

Алгебра

материал по лекциям Александра Владимировича Анашкина

March 2023

Содержание

Группы. Часть 1 - Вводная	2
Определение	2
Свойства	2
Группы. Часть 2	4
Группа перестановок	4
Группа диэдра	5
Группа кватернионов	6
Кольца	7
Определение	7
Свойства	7
Примеры	8
Функция Мёбиуса	9
Определение	9
Свойства	9
Примеры	9
Функция Эйлера	10
Определение	10
Свойства	10
Примеры	10
Приложение	10
Матрицы	11
Определение	11
Свойства	11
Примеры	12
Приложение	14
Отображение	15
Определение	15
Свойства	15
Примеры	15
Гомоморфизм	16
Определение	16
Свойства	16

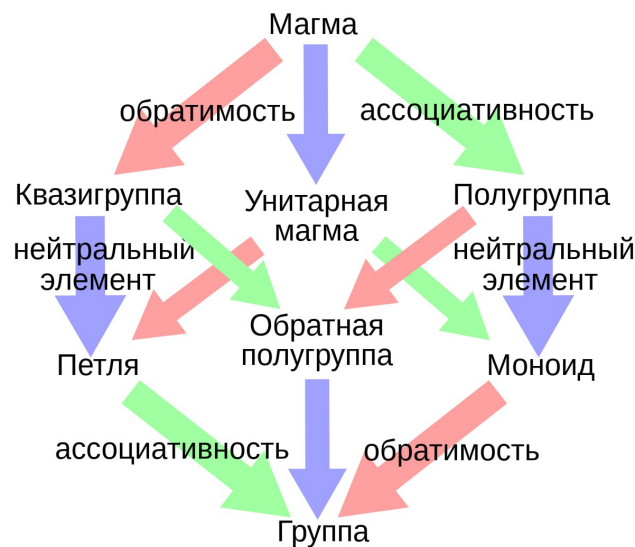
Группы. Часть 1 - Вводная

Определение

- **Группоид** - множество с операцией: $(G, *)$
 $*: G \times G \rightarrow G$
- **Полугруппа** - группоид с ассоциативной операцией
- **Моноид** - полугруппа с нейтральным элементом:
 $e*a=a*e=a$, e - нейтральный, $a, e \in (G, *)$
- **Группа** - моноид, в которой каждый элемент обратим (нейтральный сам к себе обратен), то есть для любого элемента справедливо:

$$a * a^{-1} = a^{-1} * a = e, \text{ где } a, a^{-1}, e \in (G, *)$$

Примечание: Вообще помимо указанной структуры и ее производных имеется пласт других структур. Для любознательных:



...правая половина как раз олицетворяет программу курса.

Связные теоремы

- Теорема Лагранжа: если G — группа **конечного** порядка (см. свойства) n , то порядок n_1 любой её подгруппы (см. свойства) H является делителем порядка группы. Из этого следует, что и порядок любого элемента делит порядок группы.

$$|G| < \infty, H < G \Rightarrow H/|G|$$

- Критерий множества быть подгруппой: Пусть $H \subset G$, $H \neq \emptyset$. Тогда $H < G \Leftrightarrow \forall a, b \in H \quad ab^{-1} \in H$
- 1-ая т. Силова: силовская подгруппы (см. свойства) существует
- 2-ая т. Силова: две любые силовские подгруппы сопряжены (см. свойства)
- 3-ья т. Силова: если N_p - кол-во силовских подгрупп, то $N_p \equiv 1 \pmod p$

Свойства и связанные определения

- Группа называется абелевой, если на ней выполняется коммутативность операции
- Для каждого элемента a обратный элемент a^{-1} единственен
- Нейтральный элемент единственен

- Группа H является подгруппой группы G :
 - Если H подмножество в G
 - H образует группу по той же операции, что и G

Обозначение: $H < G$

- Порядок/мощность группы G - число элементов в этой группе. Обозначается как $|G|$
- Порядок элемента - минимальная степень, в которую нужно возвести элемент, чтобы получить нейтральный:

$$\text{ord } g = \min\{n \in \mathbb{N} | g^n = e\}$$

В противном случае $\text{ord } g = \infty$

- $g \in G, gH = \{gh | h \in H\}$ - левый смежный класс (правый по аналогии) группы G по подгруппе H
- Группа называется циклической, если она порождена одним элементом и обозначается $\langle g \rangle = \{g, g^1, g^2, \dots, g^n\}$. Циклические группы всегда абелевы. Группы простых порядков всегда циклические
- Четверная группа Клейна V_4 - группа порядка четыре, в которой порядок каждого элемента, отличного от единицы, равен 2.
 $|G| = n = 4, G = \{e, \alpha, \beta, \gamma\}$

	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

$$\text{ord } \alpha = \text{ord } \beta = \text{ord } \gamma = 2$$

- Экспонента в конечной группе равна НОК'у порядков всех элементов группы, обозначается $\exp(G)$
- Пусть $g_1, g_2 \in G \Leftrightarrow$ (равносильно) $\exists h \in G, g_2 = h^{-1}g_1h$ - сопряженный элемент. Сопряженность удовлетворяет трем свойствам:
 - Рефлексивность. $g = e^{-1}ge \Leftrightarrow g \sim g$
 - Симметричность. $g_1 = h^{-1}g_2h = h^{-1^{-1}}g_2h^{-1} = \{h^{-1} = n\} \Rightarrow g_1 = n^{-1}g_2n$
 - Транзитивность. $g_2 \sim g_1$ и $g_3 \sim g_2 \Rightarrow g_3 \sim g_1$

Отношением быть сопряженными элементами на какой-то группе называется отношением эквивалентности

- H нормальный делитель G , если:
 - $\forall g \in G \Rightarrow Hg = gH$
 - $\forall g \in G \Rightarrow g^{-1}Hg = H$
 - $\forall g \in G, \forall h \in H \Rightarrow g^{-1}Hg \sim H$

Все три условия эквивалентны и являются определениями. Обозначение: $H \triangleleft G$

- Если H - нормальная подгруппа группы G , то операция умножения смежных классов $aH * bH = abH$ задает на множестве G/H структуру группы. Эта группа называется факторгруппой группы G по подгруппе H . Единицей в G/H служит смежный класс H , а элементом, обратным к смежному классу aH - смежный класс $a^{-1}H$
- $|G| = p^t s, \text{НОД}(s, p) = 1, H < G$
 - $|H| = p^t$, то H - p -подгруппа в G .
 - $|H| = p^t \Rightarrow H$ - силовская подгруппа в G

Группы. Часть 2

В данном разделе речь пойдет о разновидностях групп таких, как: группы перестановок (подстановок), диэдральных групп и групп кватернионов.

Группа перестановок S_n

Определения

Введение:

1. Расположение натуральных чисел $1, 2, 3, \dots, n$ в некотором определенном порядке называется перестановкой из n чисел
2. Операция перехода от одной перестановки к другой, при которой два числа меняются местами, а остальные остаются на своих местах, называется транспозицией. К примеру:

$$(1\ 6\ 2\ 4\ 3\ 5) \Rightarrow (1\ 3\ 2\ 4\ 6\ 5)$$

Суть:

Возьмём две различные перестановки и одну подставим под другой следующим образом (в общем виде):

$$S_n, \pi \in S_n, \pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix},$$

3. Пусть имеется некоторая перестановка чисел из $1, 2, 3, \dots, n$. Если некоторое число i из этой перестановки больше, чем некоторое число j из этой же перестановки ($i > j$), причем i предшествует j , то говорят, что эта пара чисел составляет инверсию (беспорядок). Число пар, образующих инверсию, называют числом инверсий перестановки. К примеру перестановка:

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

содержит 8 инверсий. А именно,

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

4. Перестановка называется чётной: $\delta(\pi) = 0$, если она имеет чётное число инверсий. Иначе называется нечётной $\delta(\pi) = 1$.

5. Всякое взаимно-однозначное отображение множества A первых n натуральных чисел на себя называется подстановкой n -ой степени. Причем первую перестановку в подстановке мы всегда можем переставить в тождественную, путем транспозиций. Разумеется вторая подстановка должна взаимно-однозначно отображаться на первую. Следовательно, все подстановки можно записать как:

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

6. Теорема: $x^{-1}Ax = B$ (уравнение Коши) в S_n имеет решение \Leftrightarrow циклический тип A = циклическому типу B .

Свойства

- Умножение подстановок ассоциативно
- Произведение любой подстановки на тождественную, причем слева или справа, даёт саму же эту подстановку
- Обратная перестановка для исходной выглядит "перевернутой":

$$S^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix},$$

- Подстановка S будет чётной, если общее число инверсий в двух строках любой её записи чётно, а нечётной - в противоположном случае.
- Множество A_n состоящее из всех четных перестановок степени n является подгруппой группы S_n .

$$A_n = \{\pi \in S_n | \delta(\pi) = 0\}$$

A_n - нормальная подгруппа в S_n .

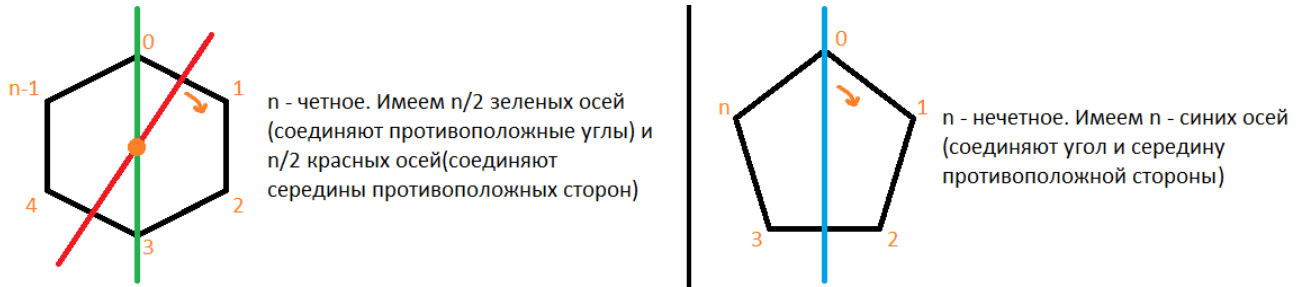
Группа диэдра D_n

Определения

Правильный n -угольник имеет $2n$ различных симметрий: n поворотов (обозначенных как r) и n осевых отражений (обозначенных как s).

$$D_n = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$$

Если n нечётно, каждая ось симметрии проходит через середину одной из сторон и противоположную вершину. Если n чётно, имеется $n/2$ осей симметрии, соединяющих середины противоположных сторон, и $n/2$ осей, соединяющих противоположные вершины.



Свойства

- $|D_n| = 2n$
- $D_n < S_n, n > 2$

Пример

$D_3 = S_3$. $|D_3| = 6$.

Таблица Кэли:

	R_0	R_1	R_2	S_0	S_1	S_2
R_0	R_0	R_1	R_2	S_0	S_1	S_2
R_1	R_1	R_2	R_0	S_1	S_2	S_0
R_2	R_2	R_0	R_1	S_2	S_0	S_1
S_0	S_0	S_2	S_1	R_0	R_2	R_1
S_1	S_1	S_0	S_2	R_1	R_0	R_2
S_2	S_2	S_1	S_0	R_2	R_1	R_0

Наглядное представление происходящего:



Из красного получаем зеленый треугольник - это первое отражение. После получаем снова красный через повторное отражение. Получился поворот на 120 градусов: $S_2S_1 = R_1$

Группа кватернионов Q_8

Определения

Группой кватернионов называется множество $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ с операцией умножения, заданной следующим образом: $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$ («по кругу»).

Свойства

1. Все подгруппы - нормальны, несмотря на то, что сама она не абелева
2. $|Q| = 8$

Кольца

Определение

Кольцо $(R, +, *)$ - множество с определенными операциями "сложения" и "умножения". Причем должны выполняться следующие условия:

1. $(R, +)$ - абелева группа
2. $(R, *)$ - полугруппа
3. Дистрибутивность операций слева и справа:
 $\forall a, b, c \in R$
 $(a + b) * c = (a * c) + (b * c)$ - справа
 $c * (a + b) = (c * a) + (c * b)$ - слева

Свойства

- Если по умножение коммутативно, то R - коммутативное кольцо
- Если по умножению есть нейтральный, то R - кольцо с единицей
- Непустое подмножество S в кольце R является подкольцом тогда и только тогда, когда $a, b \in S \Rightarrow a - b \in S, ab \in S$.
- Идеалом слева (идеалом справа аналогично) называется подкольцо I замкнутое относительно умножения на элементы из R слева:

$$\forall i \in I, \forall r \in R \Rightarrow ri \in I$$

Двусторонний идеал или просто идеал - если оба идеала слева и справа совпадают. Роль у идеалов такая же как и нормальных групп в группах

- Факторкольцом кольца R по его идеалу I называется множество смежных классов $\{r + I | r \in R\}$ аддитивной группы кольца R по идеалу I с операциями:

$$(r + I) + (s + I) = (r + s) + I \text{ и } (r + I)(s + I) = rs + I$$

- Кольцом вычетов по модулю m называется фактор кольцо кольца целых чисел по главному идеалу, порожденному элементом m . Пример: стрелки часов - $Z/12Z$, дни недели $Z/7Z$, дни в году $Z/365Z$ и т.п
- Для коммутативного кольца с единицей R кольцо $R[x]$, состоящее из формальных сумм

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n, a_0, \dots, a_n \in R, n \geq 0,$$

сложение задано правилом

$$\sum_{i=0}^n (a_i x^i) + \sum_{i=0}^n (b_i x^i) = \sum_{i=0}^n ((a_i + b_i) x^i),$$

а умножение - правилом

$$\sum_{i=0}^n (a_i x^i) * \sum_{j=0}^m (b_j x^j) = \sum_{k=0}^{n+m} \sum_{l=0}^k (a_l b_{k-l} x^k)$$

обозначается через $R[x]$ и называется кольцом многочленов над R от одной переменной x , а его элементы - многочленами (или полиномами).

- Характеристикой кольца R ($\text{char } R$) называется такое минимальное $n \in N$, что для $\forall r \in R$ выполняется условие:

$$n * r = \underbrace{r + r + \dots + r}_n = 0,$$

Если же такого числа не существует, то $\text{char } R = 0$

- $M_{m*n} = \{A_{m*n} = (a_{ij}) | a_{ij} \in R, i \in (1, m), j \in (1, n)\}$. Итого $(M_{m*n}(R), +, *)$ - кольцо матриц.
- Полем $(F, +, *)$ называется множество со следующими условиями:
 1. $(F, +)$ - абелева группа
 2. $(F, *)$ - коммутативный моноид с $F^* = F \setminus \{0\}$
(Для каждого ненулевого элемента есть обратный).
 3. Выполнения дистрибутивности слева и справа

Примеры

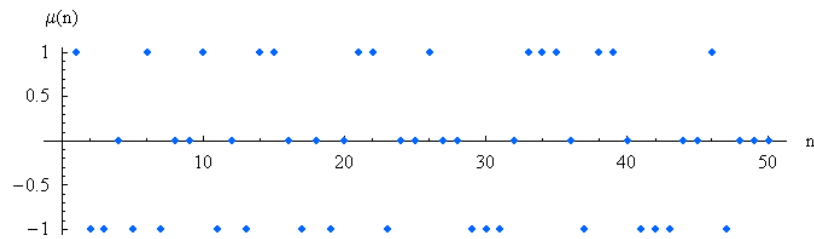
- $(R, +, *)$, $(C, +, *)$ - Поля
- $(2Z, +, *)$ - коммутативное кольцо
- $(Z, +, *)$ - кольцо с единицей

Функция Мёбиуса

Определение

Функция Мёбиуса - функция, заданная на множестве натуральных чисел по следующему правилу:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n - \text{произведение } k \text{ различных простых чисел} \\ 0, & n \text{ делится на квадрат некоторого простого числа} \end{cases}$$



Свойства

$$\mu(mn) = \mu(m)\mu(n)$$

Примеры

1. $\mu(33) = \mu(3 * 11) = (-1)^2 = 1$
2. $\mu(105) = \mu(3 * 5 * 7) = (-1)^3 = -1$
3. $\mu(20) = \mu(2^5 * 5) = 0$

Функция Эйлера

Определение

Функция Эйлера $\phi(n)$ указывает число целых чисел $1 \leq k \leq n$, взаимно простых с n .

Свойства

1. $\phi(mn) = \phi(m)\phi(n)$; $\forall m, n \in \mathbb{N}$: $\text{НОД}(m, n) = 1$
2. $a^{\phi(n)} \equiv 1 \pmod{n}$ – теорема Эйлера

Примеры

1. Если n - простое:

$$\begin{aligned}\phi(n) &= n - 1 \\ \phi(11) &= 11 - 1 = 10\end{aligned}$$

2. Если n - простое, $\alpha \in \mathbb{N}$:

$$\begin{aligned}\phi(n^\alpha) &= n^\alpha - n^{\alpha-1} \\ \phi(9) &= 3^2 - 3^1 = 6\end{aligned}$$

3. Если $d = m \cdot n$ - составное, m и n - взаимно простые:

$$\begin{aligned}\phi(d) &= \phi(m)\phi(n) \\ \phi(24) &= \phi(2^3)\phi(3) = (2^3 - 2^2)(3 - 1) = 9\end{aligned}$$

Приложение

1. Связь с функцией Мёбиуса:

$$\phi(n) = \sum_{d|n} n * \mu\left(\frac{n}{d}\right)$$

2. Используется в алгоритме RSA – для вычисления пары секретного и открытого ключей.

Матрицы

Определение

Матрица A размера $m \times n$ — это прямоугольная таблица элементов, расположенных в m строках и n столбцах. В качестве элементов можно брать как множества чисел (Натуральных, комплексных действительных и т.д), так и кольца и поля.

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

Где $a_{ij} (i = 1, \dots, m; j = 1, \dots, n)$ - элементы матрицы A . Первый индекс i - номер строки, второй индекс j - номер столбца, на пересечении которых расположен элемент a_{ij} . Сокращённое обозначение матрицы $A = (a_{ij})_{m \times n}$.

Свойства

- Два отличных от нуля вектора, которые находятся на одной прямой или параллельных прямых, называются коллинеарными векторами.
- Базис векторного пространства – это упорядоченная совокупность линейно независимых (неколлинеарных) векторов этого пространства, число которых равно размерности пространства.
- Отображение $\phi: V \rightarrow V$ называется линейным оператором, если выполнены следующие свойства:
 1. $\phi(x + y) = \phi(x) + \phi(y)$, т.е. образ суммы двух векторов совпадает с суммой образов этих векторов.
 2. $\phi(\lambda x) = \lambda \phi(x)$ – образ вектора, умноженного на число, совпадает с произведением образа этого вектора на то же число. Отсюда вытекает, что если ϕ – линейный оператор в V , то $\phi(a_1x + a_2y) = a_1\phi(x) + a_2\phi(y)$,
- Элементарными преобразованиями строк матрицы называются следующие преобразования:
 1. Умножение строки на отличное от нуля число,
 2. Прибавление одной строки к другой строке,
 3. Перестановка местами двух строк.

Элементарные преобразования столбцов матрицы определяются аналогично.

- Суммой (разностью) двух матриц $A = (a_{ij})_{m \times n}$ и $B = (b_{ij})_{m \times n}$ одинаковых размеров называется матрица $C = (c_{ij})_{m \times n} = A + B$ тех же размеров, элементы которой определяются равенствами $c_{ij} = a_{ij} + b_{ij}$:
- Умножение матрицы A на матрицу B производится по принципу "строка на столбец" при условии равенства количеств строк в матрице A со столбцами матрицы B .
- Детерминант характеризует ориентированное «растяжение» или «сжатие» многомерного евклидова пространства. Можно применять только к квадратным матрицам. Получить можно его по следующим правилам:

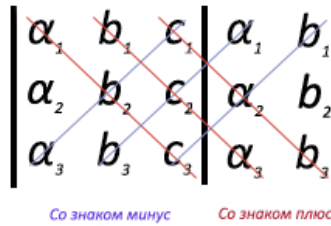
– Для матрицы 2×2 :

$$A = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc$$

– Для матрицы 3×3 :

$$A = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 * b_2 * c_3 + a_3 * b_1 * c_2 + a_2 * b_3 * c_1 - a_3 * b_2 * c_1 - a_1 * b_3 * c_2 - a_2 * b_1 * c_3$$

С какими знаками брать можно запомнить по следующему шаблону:



Также есть альтернативный способ через миноры (определитель некоторой меньшей квадратной матрицы):

1. Знаки находим по следующему алгоритму (подходит для произвольного размера матрицы):

$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

2. Алгоритм:

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

Есть особенность детерминанта, которая связывает его с отображениями: если $\det A = 0$, то нельзя построить изоморфное отображение $f: A \rightarrow xA$, где x - вектор, A - матрица.

- Транспонировать матрицу значит записать ее строки в столбцы, сохраняя порядок
- Обратная матрица находится по следующей формуле:

$$A^{-1} = \frac{1}{|A|} * A_*^T$$

Так как для её нахождения требуется поиск детерминанта, то обратная существует только для квадратных матриц.

Примеры

1. Сумма (разность):

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, B = \begin{pmatrix} 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix}$$

$$C = A + B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 7 & 7 \\ 7 & 7 & 7 \end{pmatrix}$$

2. Умножение:

$$P = \begin{pmatrix} 5 & 8 & -4 \\ 6 & 9 & -5 \\ 4 & 7 & -3 \end{pmatrix}, R = \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}$$

$$PR = \begin{pmatrix} 5 & 8 & -4 \\ 6 & 9 & -5 \\ 4 & 7 & -3 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \cdot 2 + 8 \cdot (-3) - 4 \cdot 1 \\ 6 \cdot 2 + 9 \cdot (-3) - 5 \cdot 1 \\ 4 \cdot 2 + 7 \cdot (-3) - 3 \cdot 1 \end{pmatrix} = \begin{pmatrix} -18 \\ -20 \\ -16 \end{pmatrix}$$

3. Детерминант

- Для матриц 2x2:

$$\begin{vmatrix} 11 & -3 \\ -15 & -2 \end{vmatrix} = 11 \cdot (-2) - (-15) \cdot (-3) = -22 - 45 = -67$$

- Для матриц 3x3:

$$\begin{vmatrix} 1 & -2 & 3 \\ 4 & 0 & 6 \\ -7 & 8 & 9 \end{vmatrix} = 1*0*9 + (-2)*6*(-7) + 3*4*8 - 3*0*(-7) - 1*6*8 - (-2)*4*9 = 0 + 84 + 96 - 0 - 48 + 72 = 204$$

4. Транспонирование

$$A = \begin{pmatrix} -1 & 0 & -2 \\ -5 & 4 & -7 \\ 6 & -4 & -6 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & * & * \\ 0 & * & * \\ -2 & * & * \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & -5 & * \\ 0 & 4 & * \\ -2 & -7 & * \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & -5 & -2 \\ 0 & 4 & -7 \\ -2 & -7 & -6 \end{pmatrix}$$

5. Обратная матрица. Найдем ее для:

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

- (a) Найдем определитель:

$$|A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1*4 - 3*2 = 4 - 6 = -2$$

Так как определитель не равен нулю, то можно идти дальше по алгоритму

- (b) Найдем матрицу миноров:

•

$$M = \begin{pmatrix} * & * \\ * & * \end{pmatrix}, A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

- Чтобы найти минор мысленно вычеркиваем строку и столбец, в котором находится первый (α_{11}) элемент:

$$M = \begin{pmatrix} 4 & * \\ * & * \end{pmatrix}, A = \begin{pmatrix} \underline{1} & \underline{2} \\ \underline{3} & \underline{4} \end{pmatrix}$$

- То же самое для второго, третьего и четвертого элементов:

$$M = \begin{pmatrix} 4 & 3 \\ * & * \end{pmatrix}, A = \begin{pmatrix} \underline{1} & \underline{2} \\ 3 & \underline{4} \end{pmatrix} \rightarrow M = \begin{pmatrix} 4 & 3 \\ 2 & * \end{pmatrix}, A = \begin{pmatrix} \underline{1} & \underline{2} \\ \underline{3} & \underline{4} \end{pmatrix} \rightarrow M = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}, A = \begin{pmatrix} \underline{1} & \underline{2} \\ \underline{3} & \underline{4} \end{pmatrix}$$

- (c) Найдем матрицу алгебраических дополнений. Делается это через этот объект, который в шахматном порядке задает знаки для произвольной матрицы:

$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

Там где в нашем объекте стоит минус меняем знак у минора, т.е

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

- (d) Найдем транспонированную матрицу алгебраических дополнений:

$$A_*^T = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$

- (e) Воспользуемся формулой:

$$A^{-1} = \frac{1}{|A|} * A_*^T$$

Таким образом получаем:

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

Приложение

- Квадратная матрица — это матрица у которой число строк равно числу столбцов
- Матрица-столбец (вектор-столбец) — это матрица, у которой всего один столбец. Аналогично и с матрицей строкой (вектор-строкой):

$$A = \begin{pmatrix} a_{11} \\ a_{12} \\ \dots \\ a_{1n} \end{pmatrix}, A = (a_{11} \quad a_{12} \quad \dots \quad a_{1n})$$

- Единичная матрица — это диагональная матрица, у которой все диагональные элементы равны единице:

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Отображения

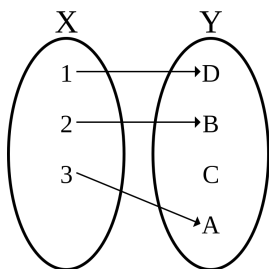
Определение

Функция, по которой каждому элементу первого множества соответствует один и только один элемент второго множества

Свойства

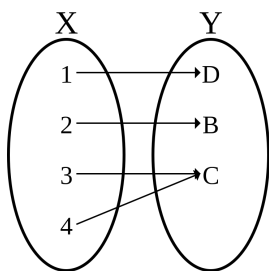
- Инъекция:

$$\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

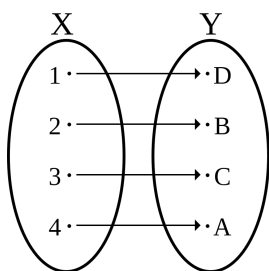


- Сюръекция:

$$\forall b \in B \exists a \in A : f(a) = b$$



- Биекция - функция, одновременно сюръективная и инъективная.



Примеры

- $f : R \rightarrow [-1; 1], f(x) = \sin(x)$ - пример сюръекции
 $f : R \rightarrow R, f(x) = x^2$ не является сюръективным, так как не существует x такого, что $f(x) = -9$
- $f : R_{>0} \rightarrow R, f(x) = x^2$ - инъективно
 $f : R \rightarrow R_{>0}, f(x) = x^2$ - не инъективно, так как $f(2) = f(-2) = 4$
- $f : R \rightarrow R, f(x) = x^3$ - биекция
 $f : R \rightarrow R, f(x) = \sin(x)$ - не биекция

Гомоморфизм

Определение

Отображение $f : G \rightarrow H$ группы $G=G(*)$ в группу $H=H(\cdot)$, $a, b \in G$ имеет место равенство

$$f(a*b) = f(a) \cdot f(b)$$

Свойства

- Если f является отображением на H , то оно называется **эпиморфизмом**. При этом H называется **гомоморфным образом** группы G . Другими словами если f - сюръективное, то это эпиморфизм
- Гомоморфизм группы G в себя называется **эндоморфизмом** этой группы.
- Если f - взаимно-однозначный гомоморфизм группы G на группу H , то он называется **изоморфизмом**, при этом группы G и H называют **изоморфными**. Другими словами, если f - сюръективное и инъективное - это изоморфизм
- Изоморфизм группы G на G называется **автоморфизмом** группы G .
- Ядром гомоморфизма $f : G \rightarrow H$ группы G в группу H называется множество

$$\text{Ker } f = \{a \in G | f(a) = e_h\},$$

здесь e_h - нейтральный элемент группы H .