a_1 x + a_2 x^2 + \ldots$. Положим $g = 1 - h + h^2 - h^3 + \ldots$. Тогда $f \cdot g = 1$.*

Доказательство. Если $v(f) = \infty$, то $h = 0$ и $f = 1 = g$, т. е. $f \cdot g = 1$. Пусть $v(f) < \infty$. Тогда $v(g) = v(h) < \infty$. Пусть $v(f \cdot g) = k < \infty$. Тогда

$$f \cdot g = (1+h)\left(1 - h + h^2 - h^3 + \ldots - h^{2k+1}\right) + (1+h)\left(h^{2k+2} - h^{2k+3} + \ldots\right) =$$

$$= 1 - h^{2k+2} + (1+h)\left(h^{2k+2} - h^{2k+3} + \ldots\right) =$$

$$= 1 - h^{2k+2} + \underbrace{\left(h^{2k+2} - h^{2k+3} + \ldots\right)}_{=f_1} + h \underbrace{\left(h^{2k+2} - h^{2k+3} + \ldots\right)}_{=f_2}.$$

$$v\left(f \cdot g\right) \geq \min\left(\underbrace{v\left(h^{2k+2}\right)}_{\geq 2k+2}, \underbrace{v\left(f_1\right)}_{\geq 2k+2}, \underbrace{v\left(f_2\right)}_{\geq 2k+2}\right) \geq 2k+2.$$

Следовательно, $v\left(f \cdot g\right) = +\infty$ и $f \cdot g = 1$. □

Поле $Q\left(F\left[x\right]\right) = F\left(x\right) = \left\{\frac{f(x)}{g(x)} : g(x) \neq 0\right\}$ называется *полем рациональных дробей*. Поле $Q\left(F\left[\left[x\right]\right]\right) = F\left(\left(x\right)\right)$ называется *полем рядов Лорана*.

Обозначим элемент $\frac{\sum\limits_{i=0}^{\infty} a_i x^i}{x^k}$ из $F\left(\left(x\right)\right)$ через $\sum\limits_{i=-k}^{\infty} a_i x^i$. Докажем следующее равенство:

$$F\left(\left(x\right)\right) = \left\{\sum_{i=-k}^{\infty} a_i x^i : a_i \in F, k \in \mathbb{N}\right\}.$$

Пусть $g = c_k x^k \left(1 + h\right)$, где $c_k \neq 0, k \in \mathbb{N}, h \in F(\left(x\right))$. Тогда

$$\frac{f}{g} = \frac{f}{c_k x^k \left(1 + h\right)} = \frac{c_k^{-1} f \cdot \left(1 - h + h^2 - h^3 + \ldots\right)}{x^k} = \sum_{i=-k}^{\infty} a_i x^i.$$

§17. Задачи

1. Доказать, что во всякой конечной полугруппе найдется идемпотент, т. е. элемент e такой, что $e^2 = e$.

2. Найти формулу числа различных расстановок скобок в неассоциативном слове.

3. Пусть S — множество и $*$ — бинарная операция на S такая что $x*(x*y) = y$, $(y*x)*x = y$ для любых $x, y \in S$. Показать, что $*$ коммутативна, но не обязательно ассоциативна.

4. Пусть S — множество и $*$ — бинарная операция на S такая что $x * x = x, (x*y)*z = (y*z)*x$ для любых $x, y, z \in S$. Показать, что $*$ коммутативна и ассоциативна.

5. Доказать, что $\{a_1, \ldots, a_{12} : f(a_i) = a_{i+1}\} \cong \{a_1, \ldots, a_{12} : g(a_i) = a_{i-1}\}$.

6. Доказать, что $\{a_1, \ldots, a_{12} : f(a_i) = a_{i+1}\} \ncong \{a_1, \ldots, a_{12} : g(a_i) = a_{i+2}\}$.

7. Верно ли, что если F — конечное множество ($|F| \geq 2$), то существует бинарная операция $*$ на F такая, что для любых $x, y, z \in F$
   1) $x * z = y * z$ влечет $x = y$ (правое сокращение);
   2) $x * (y * z) \neq (x * y) * z$ (нет ассоциативности).

8. Доказать, что корни n-й степени из единицы образуют группу относительно операции умножения комплексных чисел.

9. Доказать, что конечное множество G, в котором определена ассоциативная бинарная операция и каждое уравнение $ax = b$, $ya = b$ для любых $a, b \in G$ имеет в G не более одного решения, является группой.

10. Доказать, что в группе $\mathbb{A}_4$ нет подгрупп порядка 6.

11. Группа $SL(2, \mathbb{Z})$ содержит элементы $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Найти порядки A и B. Показать, что $\langle A \cdot B \rangle \cong \langle \mathbb{Z}; + \rangle$.

12. Доказать, что группа чётного порядка содержит элемент порядка 2.

13. Рассмотрим группу рациональных чисел по сложению $(\mathbb{Q}, +)$. Пусть $G = \{\frac{n}{2^k} : n, k \in \mathbb{Z}\}$ и $G' = \{\frac{n}{3^k} : n, k \in \mathbb{Z}\}$. Показать, что G и G' — подгруппы в $(\mathbb{Q}, +)$. Выяснить, будут ли группы G и G' изоморфны?

14. Пусть $A = (\mathbb{Z}^2; +)$ и $H = \langle (3,8), (4,-1), (5,4) \rangle \leq A$. Тогда H имеет другое множество порождающих вида $H = \langle (1,b), (0,a) \rangle$ для некоторых $a, b \in \mathbb{Z},\ a > 0$. Найти a.

15. Пусть в группе порядок любого не единичного элемента равен двум. Доказать, что группа абелева.

16. Пусть G — группа, порождённая элементами A и B такими, что $A^4 = B^7 = ABA^{-1}B = 1,\ A^2 \neq 1, B \neq 1$. Сколько элементов из G имеют вид c^2 (являются квадратами) для некоторого $c \in G$? Выписать каждый квадрат как слово от A и B.

17. Пусть A, B — элементы группы G такие, что $ABA = BA^2B, A^3 = 1$ и $B^{2n-1} = 1$ для некоторого $n \in \mathbb{N}$. Доказать, что $B = 1$.

18. Пусть G — группа матриц порядка n с определителем ± 1 и $\mathbb{S}_n$ — симметрическая группа степени n. Для каждой перестановки $\sigma \in \mathbb{S}_n$ определим матрицу $A_\sigma = (a_{ij})$ из G, полагая

$$a_{ij} = \begin{cases} 0, & \text{если } \sigma(i) \neq j, \\ 1, & \text{если } \sigma(i) = j. \end{cases}$$

Проверить, что отображение $\pi : \mathbb{S}_n \mapsto G$, заданное правилом $\pi : \sigma \mapsto A_\sigma$, является гомоморфизмом групп.

19. Известно, что для элементов u_1, u_2, v_1, v_2 группы G выполняются равенства: $u_1v_1 = v_1u_1 = u_2v_2 = v_2u_2,\ u_1^{p_1} = u_2^{p_1} = v_1^{p_2} = v_2^{p_2} = e$, где p_1, p_2 — взаимно простые натуральные числа. Доказать, что $u_1 = u_2, v_1 = v_2$.

20. На множестве комплексных чисел $\mathbb{C}$ определим новую операцию умножения

$$z \odot u = z\overline{u},$$

где $\overline{u}$ — комплексно сопряженное число к числу u. Будет ли $(\mathbb{C}, +, \odot)$ ассоциативным кольцом?

21. Пусть $K = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Показать, что K — кольцо с разложением на простые множители, 3 и $2 \pm \sqrt{-5}$ — простые элементы в K, и $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

22. Доказать, что кольца $\mathbb{Z}$ и $P[x]$, где P — поле, являются факториальными кольцами.

23. Является ли Евклидовым кольцо $F[t, t^{-1}] = \{\sum_{i=-k}^{k} \alpha_i x^i : \alpha_i \in F,\ k \in \mathbb{N}\}$ лорановских многочленов над полем F?

24. Пусть $\mathbb{R}$ — поле действительных чисел. Показать, что матрицы вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ образуют подкольцо кольца $\langle M_n(\mathbb{R}), +, \cdot \rangle$.

25. Пусть $\mathbb{R}$ — поле действительных чисел. Показать, что множество K матриц вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ образует подкольцо кольца $\langle M_2(\mathbb{R}), +, \cdot \rangle$. Является ли это подкольцо полем? Доказать, что в K разрешимо уравнение $x^2 + 1 = 0$.

26. Пусть A — конечномерная ассоциативная алгебра над полем F. Доказать, что если A имеет базис из нильпотентных элементов, то A нильпотентна.

27. Какой наименьший порядок имеет конечное ассоциативное коммутативное кольцо с единицей?

28. В кольце $\mathbb{Z}_{21}$ вычетов по модулю 21:

    1) найти все обратимые (по умножению) элементы с указанием их обратных;

    2) указать все собственные максимальные идеалы кольца $\mathbb{Z}_{21}$;

    3) проверить, будет ли мультипликативная группа (группа по умножению) обратимых элементов циклической.

29. Пусть $(\mathbb{Z}, +, \cdot)$ — кольцо целых чисел, $\mathbb{Z}[x]$ и $\mathbb{Z}_m[x]$ — кольца многочленов от переменной x. Доказать, что отображение

$$\phi : \mathbb{Z}[x] \mapsto \mathbb{Z}_m[x],$$

    заданное правилом $\phi(\sum_i a_i x^i) = \sum_i \{a_i\}_m x^i$, является гомоморфизмом колец. Найти $Ker\,\phi$.

30. Пусть I — идеал кольца $F[x]$. Тогда $I = f(x)F[x]$. Доказать, что элемент $g(x) + I$ обратим в фактор-кольце $F[x]/I$ тогда и только тогда, когда $(g(x), f(x)) = 1$. Найти $(g(x) + I)^{-1}$, если $g(x) + I$ обратим.

Предметный указатель