51

МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ БССР

В.С. Монахов

ПЕРЕСТАНОВКИ И ОПРЕДЕЛИТЕЛИ

Учебное пособие

Гомель 1987

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

УДК 512 (075.8)

Рецензенты: В.А.Ведерников - кандидат физико-математических наук, Брянский государственный педагогический институт имени акад. И.Г.Петровского; С.А.Русаков - кандидат физико-математических наук, Белорусский институт инженеров железнодорожного транспорта

Под редакцией члена-корреспондента АН БССР, доктора физико-математических наук, профессора Л.А.Шеметкова

Пособие содержит изложение следующих трех фрагментов алгебры, предусмотренных программой в I семестре: перестановки, определители, элементы теории групп.

Предназначено для студентов-математиков университетов, а также будет полезно студентам вузов, изучающим соответствующие разделы математики.

20 203 - 63

М———— I2 - 87 I702030000

М 339 - 87

© Гомельский государственный университет (ГГУ), 1987

ВВЕДЕНИЕ

Известно несколько способов построения определителей. Программой курса алгебры для государственных университетов предусмотрено изучение определителей на основе понятия перестановки.

Перестановки, то есть взаимно однозначные отображения конечного множества на себя, находят широкое применение в различных разделах математики. Так, например, еще в 18 веке Ж.Лагранж применил их при исследовании разрешимости алгебраических уравнений в радикалах. Теория групп возникла вначале как теория групп перестановок, а впоследствии многие результаты абстрактной теории групп доказывались с помощью перестановок. Многочисленные применения перестановки получили в дискретной математике.

В настоящем пособии перестановки излагаются в объеме, необходимом для построения теории определителей и для иллюстрации элементов теории групп, изучаемых студентами-математиками университетов в I семестре. Рассматривается разложение перестановки в произведение независимых циклов и в произведение транспозиций. Вводится знак перестановки и устанавливается теорема о том, что знак перестановки τ равен $(-1)^{n-c}$, где n - степень перестановки, а c - число независимых циклов в разложении τ. Изложению теории перестановок предшествуют необходимые сведения об отображениях множеств.

Теория определителей изложена в объеме, традиционном для курса алгебры. Отличие, может быть, состоит лишь в привлечении теоремы об определителе матриц вида $\begin{pmatrix} A & C \\ O & B \end{pmatrix}$, где A и

РЕПОЗИТОРИЙ ГГУ

B – квадратные матрицы порядка n и m соответственно (теорема 8.I), которая находит применение как в построении теории, так и при вычислении определителей конкретных матриц.

Заключительная часть пособия посвящена изложению элементов теории групп, предусмотренных программой I семестра курса алгебры. Для иллюстрации отдельных понятий привлекаются перестановки.

ЛИТЕРАТУРА

Милованов М.В., Тышкевич Р.И., Феденко А.С. Алгебра и аналитическая геометрия. – Мн.: Вышэйшая школа, 1984.

Кострикин А.И. Введение в алгебру. – М.: Наука. 1977.

Куликов Л.Я. Алгебра и теория чисел. – М.: Высшая школа, 1979.

Фаддеев Д.К. Лекции по алгебре. – М.: Наука. 1984.

§ I. БИНАРНЫЕ ОТНОШЕНИЯ

Множества удобно задавать, используя следующую запись: $X=\{\alpha|\beta\}$ – множество X состоит из всех элементов α, для которых выполняется условие β. За некоторыми множествами закреплены стандартные обозначения:

$\mathbb{N}$ – множество натуральных чисел;

$\mathbb{Z}$ – множество целых чисел;

$\mathbb{Q}$ – множество рациональных чисел;

$\mathbb{R}$ – множество действительных чисел.

Пусть теперь X и Y – произвольные множества. Будем рассматривать упорядоченные пары (x,y) элементов $x\in X, y\in Y$. Две пары (x_1,y_1) и (x_2,y_2), где $x_1,x_2\in X, y_1,y_2\in Y$, называются равными, если $x_1=x_2$ и $y_1=y_2$.

Множество всех упорядоченных пар (x,y) называется **декартовым (прямым) произведением** множеств X и Y и обозначается через $X\times Y$. Таким образом,

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

При $X=Y$ говорят о декартовом квадрате множества X и пишут X^2 вместо $X\times X$.

Подмножество F декартового произведения $X\times Y$ называют **бинарным отношением** между X и Y. Совокупность всех $x\in X$, для которых существует такой элемент $y\in Y$, что $(x,y)\in F$, называется **областью определения** бинарного отношения F. **Областью значения** отношения F называется множество всех $y\in Y$ таких, что $(x,y)\in F$ для некоторого $x\in X$.

Пример I. Пусть $X=\{0,1\}$, $Y=\{1,2\}$. Тогда $X\times Y=\{(0,1),(0,2),(1,1),(1,2)\}$ – декартовое произведение множеств X и Y. Выпишем все подмножества произведения $X\times Y$.

$F_1=\phi$, $F_2=\{(0,1)\}$, $F_3=\{(0,2)\}$, $F_4=\{(1,1)\}$,

$F_5=\{(1,2)\}$, $F_6=\{(0,1),(0,2)\}$, $F_7=\{(0,1),(1,1)\}$,

$F_8=\{(0,1),(1,2)\}$, $F_9=\{(0,2),(1,1)\}$, $F_{10}=\{(0,2),(1,2)\}$

РЕПОЗИТОРИЙ ГГУ

$F_{11}=\{(1,1),(1,2)\}$, $F_{12}=\{(0,1),(0,2),(1,1)\}$,

$F_{13}=\{(0,1),(0,2),(1,2)\}$, $F_{14}=\{(0,1),(1,1),(1,2)\}$,

$F_{15}=\{(0,2),(1,1),(1,2)\}$, $F_{16}=X\times Y$.

Любое из шестнадцати подмножеств определяет бинарное отношение между X и Y. Найдите область определения и область значений каждого отношения.

Пусть F – бинарное отношение на множестве X, то есть $F\subseteq X\times X$, и x,y,z – элементы множества X. Отношение F называется

р е ф л е к с и в н ы м, если $(x,x)\in F$ для всех $x\in X$;

с и м м е т р и ч н ы м, если из $(x,y)\in F$ всегда следует $(y,x)\in F$;

а н т и с и м м е т р и ч н ы м, если из $(x,y)\in F$ и $(y,x)\in F$ всегда следует $x=y$;

т р а н з и т и в н ы м, если из $(x,y)\in F$ и $(y,z)\in F$ всегда следует $(x,z)\in F$.

П р и м е р 2. Какими свойствами обладают следующие бинарные отношения на $\mathbb{N}$:

$F_1=\{(x,y)\mid x$ и y взаимно просты$\}$;

$F_2=\{(x,y)\mid x$ делит $y\}$;

$F_3=\{(x,y)\mid x=y^2\}$.

Р е ш е н и е. Подмножество F_1 декартового произведения $\mathbb{N}\times\mathbb{N}$ состоит из всех пар (x,y) натуральных чисел, у которых первый элемент взаимно прост со вторым. F_1 не будет рефлексивным, так как, например, $(4,4)\notin F_1$. Если $(x,y)\in F_1$, то x и y взаимно просты. Поэтому y и x взаимно просты, значит $(y,x)\in F_1$ и F_1 симметрично. Бинарное отношение F_1 не будет транзитивным. Действительно, $(2,3)\in F_1, (3,4)\in F_1$, но $(2,4)\notin F_1$.

Ясно, что F_2 рефлексивно и транзитивно. Но F_2 не является симметричным, поскольку $(3,6)\in F_2$, а $(6,3)\notin F_2$.

Отношение F_3 не будет рефлексивным и симметричным. Если $(x,y)\in F_3$ и $(y,z)\in F_3$, то $x=y^2$, $y=z^2$, поэтому $x=z^4$. Следовательно, $(x,z^2)\in F_3$, а $(x,z)\notin F_3$. Значит, F_3 не будет и транзитивным.

Пусть F – бинарное отношение на множестве X, то есть $F\subseteq X\times X$. Если $(x,y)\in F$, то пишут xFy, что

означает: элемент x находится в бинарном отношении F с элементом y. Бинарные отношения из примера 2 будут записываться так:

F_1: $x F_1 y \iff x$ и y взаимно просты;

F_2: $x F_2 y \iff x$ делит y;

F_3: $x F_3 y \iff x=y^2$.

Отношением э к в и в а л е н т н о с т и называют бинарное отношение, которое рефлексивно, симметрично и транзитивно. Отношение эквивалентности обозначается символом $\sim$. Таким образом, для отношения эквивалентности $\sim$ на множестве X выполняются следующие свойства: рефлексивность – $x\sim x$ для всех $x\in X$; симметричность – если $x\sim y$, то $y\sim x$; транзитивность – если $x\sim y$ и $y\sim z$, то $x\sim z$.

Пусть X – множество с отношением эквивалентности $\sim$. Подмножество $cl(a)=\{b\in X\mid b\sim a\}$ всех элементов, эквивалентных данному элементу a, называют к л а с с о м э к в и в а л е н т н о с т и, с о д е р ж а щ и м a. Совокупность всех классов эквивалентности обозначают $X/\sim$ и называют ф а к т о р м н о ж е с т в о м множества X относительно $\sim$.

Т е о р е м а I.1. Пусть X – множество с отношением эквивалентности $\sim$. Тогда два класса эквивалентности либо совпадают, либо не пересекаются, то есть их пересечение пусто.

Д о к а з а т е л ь с т в о. Пусть $cl(a)\cap cl(b)\neq\emptyset$ и $c\in cl(a)\cap cl(b)$. Тогда $c\sim a$ и $c\sim b$. Так как отношение $\sim$ симметрично, то $b\sim c$, а так как транзитивно, то $b\sim a$ и $b\in cl(a)$.

Если b' – произвольный элемент из $cl(b)$, то $b'\sim b$ и $b'\sim a$, то есть $b'\in cl(a)$ и $cl(b)\subseteq cl(a)$.

Аналогично проверяется обратное включение. Теорема I.1 доказана.

Поскольку $a\in cl(a)$, то справедливо

С л е д с т в и е. Множество с отношением эквивалентности является объединением непересекающихся классов эквивалентности.

Т е о р е м а I.2. Если некоторое множество X являет-

РЕПОЗИТОРИЙ ГГУ

ся объединением непересекающихся подмножеств K_a, то подмножества K_a будут классами эквивалентности для некоторого отношения эквивалентности.

Доказательство. По условию каждый элемент $x \in X$ содержится точно в одном подмножестве K_a. Зададим бинарное отношение $\sim$, считая, что $x \sim y$ в том и только в том случае, когда x и y лежат в одном подмножестве K_a. Очевидно, что $\sim$ рефлексивно, симметрично и транзитивно, то есть $\sim$ – отношение эквивалентности. Если $x \in K_a$, то класс эквивалентности $cl(x)$ содержится в K_a. Обратно, если $y \in K_a$, то $y \sim x$ и $y \in cl(x)$. Таким образом, $K_a \subseteq cl(x)$ и $K_a = cl(x)$. Теорема доказана.

Теоремы I.I и I.2 показывают, что задание отношения эквивалентности на множестве X равносильно представлению X в виде объединения непересекающихся подмножеств.

Пример 3. Зафиксируем натуральное число k. Введем бинарное отношение $\sim$ на $\mathbb{Z}$, считая $x \sim y$ тогда и только тогда, когда равны остатки при делении x и y на k. Отношение $\sim$ будет отношением эквивалентности. Класс эквивалентности $cl(x) = \bar{x}$ состоит из всех целых чисел, которые при делении на k имеют один и тот же остаток. Остатки могут принимать значения $0, 1, \ldots, k-1$. Поэтому фактор-множество состоит из k элементов:

$$\mathbb{Z}/\sim = \{\bar{0}, \bar{1}, \ldots, \overline{k-1}\}.$$

Упорядочением множества называют бинарное отношение на нем, которое рефлексивно, транзитивно и антисимметрично. Упорядочение обозначают символом $\leqslant$. Итак, для множества X с упорядочением $\leqslant$ выполняются следующие свойства: рефлексивность – $x \leqslant x$ для всех $x \in X$; антисимметричность – если $x \leqslant y$ и $y \leqslant x$, то $x = y$; транзитивность – если $x \leqslant y$ и $y \leqslant z$, то $x \leqslant z$.

Множество X с упорядочением $\leqslant$ называют частично упорядоченным. Если для любой пары элементов x и y из X либо $x \leqslant y$, либо $y \leqslant x$, то X называют линейно упорядоченным множеством.

Наибольшим элементом частично упорядоченного

множества X называется элемент $n \in X$ такой, что $x \leqslant n$ для всех $x \in X$, а максимальным – элемент $m \in X$ такой, что из $m \leqslant x$ следует $m = x$. Наибольший элемент всегда максимален, причем наибольший элемент находится в бинарном отношении $\leqslant$ с каждым элементом из X. Однако максимальный элемент может не состоять в бинарном отношении $\leqslant$ с некоторыми элементами из X, в частности, максимальный элемент может не быть наибольшим. Максимальных элементов, если они существуют, может быть несколько. Наибольший элемент, если он существует, определен однозначно.

Подобным образом вводятся наименьший элемент и минимальные.

Очевидно, в конечном частично упорядоченном множестве всегда имеются минимальные и максимальные элементы. В бесконечном множестве $\mathbb{Z}$ с обычным отношением $\leqslant$ нет минимальных и максимальных элементов.

Пример 4. Пусть X – произвольное множество и $\mathcal{P}(X)$ – совокупность всех подмножеств из X. Зададим бинарное отношение B на $\mathcal{P}(X)$, считая $X_1 B X_2$ тогда и только тогда, когда $X_1 \subseteq X_2$. Очевидно, B рефлексивно, антисимметрично и транзитивно. Значит, $\mathcal{P}(X)$ – частично упорядоченное множество. X будет наибольшим, а ϕ – наименьшим элементом в $\mathcal{P}(X)$. Если $x \neq y$ – элементы из X, то одноэлементные множества $\{x\}$ и $\{y\}$ принадлежат $\mathcal{P}(X)$. Кроме того, $\{x\}$ и $\{y\}$, а также $\{y\}$ и $\{x\}$, не находятся в бинарном отношении B. Поэтому $\mathcal{P}(X)$ не будет линейно упорядоченным.

РЕПОЗИТОРИЙ ГГУ

§ 2. ОТОБРАЖЕНИЯ

Пусть даны два множества X и Y. **Отображением** множества X во множество Y называется бинарное отношение φ между X и Y, обладающее следующим свойством: для каждого $x \in X$ существует единственный $y \in Y$ такой, что $x \varphi y$.

Другими словами, отображение φ множества X во множество Y сопоставляет каждому элементу $x \in X$ единственный элемент $y \in Y$. Отображения записывают так:

$$\varphi : X \to Y \qquad \text{или} \qquad X \xrightarrow{\varphi} Y$$

Если при отображении $\varphi : X \to Y$ элемент $x \in X$ переходит в элемент $y \in Y$, то пишут

$$\varphi : x \mapsto y \qquad \text{или} \qquad x \xmapsto{\varphi} y,$$

а элемент y обозначают через $\varphi(x)$ и называют **образом** элемента x.

Итак, чтобы задать отображение $\varphi : X \to Y$, надо определить два множества X и Y и закон φ, по которому каждому элементу множества X ставится в соответствие единственный элемент множества Y.

Два отображения $\varphi : X \to Y$ и $\varphi' : X' \to Y'$ называются **равными**, если $X = X'$, $Y = Y'$ и $\varphi(x) = \varphi'(x)$ для всех $x \in X$. Другими словами, два отображения равны, если они действуют на одних и тех же множествах, и их действие на элементах совпадает.

Пусть $\varphi : X \to Y$ – отображение множества X во множество Y. Если $X_0 \subseteq X$, то $\operatorname{Im} X_0 = \{\varphi(x) \mid x \in X_0\}$ – образ множества X_0 при отображении φ, а $\operatorname{Im} \varphi = \operatorname{Im} X$ – образ отображения φ.

Отображение $\varphi : X \to X$ называется **преобразованием** множества X. **Единичным** или **тождественным** преобразованием множества X называется отображение $\varepsilon_X : X \to X$, переводящее каждый элемент $x \in X$ в себя, то есть $\varepsilon_X(x) = x$.

Отображение $\varphi : X \to Y$ называется

инъективным, если $\varphi(x_1) \neq \varphi(x_2)$ для любых

сюръективным, если $\operatorname{Im} \varphi = Y$;

биективным, если φ одновременно инъективно и сюръективно.

При инъективном отображении различные элементы множества X переходят в различные элементы множества Y. Равенство $\operatorname{Im} \varphi = Y$ означает, что при сюръективном отображении каждый элемент множества Y является образом некоторого элемента множества X. Поэтому сюръективное отображение можно назвать отображением множества X на множество Y.

Биективное отображение называют также **взаимно однозначным** отображением множества X на множество Y. Поэтому, если $\varphi : X \to Y$ – взаимно однозначное отображение множества X на множество Y, то

(1) различные элементы множества X переходят в различные элементы множества Y;

(2) каждый элемент множества Y является образом некоторого элемента множества X.

Из (1) и (2) легко получить

(3) различные элементы множества Y являются образами различных элементов множества X.

Пример 1. Зафиксируем натуральное число k. Зададим отображения $\varphi : \mathbb{N} \to \mathbb{N}$ и $\psi : \mathbb{N} \to \mathbb{N}$, полагая для каждого $x \in \mathbb{N}$

$\varphi(x) = k$ и

$$\psi(x) = \begin{cases} k - x & \text{, если } x < k; \\ k + x & \text{, если } x \geq k. \end{cases}$$

Очевидно, $\operatorname{Im} \varphi = \{k\}$, причем φ не является ни инъективным, ни сюръективным. Так как $\psi(1) = k-1$, $\psi(2) = k-2$, ..., $\psi(k-1) = 1$, $\psi(k) = 2k$, $\psi(k+1) = 2k+1$, ..., то

$\operatorname{Im} \psi = \mathbb{N} - \{k, k+1, \ldots, 2k-1\}$ и ψ не сюръективно. Но ψ инъективно.

Рассмотрим понятие умножения отображений. Пусть даны два отображения: $\varphi : X \to Y$ и $\psi : U \to V$. Предположим, что $Y \subseteq U$. Так как $\varphi(x) \in Y$ и $Y \subseteq U$, то существует образ $\psi(\varphi(x))$, причем $\psi(\varphi(x)) \in V$. Таким образом, мы можем определить отображение

$$\psi\varphi : x \mapsto \psi(\varphi(x))$$

РЕПОЗИТОРИЙ ГГУ

множества X во множество Y, которое называется *произведением* отображений φ и ψ.

Итак, произведение отображений $\varphi: X \to Y$ и $\psi: U \to V$, где $Y \subseteq U$, это такое отображение $\psi\varphi: X \to V$, что $\psi\varphi(x) = \psi(\varphi(x))$ для всех $x \in X$.

Пример 2. Пусть φ и ψ – отображения из примера I. Тогда $\psi\varphi(x) = \psi(\varphi(x)) = \psi(k) = 2k$ для всех $x \in \mathbb{N}$, то есть $\psi\varphi: \mathbb{N} \to \mathbb{N}$ – отображение, которое каждый элемент $x \in \mathbb{N}$ переводит в $2k$.

Рассмотрим произведение $\varphi\psi$. Так как $\varphi\psi(x) = \varphi(\psi(x)) = k = \varphi(x)$, то $\varphi\psi: \mathbb{N} \to \mathbb{N}$ – отображение, которое совпадает с φ, то есть $\varphi\psi = \varphi$.

В частности, $\psi\varphi \neq \varphi\psi$, то есть умножение отображений некоммутативно.

Теорема 2.I. Умножение отображений подчиняется закону ассоциативности, то есть если $f: X \to Y$, $\varphi: Y \to U$ и $\psi: U \to V$ – три отображения, то $\psi(\varphi f) = (\psi\varphi)f$.

Доказательство. Напомним, что два отображения равны, если они действуют на одних и тех же множествах и их действие на элементах совпадает. Отображение φf элементы множества X переводит в элементы множества U, поэтому $\psi(\varphi f)$ действует из X в V. Аналогично, $\psi\varphi$ действует из Y в V, поэтому $(\psi\varphi)f$ переводит элементы X в элементы V. Итак, оба отображения $\psi(\varphi f)$ и $(\psi\varphi)f$ действуют из X в V.

Согласно определению произведения отображений имеем

$$\psi(\varphi f)(x) = \psi(\varphi f(x)) = \psi(\varphi(f(x))) = (\psi\varphi)(f(x)) = (\psi\varphi)f(x),$$

то есть действия $\psi(\varphi f)$ и $(\psi\varphi)f$ на элементах совпадает. Теорема доказана.

§ 3. ОБРАТНОЕ ОТОБРАЖЕНИЕ

Пусть $\varphi: X \to Y$ – отображение множества X в Y, а ε_X и ε_Y – тождественные преобразования множеств X и Y. Легко проверить, что $\varphi\varepsilon_X = \varphi$ и $\varepsilon_Y\varphi = \varphi$, то есть ε_X и ε_Y играют роль единичного элемента при умножении отображений.

Естественный интерес представляют отображения, произведение которых является тождественным преобразованием.

Теорема 3.I. Если $\varphi: X \to Y$ и $\psi: Y \to X$ – отображения, для которых $\psi\varphi = \varepsilon_X$, то φ инъективно, а ψ сюръективно.

Доказательство. Предположим, что $\varphi(x_1) = \varphi(x_2)$, для некоторых $x_1, x_2 \in X$. Тогда

$$x_1 = \varepsilon_X(x_1) = \psi\varphi(x_1) = \psi(\varphi(x_1)) = \psi(\varphi(x_2)) = \psi\varphi(x_2) = \varepsilon_X(x_2) = x_2,$$

то есть φ инъективно.

Если x – произвольный элемент из X, то

$$x = \varepsilon_X(x) = \psi\varphi(x) = \psi(\varphi(x)),$$

то есть x является образом элемента $\varphi(x) \in Y$ при отображении ψ. Значит, ψ сюръективно. Теорема доказана.

Отображение $\varphi: X \to Y$ называется *обратимым*, если существует такое отображение $\psi: Y \to X$, что $\psi\varphi = \varepsilon_X$, а $\varphi\psi = \varepsilon_Y$. В этом случае отображение ψ называют *обратным* к отображению φ и обозначают через φ^{-1}.

Теорема 3.2. Отображение обратимо тогда и только тогда, когда оно биективно.

Доказательство. Предположим, что $\varphi: X \to Y$ – обратимое отображение, то есть существует такое отображение $\psi: Y \to X$, что $\psi\varphi = \varepsilon_X$ и $\varphi\psi = \varepsilon_Y$. Из теоремы 3.I и первого равенства следует, что φ инъективно, а ψ сюръективно. Из второго равенства следует, что φ сюръективно, а ψ инъективно. Итак, φ – биективное отображение, причем обратное к нему отображение ψ также биективно.

Допустим теперь, что $\varphi: X \to Y$ – биективное отображение, и покажем, что φ обратимо.

Рассмотрим отображение $\psi: Y \to X$, определенное так:

РЕПОЗИТОРИЙ ГГУ

если $\varphi: x \mapsto y$, то $\psi: y \mapsto x$. Так как φ биективно, то каждый элемент $y \in Y$ является образом единственного элемента $x \in X$, см. свойство (3) биективных отображений. Поэтому $\psi: y \mapsto x$, где $y = \varphi(x)$ является отображением множества Y во множество X. Ясно, что $\psi\varphi = \varepsilon_X$ и $\varphi\psi = \varepsilon_Y$.

Следствие. Если отображение биективно, то обратное к нему отображение также биективно.

Заметим, что в доказательстве теоремы 3.2 мы указали *способ построения* обратного отображения. А именно, если $\varphi: X \to Y$ – биективное отображение, то обратное отображение $\varphi^{-1}: Y \to X$ действует так: $\varphi^{-1}: y \mapsto x$ тогда и только тогда, когда $\varphi: x \mapsto y$.

Следующая теорема показывает, что обратное отображение определяется однозначно.

Теорема 3.3. Обратимое отображение обладает единственным обратным отображением.

Доказательство. Пусть $\varphi: X \to Y$ – обратимое отображение. Допустим, что $\psi_1: Y \to X$ и $\psi_2: Y \to X$ – обратные к φ отображения, то есть $\psi_1\varphi = \psi_2\varphi = \varepsilon_X$ и $\varphi\psi_1 = \varphi\psi_2 = \varepsilon_Y$. Тогда

$$\psi_1(y) = \varepsilon_X\psi_1(y) = (\psi_2\varphi)\psi_1(y) = \psi_2(\varphi\psi_1)(y) = \psi_2\varepsilon_Y(y) = \psi_2(y)$$

то есть $\psi_1 = \psi_2$. В цепочке равенств мы использовали ассоциативность умножения отображений (теорема 2.1) и свойства: $\varepsilon_X\psi_1 = \psi_1$, $\psi_2\varepsilon_Y = \psi_2$.

Теорема 3.4. Если $\varphi: X \to Y$, $\psi: Y \to U$ – биективные отображения, то произведение $\psi\varphi$ также биективно и $(\psi\varphi)^{-1} = \varphi^{-1}\psi^{-1}$.

Доказательство. Ясно, что $\psi\varphi: X \to U$ биективное отображение. По теореме 3.2 существуют обратные отображения $\varphi^{-1}: Y \to X$ и $\psi^{-1}: U \to Y$, а их произведение $\varphi^{-1}\psi^{-1}$ есть отображение из U в X. Используя ассоциативность умножения отображений заключаем, что

$$(\psi\varphi)(\varphi^{-1}\psi^{-1}) = ((\psi\varphi)\varphi^{-1})\psi^{-1} = (\psi(\varphi\varphi^{-1}))\psi^{-1} = (\psi\varepsilon_Y)\psi^{-1} = \psi\psi^{-1} = \varepsilon_U;$$

$$(\varphi^{-1}\psi^{-1})(\psi\varphi) = ((\varphi^{-1}\psi^{-1})\psi)\varphi = (\varphi^{-1}(\psi^{-1}\psi))\varphi = (\varphi^{-1}\varepsilon_Y)\varphi = \varphi^{-1}\varphi = \varepsilon_X,$$

то есть $\varphi^{-1}\psi^{-1}$ – обратное отображение к $\psi\varphi$. Значит, $(\psi\varphi)^{-1} = \varphi^{-1}\psi^{-1}$ и теорема доказана.

§ 4. ПЕРЕСТАНОВКИ

Пусть $X = \{1, 2, \ldots, n\}$. Биекция, то есть взаимно однозначное отображение множества X на себя, называется *перестановкой*. Совокупность всех перестановок множества X называют *симметрической группой степени* n и обозначают через S_n. Перестановку $\tau \in S_n$ удобно изображать двухстрочной таблицей, полностью указывая образы всех элементов:

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix}$$

или

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

где $\{a_1, a_2, \ldots, a_n\} = X$, $\tau: 1 \mapsto a_1, 2 \mapsto a_2, \ldots, n \mapsto a_n$ или кратко $a_k = \tau(k)$.

Тождественное преобразование ε_X является биекцией и поэтому $\varepsilon_X \in S_n$. Очевидно, что

$$\varepsilon = \varepsilon_X = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Произведение $\sigma\tau$ двух перестановок σ и τ находится как произведение отображений: $\sigma\tau(k) = \sigma(\tau(k))$, $k = 1, 2, \ldots, n$. Например, перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

РЕПОЗИТОРИЙ ГГУ

принадлежащие симметрической группе S_4 степени 4, перемножаются так

$$\sigma\tau = \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{matrix}1&2&3&4\\\downarrow&\downarrow&\downarrow&\downarrow\\3&4&1&2\\\downarrow&\downarrow&\downarrow&\downarrow\\2&1&3&4\end{matrix} = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}.$$

Вычислим $\tau\sigma$.

$$\tau\sigma = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} = \begin{matrix}1&2&3&4\\\downarrow&\downarrow&\downarrow&\downarrow\\3&4&2&1\\\downarrow&\downarrow&\downarrow&\downarrow\\1&2&4&3\end{matrix} = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}.$$

В частности, умножение перестановок некоммутативно.

Из теорем 3.4, 2.I, 3.2 получаем следующие свойства умножения:

произведение двух перестановок вновь есть перестановка, то есть если $\tau \in S_n$ и $\sigma \in S_n$, то $\tau\sigma \in S_n$;

умножение перестановок ассоциативно, то есть $(\chi\tau)\sigma = \chi(\tau\sigma)$ для всех $\chi, \tau, \sigma \in S_n$;

существует единичная перестановка, то есть такая перестановка $\varepsilon \in S_n$, что $\tau\varepsilon = \varepsilon\tau = \tau$ для всех $\tau \in S_n$;

каждая перестановка обладает обратной перестановкой, то есть для любой перестановки $\tau \in S_n$ существует такая перестановка $\tau^{-1} \in S_n$, что $\tau\tau^{-1} = \tau^{-1}\tau = \varepsilon$.

В доказательстве теоремы 3.2 мы построили обратное отображение. Обратную перестановку τ^{-1} получим переставив строки местами в перестановке τ. Например,

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

Если A – конечное множество, то $|A|$ обозначает число элементов во множестве A. Через $n!$ (читается эн факториал) обозначается произведение $1\cdot2\cdot3\dots n$, то есть $n! = 1\cdot2\cdot3\dots n$. Например, $1! = 1$; $2! = 2$; $3! = 6$; $4! = 24$; $5! = 120$; $6! = 720$ и т.д.

Т е о р е м а 4.I. Число перестановок степени n равно

$n!$, то есть $|S_n| = n!$.

Д о к а з а т е л ь с т в о. Надо сосчитать число различных перестановок

$$\tau = \begin{pmatrix}1&2&\dots&n\\\tau(1)&\tau(2)&\dots&\tau(n)\end{pmatrix},$$

где $\{\tau(1), \tau(2), \dots, \tau(n)\} = \{1, 2, \dots, n\}$. Перестановка τ символ I может перевести в любой символ из множества $\{1, 2, \dots, n\}$, для чего существует n вариантов. Зафиксируем образ $\tau(1)$ символа I. Так как τ – инъекция, то $\tau(2)$ не может совпасть с $\tau(1)$, поэтому в качестве $\tau(2)$ можно выбрать любой из оставшихся $(n-1)$ символов. Всего различных пар $\tau(1), \tau(2)$ мы получим $n(n-1)$. Если $\tau(1)$ и $\tau(2)$ зафиксированы, то в качестве $\tau(3)$ можно выбрать любой отличный от $\tau(1)$ и $\tau(2)$ символ, то есть для $\tau(3)$ имеется $(n-2)$ варианта, и т.д. Всего число вариантов выбора $\tau(1), \tau(2), \dots, \tau(n)$ равно $n(n-1)(n-2)\dots2\cdot1 = n!$. Теорема доказана.

Перестановка

$$\tau = \begin{pmatrix}a_1&a_2&\dots&a_{k-1}&a_k&a_{k+1}&\dots&a_n\\a_2&a_3&\dots&a_k&a_1&a_{k+1}&\dots&a_n\end{pmatrix}$$

называется ц и к л о м д л и н ы k и кратко записывается так: $\tau = (a_1 a_2 \dots a_k)$. В этом случае

$$a_1 \xrightarrow{\tau} a_2 \xrightarrow{\tau} a_3 \xrightarrow{\tau} \dots \xrightarrow{\tau} a_k \xrightarrow{\tau} a_1,$$

остальные символы перестановка τ переводит в себя.

Циклы без общих символов называются н е з а в и с и м ы м и.

Произвольную перестановку τ можно записать в виде произведения независимых циклов. Для этого берем произвольный символ $a_1 \in X$ и находим $\tau(a_1) = a_2$. Если $a_2 = a_1$, то получаем цикл (a_1) длины I. Если $a_2 \neq a_1$, то берем $\tau(a_2) = a_3$. Так как τ – инъекция и $\tau(a_1) = a_2$, то $a_3 = \tau(a_2) \neq a_2$. Если $a_3 = a_1$, то имеем цикл $(a_1 a_2)$. При $a_3 \neq a_1$ находим $a_4 = \tau(a_3)$. Если $a_4 \in \{a_1, a_2, a_3\}$, то инъективность τ приводит к тому, что $a_4 = a_1$ и получен цикл $(a_1 a_2 a_3)$. И так далее. Перебирая все символы

РЕПОЗИТОРИЙ ГГУ

из X, получаем запись перестановки в виде произведения независимых циклов. Очевидно, такое разложение единственно.

Пример 1. Записать в виде произведения независимых циклов перестановку

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}.$$

Решение. Перестановка переводит $1 \mapsto 5 \mapsto 2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 6 \mapsto 4$, поэтому

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix} = (1\,5\,2)(3)(4\,6).$$

Пример 2. Записать в виде таблицы перестановку

$$(1\,3\,5)(2)(4\,6\,7)$$

Решение. Перестановка переводит $1 \mapsto 3 \mapsto 5 \mapsto 1$, $2 \mapsto 2$, $4 \mapsto 6 \mapsto 7 \mapsto 4$, поэтому

$$(1\,3\,5)(2)(4\,6\,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 6 & 1 & 7 & 4 \end{pmatrix}.$$

Поскольку независимые циклы не имеют общих символов, то они являются коммутирующими перестановками. Циклы с общими символами не коммутируют. Например, $(1\,2)(1\,3) = (1\,5\,2)$, а $(1\,3)(1\,2) = (1\,2\,3)$.

Цикл длины 2 называется **транспозицией**. Транспозиция $(i\,j)$ все элементы, отличные от i и j, переводит в себя

$$(i\,j) = \begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & 3 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

Лемма 4.2. Каждый цикл длины k можно записать в виде произведения $k-1$ транспозиций.

Доказательство. Пусть $(a_1 a_2 \dots a_k)$ – цикл длины k. Тогда

$$(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2).$$

Записав правую часть, убеждаемся в справедливости этого равенства.

Теорема 4.3. Всякую перестановку $\tau \in S_n$ можно

записать в виде произведения $n-c$ транспозиций, где c – число независимых циклов (включая циклы длины 1).

Доказательство. Пусть

$$\tau = (i_1 i_2 \dots i_{k_1})(j_1 j_2 \dots j_{k_2}) \dots (t_1 t_2 \dots t_{k_c})$$

запись перестановки τ в виде произведения независимых циклов. Так как циклы независимы, то $k_1 + k_2 + \dots + k_c = n$. По лемме 4.2 каждый цикл длины k разложим на $k-1$ транспозицию. Поэтому вся перестановка τ распадается в произведение

$$(k_1 - 1) + (k_2 - 1) + \dots + (k_c - 1) = (k_1 + \dots + k_c) - (1 + \dots + 1) = n - c$$

транспозиций.

Пример 3. Разложить в произведение транспозиций перестановку

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

Решение. Вначале запишем перестановку в виде произведения независимых циклов, а затем каждый цикл представим как произведение транспозиций

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 4 & 8 & 5 & 7 & 2 & 3 \end{pmatrix} = (1\,6\,7\,2)(3\,4\,8)(5) =$$

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

§ 5. ЗНАК ПЕРЕСТАНОВКИ

Нам понадобится функция $y = \operatorname{sign} x$ (signum – знак), которая отображает $\mathbb{R}$ на множество $\{-1, 0, 1\}$ следующим образом

$$x \mapsto \operatorname{sign} x = \begin{cases} -1, & \text{если } x < 0, \\ 0, & \text{если } x = 0, \\ 1, & \text{если } x > 0 \end{cases}$$

Очевидно, $\operatorname{sign}(xy) = \operatorname{sign} x \operatorname{sign} y$ – знак произведения двух действительных чисел равен произведению знаков этих

РЕПОЗИТОРИЙ ГГУ

чисел.

Введем отображение $sgn : S_n \to \{-1, 1\}$, считая

$$(I) \quad sgn\,\tau = sign \prod_{\substack{i \neq k \\ \{i,k\} \subset X}} \frac{i-k}{\tau(i)-\tau(k)},$$

где $\tau \in S_n$, $X = \{1, 2, \ldots, n\}$. Поскольку τ – биекция, то $\tau(i) \neq \tau(k)$ при $i \neq k$, и знаменатель каждой дроби отличен от нуля. Произведение вычисляется по всем неупорядоченным подмножествам $\{i,k\}$ различных натуральных чисел, значит каждая дробь отличне от нуля и $sgn\,\tau \in \{-1, 1\}$, то есть $Im\, sgn \subset \{-1, 1\}$. Дробь

$$\frac{i-k}{\tau(i)-\tau(k)} = \frac{k-i}{\tau(k)-\tau(i)}$$

встречается по одному разу для каждой пары $\{i,k\}$. Поэтому мы можем знак произведения вычислять только по парам $\{i,k\}$, у которых $i > k$. В этом случае

$$sgn \frac{i-k}{\tau(i)-\tau(k)} = sgn\,(\tau(i)-\tau(k))$$

и равенство (I) примет вид

$$(I') \quad sgn\,\tau = sign \prod_{1 \le k < i \le n} (\tau(i)-\tau(k)).$$

Перестановку τ назовем **четной**, если $sgn\,\tau = 1$ и **нечетной**, если $sgn\,\tau = -1$. Ясно, что $sgn\,\varepsilon = 1$.

Теорема 5.1. Если σ и $\tau \in S_n$, то $sgn\,\sigma\tau = sgn\,\sigma \cdot sgn\,\tau$, то есть знак произведения перестановок равен произведению знаков.

Доказательство. Пусть

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}, \quad \sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix},$$

тогда

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

и

$$sgn\,\sigma \cdot sgn\,\tau = sign \prod_{a_i > a_k} \frac{a_i - a_k}{b_i - b_k} \cdot sign \prod_{\{i,k\} \subset X} \frac{i-k}{a_i - a_k} =$$

$$= sign \prod_{\substack{i \neq k \\ \{i,k\} \subset X}} \frac{a_i - a_k}{b_i - b_k} \cdot \frac{i-k}{a_i - a_k} = sign \prod_{\substack{i \neq k \\ \{i,k\} \subset X}} \frac{i-k}{b_i - b_k} = sgn\,\sigma\tau.$$

Следствие 1. Произведение двух четных или двух нечетных перестановок есть четная перестановка.

Следствие 2. Произведение четной и нечетной перестановки есть нечетная перестановка.

Следствие 3. Любая перестановка имеет ту же четность, что и ей обратная, то есть $sgn\,\tau = sgn\,(\tau^{-1})$.

Теорема 5.2. Любая транспозиция является нечетной перестановкой.

Доказательство. Рассмотрим вначале транспозицию

$$\tau = (1\,2) = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}.$$

Здесь $\tau(1) = 2, \tau(2) = 1$ и $\tau(i) = i$ при $i \geq 3$. Из формулы (I') получаем, что $sgn\,(1\,2) = -1$.

Пусть теперь $\sigma = (a_1 a_2)$ – произвольная транспозиция и

$$\chi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix},$$

где $\{a_1, a_2, \ldots, a_n\} = X$. Так как

$$\chi(1\,2)\chi^{-1} = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ 1 & 2 & \ldots & n \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_2 & a_1 & a_3 & \ldots & a_n \end{pmatrix} = (a_1 a_2) = \sigma,$$

то

РЕПОЗИТОРИЙ ГГУ

$$\operatorname{sgn}\sigma = \operatorname{sgn}(\chi(12)\chi^{-1}) = \operatorname{sgn}\chi \cdot \operatorname{sgn}(12)\cdot\operatorname{sgn}\chi^{-1} = -1.$$

Следствие. Если $\tau \in S_n$ и c – число независимых циклов, в произведение которых разлагается τ, то $\operatorname{sgn}\tau = (-1)^{n-c}$.

Доказательство. Перестановку τ по теореме 4.3 можно записать в виде произведения $n-c$ транспозиций. Остается применить теоремы 5.1 и 5.2.

Пример 1. Вычислить знак перестановки

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

Решение. Так как

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 9 & 5 & 1 & 7 & 6 & 3 & 8 \end{pmatrix} = (145)(2)(398)(67),$$

то $n-c = 9-4 = 5$, и перестановка нечетная.

Лемма 5.3. Зафиксируем перестановку $\pi \in S_n$. Каждое из отображений

$$\alpha: \tau \mapsto \tau^{-1};$$
$$\beta: \tau \mapsto \tau\pi;$$
$$\gamma: \tau \mapsto \pi\tau$$

является биекцией множества S_n. Поэтому

$$S_n = \{\tau^{-1} \mid \tau \in S_n\};$$
$$S_n = \{\tau\pi \mid \tau \in S_n\},$$
$$S_n = \{\pi\tau \mid \tau \in S_n\}.$$

Доказательство. Инъективность α следует из того, что перестановка τ^{-1} получается из τ переменой строк. Так как каждая перестановка $\chi \in S_n$ является обратной для χ^{-1}, то α сюръективно. Значит, α – биекция. Поэтому $\operatorname{Im}\alpha = \{\tau^{-1} \mid \tau \in S_n\} = S_n$.

Если $\tau_1\pi = \tau_2\pi$, то $\tau_1\pi\pi^{-1} = \tau_2\pi\pi^{-1}$, откуда $\tau_1 = \tau_2$. Итак, β – инъекция. Если χ – произвольная перестановка из S_n, то $\chi = (\chi\pi^{-1})\pi$, то есть χ является образом перестановки $\chi\pi^{-1}$ при отображении β. Значит,

β – сюръекция и $\operatorname{Im}\beta = \{\tau\pi \mid \tau \in S_n\} = S_n$.

Для отображения γ проверка аналогична. Лемма доказана.

Совокупность всех четных перестановок из S_n обозначим через A_n и назовем **знакопеременной группой степени** n.

Теорема 5.4. Совокупность A_n всех четных перестановок степени n обладает следующими свойствами:

(1) если τ и $\sigma \in A_n$, то $\tau\sigma \in A_n$;

(2) тождественная перестановка ε четная, то есть $\varepsilon \in A_n$;

(3) если $\tau \in A_n$, то $\tau^{-1} \in A_n$;

(4) $|A_n| = n!/2$.

Доказательство. Первые три свойства уже доказаны, см. следствие теоремы 5.1. Ясно, что $S_n = A_n \cup \bar{A}_n$ и $A_n \cap \bar{A}_n = \phi$, где $\bar{A}_n$ – совокупность нечетных перестановок степени n. Отображение $\gamma: \tau \mapsto (12)\tau$ по лемме 5.3 биективно, причем перестановки τ и $(12)\tau$ имеют разную четность. Поэтому $\operatorname{Im}A_n = \bar{A}_n$, а $\operatorname{Im}\bar{A}_n = A_n$. Следовательно, $|A_n| = |\bar{A}_n| = n!/2$.

Рассмотрим симметрические группы S_n степени n для $n = 1, 2, 3$.

Очевидно, $S_1 = \{\varepsilon\}, A_1 = \{\varepsilon\}$, где $\varepsilon = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Ясно также, что $S_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\} = \{\varepsilon, (12)\}$, а $A_2 = \{\varepsilon\}$.

Пусть $n = 3$ и $X = \{1, 2, 3\}$. Выпишем все перестановки множества X и разложим их в произведение независимых циклов.

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)(1),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)(2),$$

РЕПОЗИТОРИЙ ГГУ

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2)(3),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$$

Итак, $S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}$, а $A_3 = \{\varepsilon, (123), (132)\}$.

Составим таблицы умножения для S_3 и A_3. На пересечении "строки" τ и "столбца" π ставим произведение $\tau\pi$

S_3	ε	(12)	(13)	(23)	(123)	(132)
ε	ε	(12)	(13)	(23)	(123)	(132)
(12)	(12)	ε	(132)	(123)	(23)	(13)
(13)	(13)	(123)	ε	(132)	(12)	(23)
(23)	(23)	(132)	(123)	ε	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	ε
(132)	(132)	(23)	(12)	(13)	ε	(123)

A_3	ε	(123)	(132)
ε	ε	(123)	(132)
(123)	(123)	(132)	ε
(132)	(132)	ε	(123)

Аналогично можно было бы поступить и с S_4. Но $|S_4| = 4! = 24$, и при составлении таблицы умножения для S_4 пришлось бы заполнить $24 \cdot 24 = 576$ клеток.

§ 6. МАТРИЦЫ

Пусть $\mathbb{R}$ – множество действительных чисел, k и ℓ – натуральные числа. $k \times \ell$ -Матрицей над $\mathbb{R}$ назовем прямоугольную таблицу

$$(I) \qquad A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1\ell} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2\ell} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{i\ell} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kj} & \dots & a_{k\ell} \end{pmatrix}$$

составленную из действительных чисел.

Элементы $a_{i1}, a_{i2}, \dots, a_{i\ell}$ имеют первым индексом число i и составляют в матрице ее i -ю **строку**, которая обозначается через $A_i = (a_{i1}\, a_{i2} \dots a_{i\ell})$. Элементы $a_{1j}, a_{2j}, \dots, a_{kj}$ имеют вторым индексом число j и составляют j -й **столбец**, который обозначается через

$$A^j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{kj} \end{pmatrix} = [a_{1j}\, a_{2j} \dots a_{kj}].$$

Элемент a_{ij} стоит в i -й строке и в j -ом столбце. Матрицу A записывают в виде таблицы (I), либо сокращенно

$$A = (a_{ij}),\ i = 1, 2, \dots, k;\ j = 1, 2, \dots, \ell,$$

либо перечислив все ее строки

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_k \end{pmatrix} = [A_1 A_2 \dots A_k],$$

либо перечислив все ее столбцы

$$A = (A^1 A^2 \dots A^\ell)$$

Ясно, что $A = (a_{ij})$ – квадратная

РЕПОЗИТОРИЙ ГГУ

рица порядка k.

$k \times \ell$ -Матрица $A=(a_{ij})$ и $m \times n$ -матрица $B=(b_{ij})$ считаются **равными**, если $k=m$, $\ell=n$ и $a_{ij}=b_{ij}$ для всех i и j.

Матрицу, все элементы которой равны нулю, назовем **нулевой** матрицей и обозначим через O, то есть

$$O=\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Пусть теперь $A=(a_{ij})$ и $B=(b_{ij})$ - $k \times \ell$ -матрицы. **Суммой** $k \times \ell$ матриц A и B называется $k \times \ell$ -матрица $C=(c_{ij})$ такая, что $c_{ij}=a_{ij}+b_{ij}$ для всех i и j, то есть

$$\begin{pmatrix} a_{11} & \dots & a_{1\ell} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{k\ell} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1\ell} \\ \dots & \dots & \dots \\ b_{k1} & \dots & b_{k\ell} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1\ell}+b_{1\ell} \\ \dots & \dots & \dots \\ a_{k1}+b_{k1} & \dots & a_{k\ell}+b_{k\ell} \end{pmatrix}$$

Произведением fA действительного числа f и матрицы A называется $k \times \ell$ -матрица $D=(d_{ij})$ такая, что $d_{ij}=f a_{ij}$ для всех i и j, то есть

$$f\begin{pmatrix} a_{11} & \dots & a_{1\ell} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{k\ell} \end{pmatrix} = \begin{pmatrix} fa_{11} & \dots & fa_{1\ell} \\ \dots & \dots & \dots \\ fa_{k1} & \dots & fa_{k\ell} \end{pmatrix}.$$

Перечислим следующие очевидные свойства сложения матриц и умножения числа на матрицу.

1. Сложение матриц коммутативно, то есть $A+B=B+A$.
2. Сложение матриц ассоциативно, то есть $(A+B)+C=A+(B+C)$;
3. $A+O=A$;
4. $A+(-A)=O$, где $-A$ - матрица, противоположная матрице A;
5. $1 \cdot A=A$, $0 \cdot A=O$.

6. $(fg)A=f(gA)$.
7. $f(A+B)=fA+fB$
8. $(f+g)A=fA+gA$, где f и $g \in \mathbb{R}$.

Пример I. Найти 2×2 -матрицу X, удовлетворяющую условию

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

Решение. Обозначим $X=\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ и, подставив в уравнение, вычислим левую часть

$$\begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix} - \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 2-x_1 & 4-x_2 \\ 6-x_3 & 8-x_4 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

Две матрицы равны, если равны элементы, стоящие на одинаковых местах. Поэтому последнее равенство матриц приводит к уравнениям

$$2-x_1=3,\ 4-x_2=0,\ 6-x_3=0,\ 8-x_4=3,$$

откуда $x_1=-1$, $x_2=4$, $x_3=6$, $x_4=5$.

Ответ. $X=\begin{pmatrix} -1 & 4 \\ 6 & 5 \end{pmatrix}$.

Рассмотрим теперь умножение матриц. Пусть $A=(a_{ij})$ - $k \times \ell$ -матрица, $B=(b_{ij})$ - $\ell \times m$ -матрица. Мы сразу требуем, чтобы число столбцов первой матрицы было равно числу строк второй матрицы.

Произведением i-й строки A_i на j-й столбец B^j определяется так

$$(2)\qquad A_i B^j = (a_{i1}\ a_{i2}\ \dots\ a_{i\ell})\begin{bmatrix} b_{1j} \\ b_{2j} \\ \dots \\ b_{\ell j} \end{bmatrix} =$$

$$= a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{i\ell}b_{\ell j} = \sum_{t=1}^{\ell} a_{it}b_{tj}.$$

Обратим внимание, что произведением строки на столбец является число.

Произведением $k \times \ell$ -матрицы $A=(a_{ij})$ и

РЕПОЗИТОРИЙ ГГУ

$\ell \times m$ -матрицы $B=(b_{ij})$ называется $k \times m$ -матрица

$$AB=\begin{pmatrix} A_1B^1 & A_1B^2 & \dots & A_1B^m \\ A_2B^1 & A_2B^2 & \dots & A_2B^m \\ \dots & \dots & \dots & \dots \\ A_kB^1 & A_kB^2 & \dots & A_kB^m \end{pmatrix} \tag{3}$$

Для получения первой строки произведения AB надо первую строку матрицы A умножить на каждый столбец матрицы B. Для получения второй строки произведения AB надо вторую строку матрицы A умножить на каждый столбец матрицы B и т.д. Вообще, в произведении AB на пересечении i -й строки и j -го столбца стоит число, равное произведению i -й строки матрицы A на j -й столбец матрицы B, которое вычисляется по формуле (2).

Вывод: 1) Перемножать можно матрицы A и B, у которых число столбцов первого сомножителя A равно числу строк второго сомножителя B. Если это требование выполняется, то говорят, что умножение матриц A и B определено. Отметим, что умножение квадратных матриц одного порядка всегда определено.

2) Перемножать матрицы следует по правилу "строки на столбец". Строка первого сомножителя умножается на столбец второго сомножителя по формуле (2).

3) Произведением является $k \times m$ -матрица, определяемая формулой (3). Здесь k – число строк первого сомножителя, m – число столбцов второго сомножителя.

Пример 2. Перемножить матрицы

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

Решение.

$$\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 4 & 3 \\ -1 & 0 & 2 \end{pmatrix}=\begin{pmatrix} 1\cdot1+2\cdot(-1) & 1\cdot4+2\cdot0 & 1\cdot3+2\cdot2 \\ 0\cdot1+(-1)\cdot(-1) & 0\cdot4+(-1)\cdot0 & 0\cdot3+(-1)\cdot2 \end{pmatrix}=$$

$$=\begin{pmatrix} -1 & 4 & 7 \\ 1 & 0 & -2 \end{pmatrix}$$

Квадратную матрицу

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

порядка ℓ назовем единичной и обозначим через E_ℓ.

Теорема 6.1. Если A – $k \times \ell$ -матрица, то

$$AE_\ell = E_kA = A.$$

Доказательство. Вычислив произведения AE_ℓ и E_kA получим матрицу A.

Теорема 6.2. Умножение матриц ассоциативно. Более точно, если определено одно из произведений $(AB)C$, $A(BC)$, то определено и другое, и $(AB)C = A(BC)$.

Доказательство. Пусть определено произведение $(AB)C$, а значит и AB. Если $A=(a_{ij})$ – $k \times \ell$ -матрица, то $B=(b_{ij})$ – $\ell \times m$ -матрица, а AB – $k \times m$ -матрица. Поэтому $C=(c_{ij})$ должна быть $m \times n$ -матрицей, а $(AB)C$ – $k \times n$ -матрицей.

Теперь BC – $\ell \times n$ -матрица, а $A(BC)$ – $k \times n$ -матрица, то есть размеры матриц $(AB)C$ и $A(BC)$ совпадают. Осталось показать, что у этих матриц равны элементы, стоящие на одинаковых местах, то есть $(AB)_i C^j = A_i(BC)^j$ для всех i и j.

Так как $(AB)_i = (A_iB^1\ A_iB^2 \dots A_iB^m)$,

где $A_iB^t = \sum_{s=1}^{\ell} a_{is}b_{st}$, то

$$(AB)_i C^j = (A_iB^1\ A_iB^2 \dots A_iB^m)[c_{1j}\ c_{2j} \dots$$

$$\dots c_{mj}] = (A_iB^1)c_{1j} + (A_iB^2)c_{2j} + \dots$$

$$\dots + (A_iB^m)c_{mj} = \sum_{t=1}^{m}\left(\sum_{s=1}^{\ell} a_{is}b_{st}\right)c_{tj}.$$

РЕПОЗИТОРИЙ ГГУ

Для матрицы BC из (2) и (3) получаем

$$(BC)^j=[B_1C^j\ B_2C^j\ \dots\ B_\ell C^j],$$

где

$$B_sC^j=\sum_{t=1}^{m}b_{st}c_{tj}.$$

Поэтому

(5) $$A_i(BC)^j=(a_{i1}a_{i2}\dots a_{i\ell})[B_1C^j\dots$$
$$\dots B_\ell C^j]=a_{i1}B_1C^j+a_{i2}B_2C^j+\dots$$
$$\dots+a_{i\ell}B_\ell C^j=\sum_{s=1}^{\ell}a_{is}\Big(\sum_{t=1}^{m}b_{st}c_{tj}\Big).$$

Поскольку правые части (4) и (5) равны, то $(AB)_iC^j=A_i(BC)^j$, что и требовалось доказать.

Доказательство следующих двух теорем проведем лишь для квадратных матриц.

Т е о р е м а 6.3. Умножение матриц дистрибутивно относительно сложения, то есть $(A+B)\cdot C=AC+BC$.

Д о к а з а т е л ь с т в о. Пусть $A=(a_{ij})$, $B=(b_{ij})$, $C=(c_{ij})$ – квадратные матрицы порядка n. Тогда

$$(A+B)_iC^j=(a_{i1}+b_{i1}\ a_{i2}+b_{i2}\dots$$
$$\dots a_{in}+b_{in})[c_{1j}\ c_{2j}\dots c_{nj}]=$$
$$=\sum_{t=1}^{n}(a_{it}+b_{it})c_{tj}=\sum_{t=1}^{n}a_{it}c_{tj}+$$
$$+\sum_{t=1}^{n}b_{it}c_{tj}=A_iC^j+B_iC^j,$$

то есть $(A+B)C=AC+BC$. Второе равенство проверяется аналогично.

Т е о р е м а 6.4. $f(AB)=(fA)B=A(fB)$ для любого действительного числа и любых квадратных матриц порядка n.

Д о к а з а т е л ь с т в о. Так как по формуле (2)

$$f(A_iB^j)=f\sum_{t=1}^{n}a_{it}b_{tj}=\sum_{t=1}^{n}(fa_{it})b_{tj}=(fA)_iB^j=$$
$$=\sum_{t=1}^{n}a_{it}(fb_{tj})=A_i(fB)^j,$$

то требуемое равенство доказано. Конечно, здесь мы использовали ассоциативность, коммутативность и дистрибутивность сложения и умножения действительных чисел.

П р и м е р 3. Вычислить значение многочлена $f(x)=x^2-2x+3$ от матрицы $A=\begin{pmatrix}2&0\\1&-1\end{pmatrix}$.

Р е ш е н и е. Так как $f(A)=A^2-2A+3E$, то

$$f\left(\begin{pmatrix}2&0\\1&-1\end{pmatrix}\right)=\begin{pmatrix}2&0\\1&-1\end{pmatrix}\begin{pmatrix}2&0\\1&-1\end{pmatrix}-2\begin{pmatrix}2&0\\1&-1\end{pmatrix}+3\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}3&0\\-1&6\end{pmatrix}.$$

Пусть $A=(a_{ij})$ – $k\times l$ –матрица, а $B=(b_{ij})$ – $l\times k$ –матрица, у которой i –й столбец совпадает с i –й строкой матрицы A, то есть $B^i=A_i$ при любом $i=1,2,\dots,k$. В этом случае матрица B называется т р а н с п о н и р о в а н н о й к матрице A и обозначается через ${}^tA$.

Т е о р е м а 6.5. Пусть $A=(a_{ij})$, $B=(b_{ij})$ – $k\times l$ –матрицы, $C=(c_{ij})$ – $l\times m$ –матрица, а f – действительное число. Тогда

1) ${}^t({}^tA)=A$;

2) $f({}^tA)={}^t(fA)$;

3) ${}^t(A+B)={}^tA+{}^tB$;

4) ${}^t(AC)={}^tC\,{}^tA$.

Д о к а з а т е л ь с т в о. Первые три утверждения очевидны. Проверим четвертое. Так как $({}^tC)_i=C^i$, а $({}^tA)^j=A_j$, то

(6) $$({}^tC)_i({}^tA)^j=C^iA_j=[c_{1i}\ c_{2i}\dots c_{li}](a_{j1}\ a_{j2}\dots$$
$$\dots a_{jl})=\sum_{t=1}^{l}c_{ti}a_{jt}=\sum_{t=1}^{l}a_{jt}c_{ti}=A_jC^i$$

Но число A_jC^i стоит на пересечении j –й строки и i –го столбца матрицы AC, поэтому в матрице ${}^t(AC)$ это число A_jC^i

РЕПОЗИТОРИЙ ГГУ

стоит на пересечении i -й строки и j -го столбца. Теперь формула (6) доказывает требуемое равенство.

§ 7. ОПРЕДЕЛИТЕЛИ

Будем рассматривать только квадратные матрицы. Пусть $A = (a_{ij})$ - квадратная матрица порядка n . **Определителем** или **детерминантом** матрицы A называется число $\det A$, вычисляемое по следующей формуле

$$(I) \quad \det A = \sum_{\tau \in S_n} \operatorname{sgn} \tau \, a_{1\tau(1)} a_{2\tau(2)} \cdots a_{n\tau(n)}.$$

Здесь суммирование ведется по всем элементам из S_n, поэтому в правой части формулы (I) $n!$ слагаемых. Каждое слагаемое

$$a_{1\tau(1)} a_{2\tau(2)} \cdots a_{n\tau(n)}$$

состоит из n сомножителей, взятых по одному из каждой строки и каждого столбца. Так как $\operatorname{sgn}\tau = -1$ или $+1$, то каждое слагаемое умножается на -1 или $+1$ в зависимости от того, нечетная перестановка τ или четная.

Пример I. Очевидно, 1×1 -матрица (a) имеет определитель, равный a.

Пример 2. Для $n=2$ матрица

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

Поэтому

$$\det A = \sum_{\tau \in S_2} \operatorname{sgn} \tau \, a_{1\tau(1)} a_{2\tau(2)} = a_{11}a_{22} - a_{12}a_{21}.$$

Пример 3. Пусть $n=3$. Тогда

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\},$$

а матрица

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Поэтому

$$\det A = \sum_{\tau \in S_3} \operatorname{sgn} \tau \, a_{1\tau(1)} a_{2\tau(2)} a_{3\tau(3)} =$$

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

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

Эту формулу легче запомнить с помощью следующего рисунка

Пример 4. Вычислим определитель треугольной матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & a_{22} & \cdots & a_{2,n-1} & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

В (I) нас интересуют только ненулевые слагаемые. Очевидно, $a_{n\tau(n)}$ может быть отлично от нуля только при $\tau(n)=n$. Элемент $a_{n-1,\tau(n-1)} \neq 0$ только при $\tau(n-1)=n-1$ и т.д. Итак в сумме (I) только одно слагаемое $a_{11}a_{22}\cdots a_{nn}$ может быть отлично от нуля. Это слагаемое соответствует единичной перестановке, знак которой $+1$. Таким образом, определитель треугольной матрицы равен произведению диагональных элементов. В частности, определитель единичной матрицы равен 1.

Рассмотрим теперь свойства определителей. Поскольку в любом слагаемом из (I) есть представитель каждой строки и каждого столбца, то выполняется

Свойство I. Определитель матрицы с нулевой строкой или с нулевым столбцом равен нулю.

Свойство 2. При транспонировании матрицы определитель не меняется, то есть $\det A = \det({}^tA)$

Доказательство. Перестановка

$$\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

является обратной к τ и $\operatorname{sgn}\tau = \operatorname{sgn}\tau^{-1}$. Пусть $A = (a_{ij})$,

РЕПОЗИТОРИЙ ГГУ

$^tA=(t_{ij})$ и $b_{ij}=a_{ji}$. Применяя лемму 5.3, имеем

$$\det {}^tA=\sum_{\tau\in S_n}\operatorname{sgn}\tau\, b_{1\tau(1)}\dots b_{n\tau(n)}=$$

$$=\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{\tau(1)1}\dots a_{\tau(n)n}=$$

$$=\sum_{\tau^{-1}\in S_n}\operatorname{sgn}\tau^{-1}a_{\tau^{-1}(1)1}\dots a_{\tau^{-1}(n)n}=\det A.$$

Свойство 2 позволяет все утверждения об определителе матрицы, связанные со строками, переносить на определители матриц, высказанные для столбцов.

Свойство 3. Если матрица B получается из матрицы A после умножения каждого элемента некоторой строки на число f, то $\det B=f\det A$.

Доказательство. Пусть $A=(a_{ij})$, а матрица B получается из матрицы A после умножения i-й строки на число f, то есть $B_i=fA_i$, но $B_j=A_j$ для всех $j\neq i$. Тогда

$$\det B=\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{1\tau(1)}\dots fa_{i\tau(i)}\dots a_{n\tau(n)}=$$

$$=f\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{1\tau(1)}\dots a_{i\tau(i)}\dots a_{n\tau(n)}=f\det A$$

Отметим, что свойство 3 позволяет при вычислении определителя общий множитель всех элементов некоторой строки (столбца) выносить за знак определителя.

Пример 5. Пусть f – число, а $A=(a_{ij})$ – квадратная матрица порядка n. Произведение числа f к матрице A является матрица

$$fA=\begin{pmatrix} fa_{11} & \dots & fa_{1n}\\ \dots & \dots & \dots\\ fa_{n1} & \dots & fa_{nn}\end{pmatrix}.$$

Вынося число f из каждой строки, получаем, что $\det(fA)=f^n\det A$

Свойство 4. Если каждый элемент k-й строки матрицы A есть сумма двух слагаемых $a_{ki}+a'_{ki}$, то определитель матрицы A равен сумме определителей двух матриц, у которых все строки, кроме k-й, прежние, а k-я строка первой матрицы состоит из первых слагаемых a_{ki}, а второй – из вторых слагаемых a'_{ki}, то есть

$$\det\begin{pmatrix} a_{11} & \dots & a_{1n}\\ \dots & \dots & \dots\\ a_{k1}+a'_{k1} & \dots & a_{kn}+a'_{kn}\\ \dots & \dots & \dots\\ a_{n1} & \dots & a_{nn}\end{pmatrix}=\det\begin{pmatrix} a_{11}\dots a_{1n}\\ \dots\dots\\ a_{k1}\dots a_{kn}\\ \dots\dots\\ a_{n1}\dots a_{nn}\end{pmatrix}+\det\begin{pmatrix} a_{11}\dots a_{1n}\\ \dots\dots\\ a'_{k1}\dots a'_{kn}\\ \dots\dots\\ a_{n1}\dots a_{nn}\end{pmatrix}$$

Доказательство. Применяя формулу (1), получаем

$$\det\begin{pmatrix} a_{11} & \dots & a_{1n}\\ \dots & \dots & \dots\\ a_{k1}+a'_{k1} & \dots & a_{kn}+a'_{kn}\\ \dots & \dots & \dots\\ a_{n1} & \dots & a_{nn}\end{pmatrix}=\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{1\tau(1)}\dots(a_{k\tau(k)}+a'_{k\tau(k)})\dots$$

$$\dots a_{n\tau(n)}=\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{1\tau(1)}\dots a_{k\tau(k)}\dots a_{n\tau(n)}+$$

$$+\sum_{\tau\in S_n}\operatorname{sgn}\tau\, a_{1\tau(1)}\dots a'_{k\tau(k)}\dots a_{n\tau(n)}=$$

$$=\det\begin{pmatrix} a_{11}\dots a_{1n}\\ \dots\dots\\ a_{k1}\dots a_{kn}\\ \dots\dots\\ a_{n1}\dots a_{nn}\end{pmatrix}+\det\begin{pmatrix} a_{11}\dots a_{1n}\\ \dots\dots\\ a'_{k1}\dots a'_{kn}\\ \dots\dots\\ a_{n1}\dots a_{nn}\end{pmatrix}$$

Свойство 5. Если матрица B получается из матрицы A после перестановки двух строк, то $\det B=-\det A$.

Доказательство проведем для столбцов. В силу свойства 2 утверждение будет верно и для строк.

Пусть матрица $B=(b_{ij})$ получается из матрицы A в результате перестановки k-го и l-столбцов, то есть

РЕПОЗИТОРИЙ ГГУ

$B^k = A^k$, $B^l = A^k$, а $B^i = A^i$ для всех $i \neq k$ и l. Транспозиция $\sigma = (kl)$ есть нечетная перестановка и $\operatorname{sgn}\sigma\tau = \operatorname{sgn}\sigma \operatorname{sgn}\tau = -\operatorname{sgn}\tau$. По условию $b_{ij} = a_{i\sigma(j)}$ для всех i и j. Поэтому, используя лемму 5.3, получаем, что

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

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

Свойство 6. Определитель матрицы с пропорциональными строками равен нулю. В частности, нулю равен определитель матрицы, содержащей две одинаковые строки.

Доказательство. Если в матрице A две строки одинаковы, то переставив их вновь получим матрицу A. Но по свойству 5 $\det A = -\det A$, откуда $\det A = 0$.

Пусть в матрице B две строки пропорциональны. По свойству 3 коэффициент пропорциональности можно вынести за знак определителя. После этого получим матрицу с двумя равными строками. Ее определитель равен 0. Поэтому $\det B = 0$.

Свойство 7. Если все элементы некоторой строки умножить на число и сложить с элементами другой строки, то получим матрицу, определитель которой равен определителю исходной матрицы.

Доказательство. Умножим каждый элемент i-й строки матрицы $A = (a_{ij})$ на действительное число f и сложим с элементами k-й строки. В полученной матрице B k-я строка имеет вид: $B_k = (fa_{i1} + a_{k1} \dots fa_{in} + a_{kn})$, а остальные строки как и у матрицы A. Через C обозначим матрицу, у которой в k-й строке стоят первые слагаемые, то есть $C_k = (fa_{i1} \dots fa_{in})$, а остальные строки как у матрицы A. В матрице C i-я строка пропорциональна k-й, значит $\det C = 0$ по свойству 6. По свойству 7 теперь

$$\det B = \det C + \det A = \det A$$

Пример 6. Доказать, что на 11 делится определитель матрицы

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 0 & 8 & 9 \\ 0 & 6 & 0 & 5 \end{pmatrix}$$

Решение. Так как числа 11, 121, 1089 и 605 делятся на 11, то умножая первый столбец на 1000, второй на 100, третий на 10 и прибавляя все это к четвертому столбцу, мы получим матрицу

$$B = \begin{pmatrix} 0 & 0 & 1 & 11 \\ 0 & 1 & 2 & 121 \\ 1 & 0 & 8 & 1089 \\ 0 & 6 & 0 & 605 \end{pmatrix}$$

По свойству 7 $\det B = \det A$, а по свойству 3 определитель матрицы B делится на 11, так как на 11 делятся все элементы последнего столбца.

§ 8. ОПРЕДЕЛИТЕЛЬ ПРОИЗВЕДЕНИЯ МАТРИЦ

Пусть

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mm} \end{pmatrix}$$

квадратные матрицы порядков n и m соответственно. Условимся через X обозначать следующую матрицу

$$X = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & a_{1n+1} & \dots & a_{1n+m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} & a_{nn+1} & \dots & a_{nn+m} \\ 0 & \dots & 0 & b_{11} & \dots & b_{1m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_{m1} & \dots & b_{mm} \end{pmatrix}$$

где

РЕПОЗИТОРИЙ ГГУ

$$C = \begin{pmatrix} a_{1,n+1} & \dots & a_{1,n+m} \\ \dots & \dots & \dots \\ a_{n,n+1} & \dots & a_{n,n+m} \end{pmatrix}$$

$n \times m$ -матрица. Ясно, что X является $(n+m)\times(n+m)$ -матрицей. Аналогично строятся матрицы

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

Теорема 8.1. $\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \det B$

Доказательство. Пусть $X = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = (x_{ij})$.

Тогда

$$\det X = \sum_{\tau \in S_{n+m}} \operatorname{sgn} \tau \; x_{1\tau(1)} \dots x_{n+m\,\tau(n+m)}$$

Нас интересуют ненулевые слагаемые этой суммы. Обозначим через

$$S = \{\tau \in S_{n+m} \mid \tau(i) > n \text{ при } i > n\}$$

Если $\delta \in S_{n+m} \setminus S$, то существует число $k > n$ такое, что $\delta(k) = l \le n$, а элемент $x_{k\delta(k)} = 0$. Таким образом, в сумме равны нулю все слагаемые которые соответствуют перестановкам из $S_{n+m} \setminus S$, и суммирование следует вести только по перестановкам из S.

Перестановка $\tau \in S$ отображает множество $\{n+1, n+2, \dots, n+m\}$ на себя, поэтому

$$x_{n+i,\tau(n+i)} = t_{i,\tau(n+i)-n}$$

Из биективности следует, что перестановка $\tau \in S$ отображает множество $\{1, 2, \dots, n\}$ на себя, поэтому

$$x_{i\tau(i)} = a_{i\tau(i)}$$

при $i \le n$.

Итак, каждую перестановку $\tau \in S$ можно представить в виде произведения $\tau = \tau_1 \tau_2$, где

$$\tau_1 = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & n+m \\ \tau(1) & \tau(2) & \dots & \tau(n) & n+1 & \dots & n+m \end{pmatrix},$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & n+m \\ 1 & 2 & \dots & n & \tau(n+1) & \dots & \tau(n+m) \end{pmatrix}.$$

Пусть $S^{(1)} = \{\tau \in S \mid \tau(n+i) = n+i,\ i = 1, 2, \dots, m\}$ и $S^{(2)} = \{\tau \in S \mid \tau(i) = i,\ i = 1, 2, \dots, n\}$. Зададим отображения $\varphi_1 : S^{(1)} \to S_n$ и $\varphi_2 : S^{(2)} \to S_m$ считая

$$\varphi_1(\tau_1) = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau_1(1) & \tau_1(2) & \dots & \tau_1(n) \end{pmatrix},$$

$$\varphi_2(\tau_2) = \begin{pmatrix} 1 & 2 & \dots & m \\ \tau_2(n+1)-n & \tau_2(n+2)-n & \dots & \tau_2(n+m)-n \end{pmatrix}$$

для всех $\tau_1 \in S^{(1)}$ и $\tau_2 \in S^{(2)}$.

Перестановка $\varphi_1(\tau_1)$ получается из τ_1 отбрасыванием последних m столбцов. Поэтому φ_1 – биекция, и $\varphi_1(\tau_1)$ пробегает S_n, если τ_1 пробегает $S^{(1)}$. Пусть c_1 – число независимых циклов в разложении $\varphi_1(\tau_1)$. Тогда $c_1 + m$ – число независимых циклов в разложении τ_1 и

$$\operatorname{sgn} \varphi_1(\tau_1) = (-1)^{n-c_1} = (-1)^{n+m-(c_1+m)} = \operatorname{sgn} \tau_1,$$

см. следствие теоремы 5.2.

Рассмотрим отображение φ_2. Очевидно, φ_2 – инъекция. Каждая перестановка $\overline{\pi} \in S_n$ будет образом при отображении φ_2 перестановки

$$\begin{pmatrix} 1 & \dots & n & n+1 & \dots & n+m \\ 1 & \dots & n & \overline{\pi}(1)+n & \dots & \overline{\pi}(m)+n \end{pmatrix},$$

поэтому φ_2 – биекция. Каждый цикл перестановки $\varphi_2(\tau_2)$ после поэлементного сложения с n превращается в цикл τ_2, поэтому число независимых циклов в разложении τ_2 равно $n + c_2$, где c_2 – число циклов перестановки $\varphi_2(\tau_2)$. Следовательно,

РЕПОЗИТОРИЙ ГГУ ИМ.

$$\operatorname{sgn}\varphi_2(\tau_2) = (-1)^{m-c_2} = (-1)^{c+m-(n+c_2)} = \operatorname{sgn}\tau_2$$

Теперь,

$$\det X = \sum_{\tau\in S} \operatorname{sgn}\tau\, a_{1\tau(1)}\cdots a_{n\tau(n)}\, b_{1(\tau(n+1)-n)}\cdots$$

$$\cdots b_{m(\tau(n+m)-n)} = \sum_{\substack{\tau_1\in S^{(c)}\\ \tau_2\in S^{(a)}}} \operatorname{sgn}\tau_1 \operatorname{sgn}\tau_2\, a_{1\tau_1(1)}\cdots$$

$$\cdots a_{n\tau_1(n)}\, b_{1(\tau_2(n+1)-n)}\cdots b_{m(\tau_2(n+m)-n)} =$$

$$= \sum_{\varphi_1(\tau_1)\in S_n} \operatorname{sgn}\varphi_1(\tau_1)\, a_{1\varphi_1(\tau_1)(1)}\cdots a_{n\varphi_1(\tau_1)(n)} \times$$

$$\times \sum_{\varphi_2(\tau_2)\in S_m} \operatorname{sgn}\varphi_2(\tau_2)\, b_{1\varphi_2(\tau_2)(1)}\cdots b_{m\varphi_2(\tau_2)(m)} =$$

$$= \det A \cdot \det B.$$

Следствие 1. $\det\begin{pmatrix} A & O \\ C & B \end{pmatrix} = \det A \det B$

Доказательство. Воспользуемся тем свойством, что при транспонировании определитель не изменяется

$$\det\begin{pmatrix} A & O \\ C & B \end{pmatrix} = \det {}^t\begin{pmatrix} A & O \\ C & B \end{pmatrix} = \det\begin{pmatrix} {}^tA & {}^tC \\ O & {}^tB \end{pmatrix} =$$

$$= \det {}^tA \det {}^tB = \det A \det B$$

Следствие 2.

$$\det\begin{pmatrix} O & A \\ B & C \end{pmatrix} = \det\begin{pmatrix} C & A \\ B & O \end{pmatrix} = (-1)^{nm} \det A \det B$$

Доказательство. Будем смещать у матрицы

$$\begin{pmatrix} O & A \\ B & C \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & a_{11} & \cdots & a_{1n} \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & 0 & a_{n1} & \cdots & a_{nn} \\ b_{11} & \cdots & b_{1m} & c_{11} & \cdots & c_{1n} \\ \cdots & & \cdots & \cdots & & \cdots \\ b_{m1} & \cdots & b_{mm} & c_{m1} & \cdots & c_{mn} \end{pmatrix}$$

последние n столбцов влево, переставляя каждый последовательно с соседним слева. $(m+1)$-й столбец будет первым после m перестановок; $(m+2)$-й столбец будет вторым после m перестановок; ...; $(m+n)$-й столбец будет n-ым после m перестановок. В результате nm перестановок мы получим матрицу $\begin{pmatrix} A & O \\ C & B \end{pmatrix}$, определитель которой равен $\det A \cdot \det B$ по следствию 1. Но каждая перестановка столбцов меняет знак по свойству 5 определителей. Поэтому

$$\det\begin{pmatrix} O & A \\ B & C \end{pmatrix} = (-1)^{nm} \det A \cdot \det B.$$

Аналогично поступая с матрицей $\begin{pmatrix} C & A \\ B & O \end{pmatrix}$, получим, что

$$\det\begin{pmatrix} C & A \\ B & O \end{pmatrix} = (-1)^{nm} \det\begin{pmatrix} A & C \\ O & B \end{pmatrix} = (-1)^{nm} \det A \det B$$

Пример 1. Вычислим определитель матрицы

$$A = \begin{pmatrix} a & 0 & a & 0 \\ b & 0 & -b & 0 \\ c & c & c & c \\ d & d & -d & -d \end{pmatrix}.$$

Переставив 2-й и 3-й столбцы, мы получим матрицу

$$B = \begin{pmatrix} a & a & 0 & 0 \\ b & -b & 0 & 0 \\ c & c & c & c \\ d & -d & d & -d \end{pmatrix}$$

Так как $\det A = -\det B$, а $\det B = \det\begin{pmatrix} a & a \\ b & -b \end{pmatrix} \det\begin{pmatrix} c & c \\ d & -d \end{pmatrix}$ по теореме 8.1, то $\det A = -4abcd$.

Теорема 8.2. Определитель произведения матриц равен произведению определителей, то есть если A и B – квадрат-

РЕПОЗИТОРИЙ ГГУ ИМ.

ные матрицы порядка n, то $\det AB = \det A \det B$.

Доказательство. Пусть $A=(a_{ij}), B=(b_{ij})$ – квадратные матрицы порядка n. Рассмотрим матрицу

$$X = \begin{pmatrix} A & O \\ -E & B \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 0 \\ -1 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & -1 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

По теореме 8.I ее определитель $\det X = \det A \det B$.

Преобразуем матрицу X в матрицу

$$Y = \begin{pmatrix} 0 & C \\ -E & B \end{pmatrix}$$

Для этого к первой строке матрицы X прибавим

$(n+1)$-ю строку, умноженную на a_{11};

$(n+2)$-ю строку, умноженную на a_{12},

и т.д.; и наконец

$2n$-ю строку, умноженную на a_{1n}.

В полученной матрице n элементов первой строки будут нулями, а n других элементов первой строки будут такими:

$$\sum_{j=1}^{n} a_{1j} b_{j1} = A_1 B^1; \quad \sum_{j=1}^{n} a_{1j} b_{j2} = A_1 B^2, \dots; \quad \sum_{j=1}^{n} a_{1j} b_{jn} = A_1 B^n.$$

Аналогично, для каждого $i = 2, 3, \dots, n$ к i-й строке прибавим

$(n+1)$-ю, умноженную на a_{i1};

$(n+2)$-ю, умноженную на a_{i2};

и т.д.; и наконец

$2n$-ю, умноженную на a_{in}.

Тогда первые n элементов i-й строки будут нулями, а n других элементов примут вид

$$\sum_{j=1}^{n} a_{ij} b_{j1} = A_i B^1; \quad \sum_{j=1}^{n} a_{ij} b_{j2} = A_i B^2, \dots; \quad \sum_{j=1}^{n} a_{ij} b_{jn} = A_i B^n.$$

В итоге получим матрицу $Y = \begin{pmatrix} 0 & C \\ -E & B \end{pmatrix}$,

у которой

$$C = \begin{pmatrix} A_1 B^1 & A_1 B^2 & \dots & A_1 B^n \\ \dots & \dots & \dots & \dots \\ A_n B^1 & A_n B^2 & \dots & A_n B^n \end{pmatrix} = AB.$$

По свойству 7 определителей $\det X = \det Y$, а по следствию теоремы 8.I

$$\det Y = (-1)^{n^2} \det C \det(-E) = (-1)^{n^2} \det(AB)(-1)^n =$$

$$= (-1)^{n(n+1)} \det(AB) = \det(AB).$$

Таким образом, $\det A \det B = \det(AB)$.

§ 9. МИНОРЫ И АЛГЕБРАИЧЕСКИЕ ДОПОЛНЕНИЯ

Пусть $A=(a_{ij})$ – квадратная матрица порядка n. Минором элемента a_{kl} называется определитель матрицы, полученной из матрицы A после вычеркивания k-й строки и l-го столбца. Минор элемента a_{kl} обозначим через M_{kl}. Произведение $(-1)^{k+l} M_{kl}$ называется алгебраическим дополнением элемента a_{kl} и обозначается через A_{kl}. Отметим, что числа M_{kl} и A_{kl} не зависят от значения элемента a_{kl}, а зависят от его местоположения в матрице.

Лемма 9.I. Если равны нулю все элементы некоторой строки (столбца) квадратной матрицы, кроме одного, то определитель равен произведению этого элемента на его алгебраическое дополнение.

Доказательство. Пусть в l-ом столбце квадратной матрицы $A=(a_{ij})$ порядка n равны нулю все элементы, кроме a_{kl}. Будем смещать l-й столбец влево, переставляя его последовательно с соседними слева столбцами. В результате $l-1$ перестановок l-й столбец будет первым. Затем k-ю строку будем смещать вверх, переставляя ее последовательно с соседней сверху строкой. После $k-1$ перестановок k-я строка будет первой и мы получим матрицу

РЕПОЗИТОРИЙ ГГУ

$$B = \begin{pmatrix} a_{k1} & a_{k1} & \dots & a_{k,i-1} & a_{k,i+1} & \dots & a_{kn} \\ 0 & a_{11} & \dots & a_{1,i-1} & a_{1,i+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{k-1,1} & \dots & a_{k-1,i-1} & a_{k-1,i+1} & \dots & a_{k-1,n} \\ 0 & a_{k+1,1} & \dots & a_{k+1,i-1} & a_{k+1,i+1} & \dots & a_{k+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{n1} & \dots & a_{n,i-1} & a_{n,i+1} & \dots & a_{nn} \end{pmatrix}.$$

По теореме 8.2 $\det B = a_{k1} M_{k1}$, где M_{k1} – минор элемента a_{k1} в матрице A. Но матрица B получается из матрицы A в результате $k+1-2$ перестановок строк и столбцов, поэтому $\det A = (-1)^{k+1} \det B$ по свойству 5 определителей. Следовательно, $\det A = a_{k1} A_{k1}$.

Теорема 9.2. Определитель квадратной матрицы $A = (a_{ij})$ порядка n равен сумме произведений элементов какой-либо строки (столбца) на их алгебраические дополнения, то есть

$$\det A = a_{k1} A_{k1} + a_{k2} A_{k2} + \dots + a_{kn} A_{kn} =$$

$$= a_{1i} A_{1i} + a_{2i} A_{2i} + \dots + a_{ni} A_{ni}$$

Доказательство. Представим k-ю строку матрицы A в виде суммы n слагаемых:

$$A_k = (a_{k1}\, 0 \dots 0) + (0\, a_{k2} \dots 0) + \dots + (0\, 0 \dots a_{kn})$$

Применяя свойство 4 определителей и теорему 9.1, получаем:

$$\det A = \det \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{k1} & 0 \dots 0 \\ a_{n1} & a_{n2} \dots a_{nn} \end{pmatrix} + \det \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ 0 & a_{k2} \dots 0 \\ a_{n1} & a_{n2} \dots a_{nn} \end{pmatrix} +$$

$$+ \dots + \det \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ 0 & 0 \dots a_{kn} \\ a_{n1} & a_{n2} \dots a_{nn} \end{pmatrix} =$$

$$= a_{k1} A_{k1} + a_{k2} A_{k2} + \dots + a_{kn} A_{kn}$$

Аналогично проверяется и вторая формула.

Пример 1. Вычислить определитель матрицы

$$A = \begin{pmatrix} 1 & 2 & -1 & -2 \\ a & b & c & d \\ 2 & -1 & -2 & 1 \\ -2 & -1 & 1 & 2 \end{pmatrix}.$$

Решение. Применим теорему 9.2 к элементам второй строки

$$\det A = a \det \begin{pmatrix} 2 & -1 & -2 \\ -1 & -2 & 1 \\ -1 & 1 & 2 \end{pmatrix} - b \det \begin{pmatrix} 1 & -1 & -2 \\ 2 & -2 & 1 \\ -2 & 1 & 2 \end{pmatrix} +$$

$$+ c \det \begin{pmatrix} 1 & 2 & -2 \\ 2 & -1 & 1 \\ -2 & -1 & 2 \end{pmatrix} - d \det \begin{pmatrix} 1 & 2 & -1 \\ 2 & -1 & -2 \\ -2 & -1 & 1 \end{pmatrix} =$$

$$= -5(a + b + c + d).$$

Теорема 9.3. Сумма произведений элементов какой-либо строки (столбца) квадратной матрицы $A = (a_{ij})$ на алгебраические дополнения соответствующих элементов другой строки (столбца) равна нулю, то есть

$$a_{k1} A_{i1} + a_{k2} A_{i2} + \dots + a_{kn} A_{in} = 0 \quad \text{при } k \neq i;$$

$$a_{1i} A_{1j} + a_{2i} A_{2j} + \dots + a_{ni} A_{nj} = 0 \quad \text{при } i \neq j$$

Доказательство. Запишем матрицу A, перечислив все ее строки: $A = [A_1, A_2 \dots A_k \dots A_i \dots A_n]$. Для определенности мы считаем, что $i > k$. Заменим i-ю строку A_i произвольным набором n чисел $B_i = (b_1, b_2 \dots b_{n-1}, b_n)$. Получаем матрицу $B = [A_1, A_2 \dots A_k \dots B_i \dots A_n]$. Ясно, что для алгебраических дополнений элементов i-ых строк матриц A и B имеем равенство: $A_{ij} = B_{ij}$ для каждого $j = 1, 2, \dots, n$. Теперь по теореме 9.2 имеем

$$\det B = b_1 A_{i1} + b_2 A_{i2} + \dots + b_n A_{in}.$$

Это равенство верно при любом наборе B_i, в частности, при $b_1 = a_{k1}, b_2 = a_{k2}, \dots, b_n = a_{kn}$, то есть $B_i = A_k$. Но в этом случае в матрице B будут две равные строки: A_k

РЕПОЗИТОРИЙ ГГУ

и B_i, поэтому $\det B = 0$ и

$$a_{k1}A_{i1} + a_{k2}A_{i2} + \ldots + a_{kn}A_{in} = 0.$$

§ 10. ОБРАТНАЯ МАТРИЦА

Квадратная матрица A порядка n называется **обратимой**, если существует матрица B такая, что $AB = BA = E$, где E – единичная матрица порядка n. В этом случае матрица B называется **обратной** к матрице A.

Лемма 10.1. Если матрица обратима, то существует только одна ей обратная матрица.

Доказательство. По условию матрица A обратима, значит обратные матрицы существуют. Пусть B и C – обратные к A матрицы, то есть $AB = BA = AC = CA = E$. Тогда

$$B = BE = B(AC) = (BA)C = EC = C.$$

Лемма доказана.

Если A – обратимая матрица, то обратная матрица обозначается через A^{-1}. Матрица, определитель которой отличен от нуля, называется **невырожденной**.

Лемма 10.2. Обратимая матрица невырождена.

Доказательство. Если A – обратимая матрица, и A^{-1} ей обратная, то $AA^{-1} = E$. Поэтому $\det A \det A^{-1} = 1$ и $\det A \neq 0$. Кроме того,

$$\det A^{-1} = 1/\det A.$$

Лемма 10.3. Если A и B – обратимые матрицы порядка n, то AB обратима, и $(AB)^{-1} = B^{-1}A^{-1}$.

Доказательство. Поскольку

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = E,$$
$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = E,$$

то $B^{-1}A^{-1}$ – обратная к матрице AB, то есть $(AB)^{-1} = B^{-1}A^{-1}$. Лемма доказана.

Для квадратной матрицы $A = (a_{ij})$ порядка n построим матрицу

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

которую назовем **присоединенной (или взаимной)** матрицей к матрице A. Чтобы получить присоединенную матрицу $A^{\vee}$ надо поставить вместо каждого элемента a_{ij} его алгебраическое дополнение A_{ij}, а затем перейти к транспонированной матрице.

Теорема 10.4. Квадратная матрица обратима тогда и только тогда, когда она невырождена. Если A невырождена, то $A^{-1} = \frac{1}{\det A} A^{\vee}$.

Доказательство. По лемме 10.2 обратимая матрица невырождена.

Обратно, пусть A невырождена и $d = \det A$. Присоединенная матрица $A^{\vee}$ существует всегда. Перемножим матрицы A и $A^{\vee}$:

$$A_i(A^{\vee})^j = (a_{i1}\ a_{i2}\ \ldots\ a_{in})[A_{j1}, A_{j2} \ldots A_{jn}] =$$
$$= a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn}.$$

Если $i = j$, то $A_i(A^{\vee})^j = d$ по теореме 9.2.
Если $i \neq j$, то $A_i(A^{\vee})^j = 0$ по теореме 9.3. Поэтому

$$A(d^{-1}A^{\vee}) = d^{-1}(AA^{\vee}) = d^{-1}\begin{pmatrix} d & 0 & \ldots & 0 \\ 0 & d & & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d \end{pmatrix} = E.$$

Аналогично проверяется, что $(d^{-1}A^{\vee})A = E$. Таким образом, если A невырождена, то A^{-1} существует и $A^{-1} = d^{-1}A^{\vee}$.

Пример 1. Найти обратную к матрице 2-го порядка.

Решение. Пусть $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ – матрица 2-го порядка. Найдем все алгебраические дополнения:

РЕПОЗИТОРИЙ ГГУ

$A_{11} = a_{22}$, $A_{12} = -a_{21}$, $A_{21} = -a_{12}$, $A_{22} = a_{11}$.

Поэтому присоединенная матрица A^* имеет вид

$$A^* = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Если $\det A = a_{11}a_{22} - a_{12}a_{21} \neq 0$, то

$$A^{-1} = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Пример 2. Найти обратную к матрице

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 4 & 1 \\ -1 & 5 & 2 \end{pmatrix}.$$

Решение. Вычислим определитель матрицы A, а затем найдем присоединную матрицу

$$\det A = 8 + 5 + 4 - 2 - 5 - 4 = 6.$$

$A_{11} = \det\begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} = 3$; $A_{12} = -\det\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} = -3$;

$A_{13} = \det\begin{pmatrix} 1 & 4 \\ -1 & 5 \end{pmatrix} = 9$; $A_{21} = -\det\begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix} = 1$;

$A_{22} = \det\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} = 3$; $A_{23} = -\det\begin{pmatrix} 1 & 2 \\ -1 & 5 \end{pmatrix} = -7$;

$A_{31} = \det\begin{pmatrix} 2 & 1 \\ 4 & 1 \end{pmatrix} = -2$; $A_{32} = -\det\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 0$;

$A_{33} = \det\begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix} = 2$.

Поэтому

$$A^* = \begin{pmatrix} 3 & 1 & -2 \\ -3 & 3 & 0 \\ 9 & -7 & 2 \end{pmatrix}$$

и

$$A^{-1} = \frac{1}{6}\begin{pmatrix} 3 & 1 & -2 \\ -3 & 3 & 0 \\ 9 & -7 & 2 \end{pmatrix}.$$

Сделаем проверку

$$A^{-1}A = \frac{1}{6}\begin{pmatrix} 3 & 1 & -2 \\ -3 & 3 & 0 \\ 9 & -7 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 1 \\ 1 & 4 & 1 \\ -1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E$$

Аналогично, $AA^{-1} = E$

Ответ.

$$A^{-1} = \frac{1}{6}\begin{pmatrix} 3 & 1 & -2 \\ -3 & 3 & 0 \\ 9 & -7 & 2 \end{pmatrix}$$

§ II. КРАМЕРОВСКИЕ СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Пусть k и ℓ – натуральные числа. Рассмотрим совокупность k линейных уравнений с ℓ неизвестными

$$(I) \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1\ell}x_\ell = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2\ell}x_\ell = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{k\ell}x_\ell = b_k. \end{cases}$$

Здесь a_{ij} – действительные числа, называемые коэффициентами системы (I), $x_1, x_2, \ldots, x_\ell$ – неизвестные, $b_1, b_2, \ldots, b_k$ – свободные члены.

Множество $\{f_1, f_2, \ldots, f_\ell\}$ действительных чисел называется решением системы (I), если после подстановки в любое из уравнений вместо x_i числа f_i, $i = 1, 2, \ldots, \ell$, каждое уравнение обращается в тождество. Система называется совместной, если она имеет хотя бы одно решение, и несовместной – в противном случае.

$k \times \ell$ -матрица $A = (a_{ij})$, составленная из коэффициентов системы (I), называется матрицей системы (I).

Матрицы

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_\ell \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_k \end{pmatrix}$$

РЕПОЗИТОРИЙ ГГУ

называются столбцом неизвестных и столбцом свободных членов.

Вычислив произведение AX, получим $k\times 1$-матрицу

$$AX=\begin{pmatrix} a_{11}x_1+a_{12}x_2+\ldots+a_{1\ell}x_\ell \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2\ell}x_\ell \\ \ldots\ldots\ldots\ldots\ldots \\ a_{k1}x_1+a_{k2}x_2+\ldots+a_{k\ell}x_\ell \end{pmatrix}$$

Система (I) требует, чтобы $k\times 1$-матрицы AX и B были равны, то есть в матричной записи система (I) принимает вид

(2) $$AX=B.$$

Матрицу $C=\begin{pmatrix} c_1 \\ c_2 \\ \ldots \\ c_\ell \end{pmatrix}$ назовем решением матричного уравнения (2), если $AC=B$, то есть матрица C есть решение уравнения (2) тогда и только тогда, когда $\{c_1,c_2,\ldots,c_\ell\}$ – решение системы (I).

Система (I) называется **крамеровской**, если число уравнений совпадает с числом неизвестных, и определитель матрицы системы не равен нуло, то есть $k=\ell$ и $\det A\neq 0$.

Теорема II.1. Крамеровская система имеет единственное решение

$$x_i=\frac{d_i}{d},\quad i=1,2,\ldots,k,$$

где $d=\det A$ – определитель системы, а d_i – определитель матрицы, у которой в i-ом столбце стоят свободные члены $b_1,b_2,\ldots,b_k$, а остальные столбцы как и у матрицы A.

Доказательство. Пусть система (I) крамеровская. Тогда $\det A=d\neq 0$ и существует обратная матрица A^{-1}. Умножим слева обе части уравнения (2) на A^{-1}, получим $X=A^{-1}B$. Таким образом, уравнение (2), а следовательно и система (I), имеет единственное решение

$$X=A^{-1}B=\begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_k \end{pmatrix}.$$

Так как

$$A^{-1}=d^{-1}\begin{pmatrix} A_{11} & A_{21} & \ldots & A_{k1} \\ A_{12} & A_{22} & \ldots & A_{k2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1k} & A_{2k} & \ldots & A_{kk} \end{pmatrix},$$

то $$x_i=(A^{-1})_i B=d^{-1}(A_{1i}A_{2i}\ldots A_{ki})[b_1b_2\ldots b_k]=$$
$$=d^{-1}(A_{1i}b_1+A_{2i}b_2+\ldots+A_{ki}b_k)=d^{-1}d_i.$$

Но d_i есть определитель матрицы

$$\begin{pmatrix} a_{11}\ldots a_{1i-1}\ b_1\ a_{1i+1}\ldots a_{1k} \\ a_{21}\ldots a_{2i-1}\ b_2\ a_{2i+1}\ldots a_{2k} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}\ldots a_{ki-1}\ b_k\ a_{ki+1}\ldots a_{km} \end{pmatrix}$$

которая получается из матрицы A заменой i-го столбца свободными членами. Теорема доказана.

Пример I. Решить систему

$$\begin{cases} x_1+2x_2+5x_3=7 \\ 2x_1-x_2+x_3=9 \\ x_1-4x_2+2x_3=11 \end{cases}$$

Решение. Вычислим определитель системы

$$d=\det\begin{pmatrix} 1 & 2 & 5 \\ 2 & -1 & 1 \\ 1 & -4 & 2 \end{pmatrix}=-25.$$

Вычислим определитель $d_i, i=1,2,3$, где d_i – определитель матрицы, которая получается из матрицы системы заменой i-го столбца свободными членами

$$d_1=\det\begin{pmatrix} 7 & 2 & 5 \\ 9 & -1 & 1 \\ 11 & -4 & 2 \end{pmatrix}=-75,$$

$$d_2=\det\begin{pmatrix} 1 & 7 & 5 \\ 2 & 9 & 1 \\ 1 & 11 & 2 \end{pmatrix}=25,$$

РЕПОЗИТОРИЙ ГГУ

$$d_3 = \det\begin{pmatrix} 1 & 2 & 7 \\ 2 & -1 & 9 \\ 1 & -4 & 11 \end{pmatrix} = -50.$$

По теореме I0.I имеем $x_1 = 3$, $x_2 = -1$, $x_3 = 2$.

Проверка. Подставляя в систему $x_1 = 3, x_2 = -1, x_3 = 2$ получим

$$3 + 2(-1) + 3 \cdot 2 = 7 \equiv 7$$
$$2 \cdot 3 - 1(-1) + 2 = 9 \equiv 9$$
$$3 - 4(-1) + 2 \cdot 2 = 11 \equiv 11$$

Поскольку каждое уравнение превратилось в тождество, то мы получили верное решение.

Ответ. $x_1 = 3; x_2 = -1; x_3 = 2$.

§ I2. ГРУППЫ

Бинарной операцией на множестве X называют отображение декартова квадрата $X \times X$ во множество X. Если $\varphi: X \times X \to X$ - бинарная операция на X, то каждой упорядоченной паре (a, b) элементов из X соответствует однозначно определенный элемент $c = \varphi(a, b) \in X$. Бинарную операцию на X обозначают одним из символов: $+, \cdot, \oplus, \otimes, \circ, *$ и т.д. Если вместо φ условимся писать $\circ$, то вместо $c = \varphi(a, b)$ пишут $c = a \circ b$.

Говорят, что на множестве X определена бинарная операция $\circ$, если $a \circ b \in X$ для всех $a, b \in X$. Множество X с определенной на X бинарной операцией $\circ$ называют алгебраической системой и обозначают через $(X, \circ)$.

Если $(a \circ b) \circ c = a \circ (b \circ c)$ для всех $a, b, c \in X$, то операция $\circ$ называется ассоциативной, а алгебраическую систему $(X, \circ)$ называют полугруппой.

Если $a \circ b = b \circ a$ для всех $a, b \in X$, то операция называется коммутативной.

Элемент $n \in X$ называется нейтральным, если $a \circ n = n \circ a = a$ для всех $a \in X$.

Симметричным элементу a называется элемент a'

такой, что $a \circ a' = a' \circ a = n$.

Теорема I2.I. В алгебраической системе может быть не более одного нейтрального элемента. Если в полугруппе имеется нейтральный элемент, то каждый элемент обладает не более, чем одним симметричным.

Доказательство. Пусть в алгебраической системе $(X, \circ)$ элементы n_1 и n_2 нейтральны. Тогда $n_1 \circ n_2 = n_1$, так как n_2 - нейтральный элемент, и $n_1 \circ n_2 = n_2$, так как n_1 нейтрален. Поэтому $n_1 = n_2$.

Пусть $(X, \circ)$ - полугруппа с нейтральным элементом n. Предположим, что a' и $\bar{a}'$ - симметричные к a элементы, то есть $a \circ a' = a' \circ a = n = \bar{a}' \circ a$. Тогда $a' = a' \circ n = a' \circ (a \circ \bar{a}') = (a' \circ a) \circ \bar{a}' = n \circ \bar{a}' = \bar{a}'$. Теорема доказана.

В математике, в основном, используются две формы записи алгебраической операции: аддитивная и мультипликативная. При аддитивной записи операцию называют сложением и вместо $\circ$ пишут $+$. При мультипликативной записи операцию называют умножением, а знак $\circ$ опускают. Связь между аддитивной и мультипликативной записями изобразим в виде следующей таблицы.

Таблица I

Мультипликативная запись	Аддитивная запись
умножение	сложение $+$
произведение ab	сумма $a + b$
единичный элемент e или 1	нулевой элемент 0
$ae = ea = a$	$a + 0 = 0 + a = a$
обратный элемент a^{-1}	противоположный элемент $-a$
$aa^{-1} = a^{-1}a = e$	$a + (-a) = (-a) + a = 0$
ассоциативность	
$(ab)c = a(bc)$	$(a + b) + c = a + (b + c)$
коммутативность	
$ab = ba$	$a + b = b + a$
$\prod_{i=1}^{n} a_i = a_1 a_2 \dots a_n$	$\sum_{i=1}^{n} a_i = a_1 + a_2 + \dots + a_n$
степень a^n	кратное na

РЕПОЗИТОРИЙ ГГУ

Продолжение таблицы I

Мультипликативная запись	Аддитивная запись
$\underbrace{a\,a\,\ldots\,a}_{n\text{ раз}}=a^n$	$\underbrace{a+a+\ldots+a}_{n\text{ раз}}=na$
$a^n a^m=a^{n+m}$	$na+ma=(n+m)a$
$(a^n)^m=a^{nm}$	$m(na)=(mn)a$
$(ab)^n=a^n b^n$, если $ab=ba$	$n(a+b)=na+nb$, если $a+b=b+a$

В дальнейшем будем использовать мультипликативную запись, а при необходимости с помощью таблицы переходить к аддитивной записи.

Теорема I2.2. Если алгебраическая операция (умножение) на множестве X ассоциативна, то результат ее последовательного применения к n элементам не зависит от расстановки скобок.

Доказательство. Пусть $a_1, a_2, \ldots, a_n$ - упорядоченная последовательность элементов из X. Не меняя порядка, мы можем многими разными способами составлять произведения длины n. Для $n=1,2,3,4$ можно составить следующие произведения

$n=1$ a_1

$n=2$ a_1a_2

$n=3$ $(a_1a_2)a_3$, $a_1(a_2a_3)$

$n=4$ $((a_1a_2)a_3)a_4$, $(a_1(a_2a_3))a_4$,
$a_1((a_2a_3)a_4)$, $a_1(a_2(a_3a_4))$, $(a_1a_2)(a_3a_4)$

и т.д.

Поскольку операция ассоциативна, то при $n=3$ имеем равенство $(a_1a_2)a_3=a_1(a_2a_3)$. Для $n=4$, используя ассоциативность, легко проверить, что все пять произведений совпадают.

Далее рассуждаем индукцией по n, считая, что для числа элементов $<n$ справедливость утверждения установлена. Нам нужно показать, что

(I) $(a_1\ldots a_k)(a_{k+1}\ldots a_n)=(a_1\ldots a_\ell)(a_{\ell+1}\ldots a_n)$

при любых k,ℓ, $1\le k,\ell\le n$. Мы выписали только внешние пары скобок, поскольку по предположению индукции расстановка внутренних скобок несущественна. В частности, $a_1a_2\ldots a_k=(\ldots((a_1a_2)a_3)a_4)\ldots)a_k$ - произведение, называемое **левонормированным**. Различаем два случая:

а) $k=n-1$. Тогда $(a_1\ldots a_{n-1})a_n=(\ldots(a_1a_2)\ldots a_{n-1})a_n$ - левонормированное произведение;

б) $k<n-1$. Ввиду ассоциативности имеем

$$(a_1\ldots a_k)(a_{k+1}\ldots a_n)=(a_1\ldots a_k)((a_{k+1}\ldots a_{n-1})a_n)=((a_1\ldots a_k)(a_{k+1}\ldots a_{n-1}))a_n=$$
$$=(\ldots((\ldots(a_1a_2)\ldots a_k)a_{k+1})\ldots a_{n-1})a_n,$$

т.е. снова левонормированное произведение. К тому же виду приводится и правая часть доказываемого равенства (I). Теорема доказана.

Теорема I2.2 позволяет в полугруппах использовать знак кратного умножения без расстановки скобок:

$\prod_{i=1}^{1}a_i=a_1a_2$, $\prod_{i=1}^{2}a_i=a_1a_2a_3,\ldots,\prod_{i=1}^{n}a_i=a_1a_2\ldots a_n$.

В частности, при $a_1=a_2=\ldots=a_n=a$ произведение $aa\ldots a$ обозначают символом a^n, называя его n-й **степенью элемента** a. Следствием теоремы I2.2 являются соотношения

(2) $a^na^m=a^{n+m}$, $(a^n)^m=a^{nm}$, $n,m\in\mathbb{N}$.

В полугруппе X с единицей e для любого $a\in X$ полагают еще $a^0=e$. Заметим еще, что если $ab=ba$, то

(3) $(ab)^n=a^nb^n$ для всех $n\in\mathbb{N}$,

что легко проверяется индукцией по n.

Для полугруппы с аддитивной записью вместо произведения $\prod_{i=1}^{n}a_i$ надо рассматривать сумму $\sum_{i=1}^{n}a_i=$
$=a_1+\ldots+a_n$, а вместо степени a^n элемента a кратное

РЕПОЗИТОРИЙ ГГУ

Формулы (2) примут вид

$$na+ma=(n+m)a\ ,\quad n(ma)=(nm)a\ ,\ n,m\in N,$$

а формула (3) для коммутирующих элементов a и b –

$$n(a+b)=na+nb\ .$$

Занесем полученные утверждения в таблицу № I.

Группой называется непустое множество G с бинарной алгебраической операцией (умножением), удовлетворяющей следующим аксиомам:

I) операция определена на G, то есть если a и $b\in G$, то $ab\in G$;

2) операция ассоциативна, то есть $(ab)c=a(bc)$ для всех $a,b,c\in G$;

3) в G существует единичный элемент, то есть такой элемент e, что $ae=ea=a$ для всех $a\in G$;

4) каждый элемент a из G обладает в G обратным элементом, то есть таким элементом a^{-1}, что $aa^{-1}=a^{-1}a=e$.

Более кратко, полугруппа с единицей, в которой каждый элемент обладает обратным, называется группой.

Определение группы мы дали для мультипликативной записи. С помощью таблицы № I для аддитивной записи получаем следующее определение:

Группой называется непустое множество G с бинарной алгебраической операцией (сложением), удовлетворяющей следующим аксиомам:

I) операция определена на G, то есть если a и $b\in G$, то $a+b\in G$;

2) операция ассоциативна, то есть $(a+b)+c=a+(b+c)$ для всех $a,b,c\in G$;

3) в G существует нулевой элемент, то есть такой элемент 0, что $a+0=0+a=a$ для всех $a\in G$;

4) каждый элемент $a\in G$ обладает в G противоположным элементом, то есть таким элементом $-a$, что $a+(-a)=-a+a=0$.

Группу с коммутативной операцией называют коммутативной или абелевой. Если G – конечное множество, являющееся группой, то G называют конечной группой, а число $|G|$ элементов в G – порядком группы G. Подмножество H группы G называется подгруппой, если H – группа относительно той же операции, что и G.

Пример I. Числовые группы.

а) $(Z,+),(Q,+),(R,+)$ – группы, причем Z – подгруппа Q и R, а Q – подгруппа R;

б) $(N,+)$ не является группой, так как в N нет нулевого элемента и противоположных. Однако, $(N,+)$ – полугруппа;

в) относительно умножения ни одно из множеств N,Z,Q,R группу не образует. Если положим $R^*=R\setminus\{0\}$, $Q^*=Q\setminus\{0\}$, то R^* и Q^* образуют группы, причем Q^* – подгруппа в R^*. Z^* и N^* не являются группами. Все указанные множества относительно умножения – полугруппы.

Множество $\{-1,1\}$ относительно умножения образует группу.

Пример 2. Матричные группы:

а) через $M(n,R)$ обозначим совокупность всех квадратных матриц порядка n с элементами из R. Ясно, что относительно умножения матриц $M(n,R)$ – полугруппа с единичным элементом $E=\begin{pmatrix}1&0&\dots&0\\0&1&\dots&0\\\dots&\dots&\dots&\dots\\0&0&\dots&1\end{pmatrix}$. Так как только невырожденные матрицы обладают обратными, то $M(n,R)$ – не группа..

б) Пусть $GL(n,R)=\{A\in M(n,R)\mid \det A\neq 0\}$. Тогда $GL(n,R)$ – группа, которую называют полной линейной группой степени n над R;

в) $SL(n,R)=\{A\in GL(n,R)\mid \det A=1\}$ – подгруппа в $GL(n,R)$, которая называется специальной линейной группой степени n над R.

Пример 3. Группы перестановок.

Совокупность S_n всех перестановок множества $X=\{1,2,\dots,n\}$ образует группу с единичным элементом $\varepsilon=\begin{pmatrix}1&2&\dots&n\\1&2&\dots&n\end{pmatrix}$, которую мы назвали в § 4 симметрической группой степени n. Четные перестановки образуют подгруппу группы S_n, которую мы назвали знакопеременной группой A_n степени n.

РЕПОЗИТОРИЙ ГГУ ИМ

Пример 4. Группы функций

а) Относительно умножения четыре функции $f_1(x)=x$, $f_2(x)=-x$, $f_3(x)=\frac{1}{x}$, $f_4(x)=-\frac{1}{x}$ образуют группу. Составим таблицу умножения

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Произведение $f_i f_j$ ставится на пересечении строки f_i и столбца f_j. Например,

$$f_2 f_3 : x \xrightarrow{f_3} \frac{1}{x} \xrightarrow{f_2} -\frac{1}{x}$$

поэтому $f_2 f_3 = f_4$.

Из таблицы видно, что умножение определено на множестве $\{f_1, f_2, f_3, f_4\}$. Поскольку умножение отображений ассоциативно, то выполняется вторая аксиома группы. Функция f_1 является единичным элементом, а $f_i^{-1}=f_i$, то есть каждый элемент себе обратен.

б) Группа $A_1(\mathbb{R})$ аффинных преобразований прямой состоит из отображений $\varphi_{a,b}: x \mapsto ax+b$, $a,b\in\mathbb{R}$, $a\neq 0$. $A_1(\mathbb{R})$ является группой с единичным элементом $\varphi_{1,0}$ и обратным элементом $\varphi_{a^{-1},-a^{-1}b}$ к элементу $\varphi_{a,b}$.

§ 13. ПОДГРУППЫ

Напомним, что подмножество H группы G называется её подгруппой, если H – группа относительно той же операции, что и G. Для подгруппы используется обозначение $H \leq G$, читается H – подгруппа группы G. Следующая теорема показывает, что для подгрупп не надо проверять все аксиомы группы.

Теорема 13.1. Непустое подмножество H группы G будет подгруппой тогда и только тогда, когда

1) $h_1 h_2 \in H$ для всех $h_1, h_2 \in H$;

2) $h^{-1} \in H$ для каждого $h \in H$.

Доказательство. Пусть H – подгруппа группы G, то есть H – группа относительно той же операции, что и в G. Поэтому на H определена алгебраическая операция из G, то есть выполняется первое требование теоремы.

Обратные элементы к элементам из H существуют и в G и в H, нам надо доказать, что они совпадают.

Вначале проверим, что единица e_0 подгруппы H совпадает с единицей e группы G. Ясно, что $e_0 e = e e_0 = e_0$, так как e_0 – элемент из G. В группе G для e_0 имеется обратный e_0^{-1}, то есть $e_0^{-1} e_0 = e_0 e_0^{-1} = e$. Так как e_0 – единица в H, то $e_0 e_0 = e_0$.

Умножим обе части на e_0^{-1}:

$$e_0^{-1}(e_0 e_0) = e_0^{-1} e_0 \quad \text{или} \quad e e_0 = e,$$

а значит $e = e_0$. Таким образом, единицы H и G совпадают.

Так как H – подгруппа, то для каждого $h \in H$ существует обратный в H элемент $h^{-1} \in H$, то есть $h^{-1}h = hh^{-1} = e_0 = e$. Это означает, что h^{-1} является обратным в G для элемента $h \in H$. Второе требование теоремы также выполняется.

Обратно, пусть справедливо 1) и 2) для непустого подмножества. Из 1) следует, что алгебраическая операция определена на H. Она ассоциативна в H, так как ассоциативность справедлива для всех элементов из G. Согласно 2) элемент h^{-1} обратный к $h \in H$ также принадлежит H. Применяя 1) получаем, что $h^{-1}h \in H$ и $hh^{-1} \in H$. Поскольку $h^{-1}h = e = hh^{-1}$, то $e \in H$ и H – группа.

Теорема 13.2. Пересечение любого семейства подгрупп группы является подгруппой.

Доказательство. Пусть $D = \bigcap H_\lambda$, где H_λ – подгруппа в G. Если d_1 и $d_2 \in D$, то d_1 и $d_2 \in H_\lambda$ для всех λ. Поэтому $d_1 d_2 \in H_\lambda$ и $d_1 d_2 \in D$. Если $d \in D$, то $d \in H_\lambda$ и $d^{-1} \in H_\lambda$ для всех λ. Поэтому $d^{-1} \in D$ и по теореме 13.1 D – подгруппа.

Зафиксируем элемент a в группе G. Пересечение всех

РЕПОЗИТОРИЙ ГГУ ИМ

подгрупп из G, содержащих элемент a, назовем **циклической подгруппой, порожденной элементом a**, и обозначим через $\langle a\rangle$. Таким образом,

$$\langle a\rangle = \bigcap_{a\in H\leq G} H$$

Теорема 13.3. Циклическая подгруппа $\langle a\rangle$, порожденная элементом a, состоит из всевозможных степеней элемента a, то есть

$$\langle a\rangle = \{a^m \mid m\in\mathbb{Z}\}.$$

Доказательство. По определению $\langle a\rangle = \bigcap_{a\in H\leq G} H$. Так как H – подгруппа и $a\in H$, то $a^m = \underbrace{a\cdot a\cdot\ldots\cdot a}_{m\text{ раз}} \in H$ для каждого натурального m. Кроме того, $a^0 = e \in H$. Далее, так как $a^{-1}\in H$, то $a^{-m}\in H$ для всех натуральных m. Итак, мы доказали, что $A=\{a^m \mid m\in\mathbb{Z}\}\subseteq H$ как только $a\in H$. Значит $A\subseteq\langle a\rangle$.

Далее, подмножество A является подгруппой, содержащей элемент a. Поэтому A встречается среди подгрупп, участвующих в пересечении $\bigcap_{a\in H\leq G} H = \langle a\rangle$, то есть $A\geq\langle a\rangle$.

Теорема доказана.

Пусть G – произвольная группа и $a\in G$. Тогда $\langle a\rangle = \{a^m \mid m\in\mathbb{Z}\}$ по предыдущей теореме. Имеются только две следующие возможности:

1) все степени элемента a различны, то есть $a^m\neq a^n$ при целых $m\neq n$. В этом случае говорят, что a имеет **бесконечный порядок**.

2) Имеются совпадения $a^m = a^n$ при $m\neq n$. Если, например, $m>n$, то $m-n>0$ и $a^{m-n}=e$, то есть существуют натуральные степени элемента a, равные единичному элементу. Пусть k – наименьшее положительное число, при котором $a^k = e$. Тогда говорят, что a – элемент **конечного порядка k**. В конечной группе все элементы, очевидно, имеют конечный порядок.

Пример 1. Покажем, что порядок перестановки есть наименьшее общее кратное длин ее независимых циклов.

Если (a_1a_2) – цикл длины 2, то $(a_1a_2)(a_1a_2)=\varepsilon$, то есть транспозиция есть перестановка порядка 2. Если

$(a_1a_2a_3)$ – цикл длины 3, то $(a_1a_2a_3)(a_1a_2a_3) = (a_1a_3a_2)$, а $(a_1a_2a_3)^3=\varepsilon$, то есть цикл длины 3 имеет порядок 3. Аналогично цикл $(a_1\ldots a_k)$ длины k есть перестановка порядка k.

Пусть теперь перестановка

$$\tau = (a_1a_2\ldots a_{\ell_1})\ldots(b_1b_2\ldots b_{\ell_t})$$

разложима в произведение независимых циклов длины $\ell_1,\ell_2,\ldots,\ell_t$. Так как независимые циклы перестановочны, то

$$\tau^k = (a_1a_2\ldots a_{\ell_1})^k\ldots(b_1b_2\ldots b_{\ell_t})^k.$$

Поэтому $\tau^k=\varepsilon$ тогда и только тогда, когда k делится на $\ell_1,\ell_2,\ldots,\ell_t$; то есть k – кратное числам $\ell_1,\ell_2,\ldots,\ell_t$. Если k – порядок перестановки τ, то k – наименьшее натуральное число, для которого $\tau^k=\varepsilon$. Следовательно, порядок перестановки есть наименьшее кратное длин ее независимых циклов.

Теорема 13.4. Пусть элемент $a\in G$ имеет конечный порядок k. Тогда $\langle a\rangle = \{e,a,a^2,\ldots,a^{k-1}\}$ и $a^m=e$ тогда и только тогда, когда $m=kq$, где q – целое число.

Доказательство. По теореме 13.3 циклическая группа $\langle a\rangle=\{a^m \mid m\in\mathbb{Z}\}$ состоит из всевозможных степеней a^m, где m пробегает все целые числа. Мы знаем, что любое целое число m можно представить в виде $m=kq+r$, где $r=0,1,\ldots,k-1$. Поэтому $a^m = a^{kq+r} = a^{kq}a^r = (a^k)^q a^r = a^r$ и $\langle a\rangle\in\{e,a,\ldots,a^{k-1}\}$.

Обратное включение очевидно, значит,

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

Так как $a^m=a^r$, то $a^m=e$ лишь при $r=0$, то есть когда $m=kq$.

Теорема 13.4 позволяет для конечных групп отбросить условие 2 в теореме 13.1.

Теорема 13.5. Пусть H – непустое подмножество произвольной группы G и предположим, что каждый элемент из H имеет конечный порядок. Если $h_1h_2\in H$ для всех h_1 и $h_2\in H$, то H – подгруппа.

Доказательство. Так как каждый элемент $h\in H$ имеет конечный порядок, то $\langle h\rangle =$

РЕПОЗИТОРИЙ ГГУ ИМ

$=\{e, h, \dots, h^{k-1}\}$, где $k=|\langle h\rangle|$. Очевидно, $hh^{k-1}=h^{k-1}h=h^k=e$ и $h^{k-1}=h^{-1}$. По условию теоремы $h^{-1}=hh\dots h\in H$. Теперь H – подгруппа по теореме I3.I.

Следствие. Если H – подмножество конечной группы G и $h_1, h_2\in H$ для всех h_1 и $h_2\in H$, то H – подгруппа.

С помощью таблицы № I сформулируем наши утверждения в аддитивной записи.

Теорема I3.3. Циклическая подгруппа $\langle a\rangle$, порожденная элементом a, состоит из всевозможных кратных элемента a, то есть

$$\langle a\rangle=\{ma \mid m\in\mathbb{Z}\}.$$

Наименьшее натуральное n, при котором $na=0$, называется порядком элемента a. Если такого n нет, то a – элемент бесконечного порядка.

Теорема I3.4. Пусть элемент $a\in G$ имеет конечный порядок k. Тогда $\langle a\rangle=\{0, a, 2a, \dots, (k-1)a\}$ и $ma=0$ тогда и только тогда, когда $m=kq$, где q – целое число.

Пример 2. Рассмотрим группу $(\mathbb{Z}, +)$ целых чисел относительно сложения. Тогда $\langle 1\rangle=\{m\cdot 1 \mid m\in\mathbb{Z}\}$, то есть циклическая подгруппа, порожденная элементом I, совпадает со всей группой. Итак, $\mathbb{Z}$ – бесконечная циклическая группа. Проверьте, что $\langle -1\rangle=\mathbb{Z}$.

Пусть H – подгруппа произвольной группы G. Левым смежным классом группы G по подгруппе H называется множество aH элементов вида ah, где a – фиксированный элемент из G, а h пробегает все элементы подгруппы H. Элемент a называется представителем смежного класса aH. Таким образом, $aH=\{ah \mid h\in H\}$.

Аналогично определяется правый смежный класс $Ha=\{ha \mid h\in H\}$.

Лемма I3.6. Пусть G – группа, H – ее подгруппа. Тогда

1) $eH=He=H$;
2) $a\in aH$ для каждого $a\in G$;
3) если $a\in H$, то $aH=H$, если $b\in aH$, то $bH=aH$,

4) $aH=bH$ тогда и только тогда, когда $b^{-1}a\in H$;
5) два смежных класса либо совпадают, либо их пересечение пусто;
6) если H – конечная подгруппа, то $|aH|=|H|$ для всех $a\in G$.

Доказательство. Первые три свойства вытекают из определения смежного класса.

4) Если $aH=bH$, то $ae=bh$, $h\in H$ и $b^{-1}a\in H$. Обратно, если $b^{-1}a\in H$, то $a=bh$ и $aH=bhH=bH$.

5) Пусть $aH\cap bH\neq\emptyset$ и $c\in aH\cap bH$. Тогда $c=ah_1=bh_2$ и $b^{-1}a=h_2h_1^{-1}\in H$. Теперь $aH=bH$ по свойству 4).

6) Пусть H – конечная подгруппа. Тогда отображение $\varphi: h\mapsto ah$ есть биекция множеств H и aH. Поэтому $|H|=|aH|$.

Теорема I3.7. Пусть G – произвольная группа, H – ее произвольная подгруппа. Тогда G является объединением непересекающихся левых смежных классов по H.

Доказательство. Если g – произвольный элемент из G, то $g\in gH$ и $G=\bigcup_{g\in G} gH$.

Так как различные смежные классы имеют пустое пересечение, то отобрав все попарно различные смежные классы, мы получим разложение $G=\cup g_\alpha H$ группы G на непересекающиеся левые смежные классы по H.

Если G – конечная группа, то число различных левых смежных классов по H также будет конечно, оно называется индексом подгруппы H в группе G и обозначается через $|G:H|$.

Теорема I3.8 (Лагранж). Если H – подгруппа конечной группы G, то $|G|=|H||G:H|$. В частности, порядок конечной группы делится на порядок каждой своей подгруппы.

Доказательство. По теореме I3.7 имеем разложение

$$G=g_1H\cup g_2H\cup\dots\cup g_nH$$

где $n=|G:H|$. Так как $|g_iH|=|H|$ для каждого i

РЕПОЗИТОРИЙ ГГУ

по свойству 6, то $|G| = |H|\,|G:H|$.

Пример 3. Найдем разложение $S_3 = \{e,(12),(13),(23),(123),(132)\}$ по подгруппе $H = \{e,(12)\}$.

Решение.

$$eH = (12)H = H;$$
$$(13)H = (13)\{e,(12)\} = \{(13),(123)\};$$
$$(23)H = (23)\{e,(12)\} = \{(23),(132)\};$$
$$(123)H = (123)\{e,(12)\} = \{(123),(13)\} = (13)H;$$
$$(132)H = (132)\{e,(12)\} = \{(132),(23)\} = (23)H;$$

$$S_3 = eH \cup (13)H \cup (23)H =$$
$$= (12)H \cup (123)H \cup (132)H.$$

Теорема 13.9. Группа простого порядка циклическая.

Доказательство. Пусть G – конечная группа простого порядка p. Выберем неединичный элемент a из G и рассмотрим циклическую подгруппу $A = \langle a \rangle$, порожденную этим элементом a.

Так как $a \neq 1$, то $A \neq 1$, а по теореме Лагранжа порядок $|A|$ делит порядок $|G| = p$. Поскольку p – простое число, то $|A| = p$ и $|A| = |G|$, то есть $A = G$ и G – циклическая группа, порожденная своим неединичным элементом.

Пример 4. Найдем все подгруппы группы S_3. Порядок $|S_3| = 6$, поэтому по теореме Лагранжа ее подгруппы могут быть только следующих порядков; 1,2,3,6. Подгруппы порядка 1 и 6 это единичная подгруппа $\langle e \rangle$ и вся группа S_3. Подгруппы порядка 2 и 3 по теореме 13.9 циклические, поэтому для их нахождения надо пересмотреть все циклические подгруппы в S_3. После этого получаем следующие подгруппы в S_3:

$$H_1 = \langle e \rangle = \{e\};$$
$$H_2 = \langle (12) \rangle = \{e,(12)\};$$
$$H_3 = \langle (13) \rangle = \{e,(13)\};$$
$$H_4 = \langle (23) \rangle = \{e,(23)\};$$

$$H_5 = \langle (123) \rangle = \{e,(123),(132)\} =$$
$$= \langle (132) \rangle = \{(132),(123),e\};$$
$$H_6 = S_3.$$

Итак, S_3 имеет шесть подгрупп.

§ 14. ИЗОМОРФИЗМ ГРУПП

Две группы $(G,\circ)$ и $(G',*)$ с операциями $\circ$ и $*$ называются изоморфными, если существует биекция $f: G \to G'$ такая, что $f(a \circ b) = f(a) * f(b)$ для всех $a, b \in G$. Факт изоморфизма групп обозначают символически $G \cong G'$.

Отметим простейшие свойства изоморфизма.

Лемма 14.1. Нейтральный элемент переходит в нейтральный, то есть если n – нейтральный элемент G, то $f(n)$ – нейтральный элемент G'.

Доказательство. $n \circ a = a \circ n = a$ для любого $a \in G$. Поэтому $f(n \circ a) = f(n) * f(a) = f(a \circ n) = f(a) * f(n) = f(a)$. Поскольку f – сюръекция, то $f(a)$ пробегает все элементы G', если a пробегает элементы G. Значит, $f(n)$ – нейтральный элемент группы G'.

Лемма 14.2. Симметричный элемент переходит в симметричный, то есть если b – симметричный элемент к a в группе G, то $f(b)$ – симметричный элемент к $f(a)$ в группе G'.

Доказательство. $a \circ b = b \circ a = n$, поэтому $f(a \circ b) = f(a) * f(b) = f(b \circ a) = f(b) * f(a) = f(n)$. Так как $f(n)$ – нейтральный элемент G', то $f(b)$ – симметричный элемент к $f(a)$.

Свойства изоморфизма даны при произвольной записи операций. Если в обеих группах используем мультипликативную запись, то при изоморфизме единица переходит в единицу (лемма 14.1), обратный в обратный (лемма 14.2). Если в обеих группах аддитивная запись, то ноль переходит в ноль, противоположный в противоположный. Если группы $(G,\cdot)$ и $(G',+)$ изоморфны, то единица переходит в ноль, а обратный элемент в противоположный.

В дальнейшем будем использовать в обеих группах мульти-

РЕПОЗИТОРИЙ ГГУ ИМ

пликативную запись.

Лемма I4.3. Каждая группа изоморфна себе, то есть $G \cong G$.

Доказательство. Отображение $e_G: G \to G$, переводящее каждый элемент в себя, то есть $e_G: g \mapsto g$ для всех $g \in G$, очевидно, изоморфизм G на G.

Мы знаем, что для каждого биективного отображения $f: G \to G'$ существует обратное отображение $f^{-1}: G' \to G$, которое также будет биекцией. Если $a \in G$ и $f(a) = a' \in G'$, то $f^{-1}(a') = a$. Пусть еще $b \in G$ и $b' = f(b) \in G'$. Тогда $f^{-1}(b') = b$ и $a'b' = f(a)f(b) = f(ab)$ поскольку f изоморфизм. Отсюда $f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b')$, что доказывает изоморфизм f^{-1}. Таким образом, мы получили следующую лемму.

Лемма I4.4. Обратное отображение $f^{-1}: G' \to G$ является изоморфизмом. Таким образом, если $G \cong G'$, то $G' \cong G$.

Лемма I4.5. Если $G \cong G'$, а $G' \cong G''$, то $G \cong G''$.

Доказательство. Пусть $f: G \to G'$ - изоморфизм групп G и G', а $\varphi: G' \to G''$ - изоморфизм G' и G''. Тогда φf - биективное отображение G на G'', причем $(\varphi f)(ab) = \varphi(f(ab)) = \varphi(f(a)f(b)) = \varphi(f(a)) \cdot \varphi(f(b)) = \varphi f(a) \varphi f(b)$ для любых a и $b \in G$. Значит, φf - изоморфизм G и G''.

Таким образом, отношение "быть изоморфными группами" согласно леммам I4.3, I4.4 и I4.5 является отношением эквивалентности. Поэтому множество всех групп распадается на пересекающиеся классы изоморфных групп. Следующая теорема утверждает, что циклические группы одного порядка попадут в один класс изоморфных групп.

Теорема I4.6. Все бесконечные циклические группы изоморфны между собой и изоморфны аддитивной группе целых чисел. Все конечные циклические группы одного порядка изоморфны между собой.

Доказательство. Пусть $\langle q \rangle$ - бесконечная циклическая группа, порожденная элементом q, а $\mathbb{Z}$ - аддитивная группа целых чисел. Все степени q^n различны, поэтому отображение $f: n \mapsto q^n$ будет биекцией между $\mathbb{Z}$ и $\langle q \rangle$. Так

как $q^m q^n = q^{m+n}$, то $f(m+n) = q^{m+n} = q^m \cdot q^n = f(m) f(n)$ и f - изоморфизм. Таким образом, каждая бесконечная циклическая группа изоморфна аддитивной группе целых чисел. Поэтому все бесконечные циклические группы изоморфны.

Пусть теперь $G_1 = \{e, g_1, g_1^2, \ldots, g_1^{k-1}\}$ и $G_2 = \{e, g_2, g_2^2, \ldots, g_2^{k-1}\}$ - две циклические группы порядка k. Для простоты рассуждения считаем, что G_1 и G_2 записаны мультипликативно. Определим отображение $f: g_1^l \mapsto g_2^l$, $l = 0, 1, 2, \ldots, k-1$. Для любых n и $m \in \{0, 1, \ldots, k-1\}$ пусть $n+m = kq + r$, $r = 0, 1, \ldots, k-1$. Тогда

$$f(g_1^n g_1^m) = f(g_1^{n+m}) = f(g_1^r) = g_2^r = g_2^{n+m} = g_2^n g_2^m = f(g_1^n) \cdot f(g_1^m)$$

Пример I. Проверим, что $G = \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$ - группа относительно умножения, изоморфная мультипликативной группе $G' = \{+1, -1\}$. Так как $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} \in G$, то $\begin{pmatrix}0&1\\1&0\end{pmatrix}^{-1} = \begin{pmatrix}0&1\\1&0\end{pmatrix} \in G$. Остальные произведения элементов из G также принадлежат G, поэтому G - группа. Отображение $\begin{pmatrix}1&0\\0&1\end{pmatrix} \mapsto 1, \begin{pmatrix}0&1\\1&0\end{pmatrix} \mapsto -1$, очевидно, будет изоморфизмом.

Пример 2. Покажем, что мультипликативная группа $(\mathbb{R}_+, \cdot)$ положительных действительных чисел изоморфна аддитивной группе $(\mathbb{R}, +)$ всех действительных чисел. В качестве изоморфного отображения f может служить логарифм $\ln x$. Если x и $y \in \mathbb{R}_+$, то $\ln(xy) = \ln x + \ln y$. Так как функция $y = \ln x$ задает биективное отображение $\mathbb{R}_+$ на $\mathbb{R}$, то $\ln$ - изоморфизм группы $(\mathbb{R}_+, \cdot)$ и $(\mathbb{R}, +)$.

Установим теперь связь между перестановками из S_n и квадратными $n \times n$ -матрицами. Матрицей перестановки $\pi \in S_n$ назовем $n \times n$ -матрицу $M(\pi) = (a_{ij})$, определенную так

$$a_{ij} = \begin{cases} 1, & \text{если } i = \pi(j) \\ 0, & \text{если } i \neq \pi(j) \end{cases}.$$

Таким образом, в матрице перестановки n единиц, остальные элементы равны нулю. Единица встречается один раз в каждой

РЕПОЗИТОРИЙ ГГУ ИМ.

строке и в каждом столбце. В j -ом столбце единица стоит на $\pi(j)$-м месте, то есть в матрице $M(\pi)$ только элементы $a_{\pi(k)k}=1$, где $k=1,2,\dots,n$, остальные - нули. Очевидно, $M(e)=E$.

Пример 3. Найдем матрицы, соответствующие перестановкам степени 3. Так как $S_3=\{e,(12),(13),(23),(132),(123)\}$, то

$$M(e)=E,\quad M(12)=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},\ M(13)=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},$$

$$M(23)=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\ M(123)=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\ M(132)=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}.$$

Теорема 14.7. Матрица произведения перестановок равна произведению матриц перестановок, то есть $M(\pi\tau)=M(\pi)M(\tau)$ для всех $\pi,\tau\in S_n$.

Доказательство. Пусть $\pi(k)=i$, тогда в строке $M(\pi)_i$ единица стоит на k -ом месте. В столбце $M(\tau)^j$ единица стоит на $\tau(j)$ -м месте. Поэтому

$$M(\pi)_i\,M(\tau)^j=(0\dots1\dots0)[0\dots1\dots0]=$$

$$=\left\{\begin{array}{l}1,\text{если } k=\tau(j),\text{ где } \pi(k)=i\\0,\text{если } k\neq\tau(j)\end{array}\right\}=\left\{\begin{array}{l}1,\text{ если } i=\pi\tau(j)\\0,\text{ если } i\neq\pi\tau(j)\end{array}\right\}.$$

Так как $M(\pi\tau)=(a_{ij})$, где $a_{ij}=\left\{\begin{array}{l}1,\text{если } i=\pi\tau(j)\\0,\text{если } i\neq\pi\tau(j)\end{array}\right\}$,

то $a_{ij}=M(\pi)_i\,M(\tau)^j$ и $M(\pi\tau)=M(\pi)M(\tau)$.

Теорема 14.8. $\det M(\pi)=\operatorname{sgn}\pi$ для всех $\pi\in S_n$.

Доказательство. В матрице $M(\pi)=(a_{ij})$ только элементы $a_{\pi(k)k}$ равны единице, где $k=1,2,\dots,n$; остальные - нули. Если $\tau\neq\pi^{-1}$, то существует число m такое, что $\tau(m)\neq\pi^{-1}(m)$ и $a_{m\pi^{-1}(m)}\neq a_{m\tau(m)}$. Но $a_{m\pi^{-1}(m)}=a_{\pi(\pi^{-1}(m))\pi^{-1}(m)}=1$, значит $a_{m\tau(m)}=0$ и в сумме $\det M(\pi)=$

$=\sum_{\tau\in S_n}\operatorname{sgn}\tau\,a_{1\tau(1)}\dots a_{n\tau(n)}$ только одно ненулевое слагаемое, которое отвечает перестановке π^{-1}. Поэтому $\det M(\pi)=\operatorname{sgn}\pi^{-1}a_{1\pi^{-1}(1)}\dots a_{n\pi^{-1}(n)}$. Поскольку $\operatorname{sgn}\pi^{-1}=\operatorname{sgn}\pi$, а $a_{i\pi^{-1}(i)}=a_{\pi\pi^{-1}(i)\pi^{-1}(i)}=1$, то $\det M(\pi)=\operatorname{sgn}\pi$.

Пример 4. Отображение $M:\tau\mapsto M(\tau)$ осуществляет изоморфизм симметрической группы S_n степени n и подгруппы $\operatorname{Im}S_n=\{M(\tau)\mid\tau\in S_n\}$ из группы $GL(n,\mathbb{R})$. Проверим этом.

Так как $\det M(\tau)=\operatorname{sgn}\tau\in\{-1,1\}$, то M отображение S_n в $GL(n,\mathbb{R})$. Из построения $M(\tau)$ следует, что M - инъекция. Покажем, что $\operatorname{Im}S_n$ - подгруппа группы $GL(n,\mathbb{R})$. Так как $M(\tau)M(\pi)=M(\tau\pi)$ по теореме 14.7, то $M(\tau)M(\pi)\in\operatorname{Im}S_n$. Далее, $M(e)=E$, и если τ имеет порядок t, то $\tau^t=e$ и $M(\tau^t)=E=M(\tau)^t$, то есть порядок матрицы $M(\tau)$ делит t. Таким образом, все матрицы перестановок имеют конечные порядки и $\operatorname{Im}S_n$ - подгруппа $GL(n,\mathbb{R})$ по теореме 13.5. Поэтому $M:S_n\to\operatorname{Im}S_n$ - биекция, а по теореме 14.7 отображение M - изоморфизм.

Теорема 14.9 (Кэли). Любая конечная группа порядка n изоморфна подгруппе симметрической группы S_n степени n.

Доказательство. Пусть G - конечная группа порядка n и $G=\{q_1=e,q_2,\dots,q_n\}$ - все ее элементы. Поскольку природа символов, переставляемых элементами из S_n, несущественна, то можно считать, что S_n - совокупность всех биективных отображений множества $\{e,q_2,\dots,q_n\}$ на себя.

Для каждого $x\in G$ определим отображение $l_x:q_i\mapsto xq_i=l_x(q_i)$ множества G в себя. Если $xq_i=xq_j$, то $q_i=q_j$ и l_x - инъекция. Но инъекция конечного множества всегда биекция, поэтому $l_x\in S_n$.

Зададим теперь отображение $\varphi:G\to S_n$, полагая $\varphi:x\mapsto l_x$. Тогда $\operatorname{Im}G=\{l_{q_1},l_{q_2},\dots,l_{q_n}\}$. Покажем, что $\operatorname{Im}G$ - подгруппа группы S_n. Если l_x и l_y - произвольные элементы из $\operatorname{Im}G$, то

РЕПОЗИТОРИЙ ГГУ им.

(I) $(l_x l_y)(g_i) = l_x(l_y(g_i)) = (xy)g_i = l_{xy}(g_i)$

и $l_x l_y = l_{xy}$. При $y = x^{-1}$ из (I) заключаем, что $l_x l_{x^{-1}}(g_i) = x x^{-1} g_i = g_i$, аналогично $(l_{x^{-1}} l_x)(g_i) = g_i$, поэтому $l_x l_{x^{-1}} = l_{x^{-1}} l_x = e$ и $e_{x^{-1}} = (e_x)^{-1} \in \mathrm{Im}\, G$. По теореме I3.I множество $\mathrm{Im}\, G$ есть подгруппа группы S_n.

Из (I) мы заключаем, что $l_x l_y = l_{xy}$, поэтому $\varphi(xy) = \varphi(x)\varphi(y)$ и φ – изоморфизм между G и $\mathrm{Im}\, G$. Теорема Кэли доказана.

Сопоставляя теорему Кэли с примером 3, мы получаем

Следствие. Любая конечная группа порядка n изоморфна подгруппе полной линейной группы $GL(n, \mathbb{R})$ степени n над $\mathbb{R}$.

Положив $G' = G$ в определении изоморфизма, мы получим изоморфное отображение группы G на себя, которое называют **автоморфизмом** группы G. Если φ и ψ – автоморфизмы G, то

$(\varphi\psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = \varphi(\psi(a))\varphi(\psi(b)) = (\varphi\psi)(a)(\varphi\psi)(b)$ для любых $a, b \in G$. Поэтому $\varphi\psi$ – автоморфизм G и произведение автоморфизмов определено. Ассоциативность умножения автоморфизмов вытекает из ассоциативности умножения отображений. Единичное отображение $e_G : G \to G$, переводящее каждый элемент в себя, является автоморфизмом. По свойству 4 при $G' = G$ каждый автоморфизм обладает обратным. Поэтому справедлива

Теорема I4.I0. Совокупность $\mathrm{Aut}\, G$ всех автоморфизмов группы G является группой.

СОДЕРЖАНИЕ

РЕПОЗИТОРИЙ ГГУ ИМ

Виктор Степанович Монахов

Перестановки и определители
Учебное пособие

Ответственный за выпуск В.С.Монахов
Редактор Л.Зайцева

Подписано к печати 20.11.87 Формат 60x84 1/16.
Бумага писчая № 1. Печать офсетная. Усл.п.л. 4,09.
Уч.-изд.л. 3,7. Тираж 150. Заказ 119 Цена 12 к.
Отпечатано на ротапринте ГГУ, г.Гомель, ул.Советская, 104.

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ