Алгебра

материал по лекциям Александра Владимировича Анашкина

March 2023

Содержание

Группы

Определение

- **Группоидом** - множество с операцией: (G, *)
  *: G x G $\to G$
- **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, то есть для любого элемента справедливо:

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

Свойства

- Группа называется абелевой, если на ней выполняется коммутативность операции
- Для каждого элемента a обратный элемент a^{-1} единственен
- Нейтральный элемент единственен
- Теорема Лагранжа: если G — группа **конечного** порядка n, то порядок n_1 любой её подгруппы G_1 является делителем порядка группы. Из этого следует, что и порядок любого элемента делит порядок группы.
- Порядок/мощность группы G - число элементов в этой группе. Обозначается как |G|
- Порядок элемента - минимальная степень в которую нужно возвести элемент, чтобы получить нейтральный:

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

  В противном случае ord g = ∞
- Группа называется циклической, если она порожденна одним элементом и обозначается <g> = $\{g, g^1, g^2, ..., g^n\}$. 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, α, β, γ}

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

  ord α = ord β = ord $\gamma = 2$
- Экспонента в конечной группы равна НОК'у порядков всех элементов группы, обозначается exp(G)

Кольца

Определение

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

1. (R, +) - абелевева группа
2. (R, *) - полугруппа
3. Дистрибутивность опреций 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
- Полем (F, +, *) называется множество со следующими условиями:
  1. (F, +) - абелева группа
  2. (F, *) - коммутативный моноид с $F^* = F \backslash \{0\}$
     (Для каждого ненулевого элемента есть обратный).
  3. Выполнения дистрибутивности слева и справа

Примеры

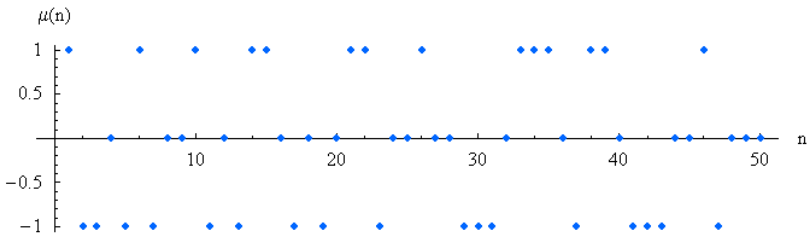
- (R, +, *), (C, +, *) - Поля
- (2Z, +, *) - коммутативное кольцо
- (Z, +, *) - кольцо с единицей

Функция Мёбиуса

Определение

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

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



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

Примеры

1. Если n - простое:

$$\phi(n) = n - 1$$
$$\phi(11) = 11 - 1 = 10$$

2. Если n - простое, $\alpha \in$ N:

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

3. Если d = m*n - составное, m и n - взаимно простые:

$$\phi(d) = \phi(m)\phi(n)$$
$$\phi(24) = \phi(2^3)\phi(3) = (2^3 - 2^2)(3 - 1) = 9$$

Приложение

1. Связь с функцие Мёбиуса:

$$\phi(n) = \sum_{n|d} n * \mu(\tfrac{d}{n})$$

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

Матрицы

Определение

Матрица A размера m×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.

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

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

Свойства

- 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=$(a_{ij})_{m*n}$ и $B = (b_{ij})_{m*n}$ одинаковых размеров называется матрица $C = (c_{ij})_{m*n} = A + B$ тех же размеров, элементы которой определяются равенствами $c_ij = a_ij + b_ij$:

- Умножение матрицы A на матрицу B производиться по принципу "строка на столбец при условии равенства количеств строк в матрице A со столбцами матрицы B.

- Детермint характеризует ориентированное «растяжение» или «сжатие» многомерного евклидова пространства. Можно применять только к квадратным матрицам. Получить можно его по следующим правилам:

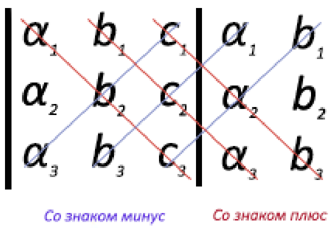
  – Для матрицы 2x2:

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

  – Для матрицы 3x3:

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

  С какими знаками брать можно запомнить по следующему шаблону:

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

1. Знаки находим по слудующему алгоритму (подходит для произвольнго размера матрицы):

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

2. Алгоритм:

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

- Транспонировать матрицу значит записать ее строки в столбцы, сохрания 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:

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

   - 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

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

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:
$$M = \begin{pmatrix} 4 & * \\ * & * \end{pmatrix}, A = \begin{pmatrix} \underline{1} & \underline{2} \\ \underline{3} & 4 \end{pmatrix}$$
- Тоже самое для второго, третьего и четвертого элементов:

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

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

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

Там где в нашем объекте стоит минус меням 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:

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

Таким образом плучаем:

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

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):
$$A = \begin{pmatrix} a_{11} \\ a_{12} \\ ... \\ a_{1n} \end{pmatrix}, A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \end{pmatrix}$$
- Единичная матрица — это диагональная матрица, у которой все диагональные элементы равны единице:
$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

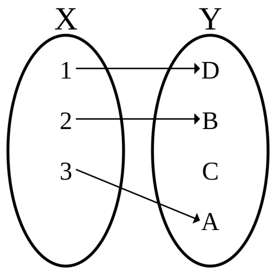
Отображение

Определение

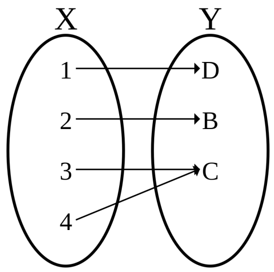
Функция по которой каждому элементу первого множества, соответствует один и только один элемент второго множества

Свойства

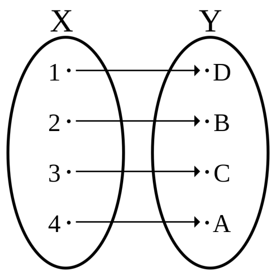
- Иньекция:
  $\forall x_1, x_2 \in X : x_1 \neq x_2 => f(x_1) \neq f(x_2)$



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



- Биекция - функция, одновременно сюръективная и инъективная.



Примеры

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

Гомоморфизм

Определение

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

$$f(\text{a*b}) = f(\text{a})\cdot f(\text{b})$$

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 иньективное - это изоморфизм
- Изоморфизм группы G на G называется **автоморфизмом** группы G.
- Ядром гомоморфизма $f : G \to H$ группы G в группу H называется множество

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

  здесь e_h – нейтральный элемент группы H.