

Белорусский государственный университет

Прикладная информатика

Минск, Беларусь

Алгебра и теория чисел

Дилер: Матвеев Геннадий Васильевич

Автор: @senkevich_s

Аннотация:

Данный электронный конспект содержит материал лекций Матвеева Г.В по предмету «Алгебра и теория чисел», информация разбита в соответствии с экзаменационными вопросами по данному предмету.

Содержание

1	Операции над комплексными числами	3
2	Геометрическая интерпретация комплексных чисел	4
3	Умножение комплексных чисел, формула Муавра, извлечение корня	5
4	Определение, примеры и простейшие свойства групп	5
5	Определение, примеры и простейшие свойства колец и полей	7
6	Арифметические операции над многочленами	8
7	Делимость многочленов	10
8	НОД. Алгоритм Евклида	11
9	Взаимно простые многочлены	12
10	Корни многочлена	13
11	Основная теорема алгебры и ее следствия	14
12	Интерполяционная формула Лагранжа	15
13	Многочлены с вещественными коэффициентами	15
14	Линейные операции над матрицами	16
15	Умножение матриц	18
16	Перестановки	19
17	Определитель и его свойства	20
18	Теорема Лапласа	22
19	Определитель произведения двух матриц	23
20	Обратная матрица	23
21	Правило Крамера	25
22	Метод Гаусса решения системы линейных уравнений	26
23	Определение и простейшие свойства векторных пространств	27
24	Линейная зависимость векторов	28
25	Основная теорема о линейной зависимости	29
26	Базис и размерность векторного пространства	29
27	Ранг матрицы	30
28	Вычисление ранга матрицы с помощью элементарных преобразований	32
29	Подпространства векторного пространства	33
30	Критерий совместности систем линейных уравнений	34

31 Однородные системы линейных уравнений	35
32 Линейные преобразования векторного пространства	37
33 Ядро и образ линейного преобразования	38
34 Матрица линейного преобразования	39
35 Подобные матрицы	40
36 Характеристическая матрица и характеристический многочлен	41
37 Собственные векторы и собственные значения линейного преобразования	42
38 Основные свойства делимости в кольце целых чисел	43
39 Основные свойства сравнений	45
40 Классы вычетов	46
41 Функция Эйлера, RSA-криптосистема	47
42 Сравнения и системы сравнений первой степени	48
43 Первообразные корни	49
44 Показатели и их свойства	50
45 Приведение квадратичной формы к каноническому ряду	51
46 Квадратичные вычеты и криптосистема Рабина	53
47 Индексирование и протокол Диффи-Хеллмана	54
48 Процесс ортогонализации	55
49 Факторизация RSA-модуля с известной секретной экспонентой	57
50 Сумма и пересечение подпространств	59

1 Операции над комплексными числами

Def. (Действительная и мнимая часть комплексного числа)

Действительные числа a и b комплексного числа $z = a + b \cdot i$ называются **действительной и мнимой частью числа z** соответственно. Обозначаются $Re(z) = a$, $Im(z) = b$.

Операции над комплексными числами

1. Сложение комплексных чисел

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$$

2. Умножение комплексных чисел

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i$$

3. Умножение комплексного числа на действительное

$$\lambda(a + bi) = \lambda a + \lambda bi$$

4. Деление комплексных чисел

$$\frac{(a_1 + b_1 i)}{(a_2 + b_2 i)} = \frac{(a_1 + b_1 i)(a_2 - b_2 i)}{(a_2 + b_2 i)(a_2 - b_2 i)} = \frac{a_1 a_2 + b_1 b_2 + (a_1 b_2 - a_2 b_1) i}{a_2^2 + b_2^2} = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{a_1 b_2 - a_2 b_1}{a_2^2 + b_2^2} i$$

Свойства операций над комплексными числами

1. Коммутативность сложения

$$z_1 + z_2 = z_2 + z_1$$

2. Ассоциативность сложения

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

3. Коммутативность умножения

$$z_1 z_2 = z_2 z_1$$

4. Ассоциативность умножения

$$z_1(z_2 z_3) = (z_1 z_2) z_3$$

5. Дистрибутивность

$$z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$$

6. $z + 0 = z$, $\forall z \in \mathbb{C}$

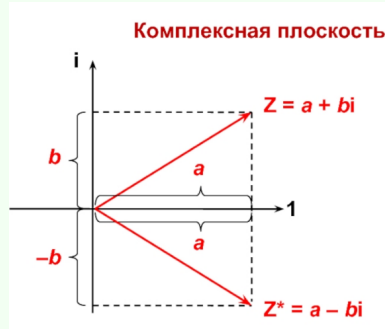
7. $\forall z \exists (-z) \mid z + (-z) = 0$

2 Геометрическая интерпретация комплексных чисел

Интерпретация

Так как комплексное число однозначно задается парой действительных чисел, то естественной геометрической интерпретацией является изображение комплексного числа $z = a + bi$ точкой плоскости с декартовыми координатами (a, b) . Число $z = 0$ является началом координат данной плоскости.

Плоскость, точки которой отождествляют с комплексными числами, называется *комплексной плоскостью*, ось абсцисс - *действительной осью*, ось ординат - *мнимой осью*.



Def. (Модуль комплексного числа)

Модулем комплексного числа $z = a + bi$ называется длина радиус-вектора, изображающего комплексное число z .

$$|z| = \sqrt{a^2 + b^2} \Rightarrow |z| \geq 0$$

Def. (Сопряженные числа)

Парой комплексно сопряженных чисел называются такие комплексные числа z и \bar{z} , что $z = a + bi$, $\bar{z} = a - bi$.

Свойства сопряженных чисел

$$1. |z| = |\bar{z}|$$

Доказательство:

$$|z| = \sqrt{a^2 + b^2} = \sqrt{a^2 + (-b)^2} = |\bar{z}|.$$

$$2. \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$$

Доказательство:

$$\overline{z_1 + z_2} = \overline{(a_1 + a_2) - (b_1 + b_2)i} = (a_1 + a_2) - (b_1 + b_2)i = (a_1 - b_1i) + (a_2 - b_2i) = \bar{z}_1 + \bar{z}_2.$$

$$3. \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$$

Доказательство:

$$\overline{z_1 \cdot z_2} = \overline{(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i} = (a_1a_2 - b_1b_2) - (a_1b_2 + a_2b_1)i$$

$$\bar{z}_1 \cdot \bar{z}_2 = (a_1 - b_1i)(a_2 - b_2i) = (a_1a_2 - b_1b_2) - (a_1b_2 + a_2b_1)i.$$

$$4. \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$$

Доказательство:

$$\overline{\left(\frac{z_1}{z_2}\right)} = \overline{\frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2} + \frac{a_1b_2 - a_2b_1}{a_2^2 + b_2^2}i} = \frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2} - \frac{a_1b_2 - a_2b_1}{a_2^2 + b_2^2}i$$

$$\frac{\bar{z}_1}{\bar{z}_2} = \frac{a_1 - b_1i}{a_2 - b_2i} = \frac{a_1a_2 + (-b_1)(-b_2)}{a_2^2 + (-b_2)^2} + \frac{a_1(-b_2) - a_2(-b_1)}{a_2^2 + (-b_2)^2}i = \frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2} - \frac{a_1b_2 - a_2b_1}{a_2^2 + b_2^2}i$$

$$5. z \cdot \bar{z} = |z|^2$$

3 Умножение комплексных чисел, формула Муавра, извлечение корня

Def. (Тригонометрическая форма комплексного числа)

Тригонометрической формой записи комплексного числа называется представление в виде $z = r(\cos\varphi + i\sin\varphi)$.

r - модуль комплексного числа, $r = |z|$.

φ - аргумент комплексного числа, $\varphi = \arg z$.

Умножение комплексных чисел в тригонометрической форме

$$z_1 z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$$

Свойства:

1. $|z_1 z_2| = |z_1| \cdot |z_2|$
2. $\arg(z_1 z_2) = \arg z_1 + \arg z_2$

Th. (Формула Муавра)

$$z^n = r^n (\cos(n\varphi) + i\sin(n\varphi)) \quad \forall n \in \mathbb{Z}.$$

Доказательство:

Докажем данную теорему для $n \in \mathbb{N}$, используя метод математической индукции.

База: $n = 1$. $z = r(\cos\varphi + i\sin\varphi)$ - верно.

Шаг: Пусть $z^n = r^n (\cos(n\varphi) + i\sin(n\varphi))$, тогда докажем, что $z^{n+1} = r^{n+1} (\cos((n+1)\varphi) + i\sin((n+1)\varphi))$.

$$z^{n+1} = z^n \cdot z = r^n (\cos(n\varphi) + i\sin(n\varphi)) \cdot r (\cos\varphi + i\sin\varphi) = r^{n+1} (\cos((n+1)\varphi) + i\sin((n+1)\varphi)).$$

При $n = 0$: $z^0 = r^0 (\cos(0) + i\sin(0)) = 1$.

$$\text{При } -n \text{ имеем: } z^{-n} = \frac{1}{z^n} = \frac{1}{r^n (\cos(n\varphi) + i\sin(n\varphi))} = r^{-n} \frac{1}{(\cos(n\varphi) + i\sin(n\varphi))} = r^{-n} \frac{(\cos(n\varphi) - i\sin(n\varphi))}{(\cos(n\varphi) + i\sin(n\varphi))(\cos(n\varphi) - i\sin(n\varphi))} = r^{-n} \frac{(\cos(n\varphi) - i\sin(n\varphi))}{1} = r^{-n} (\cos(-n\varphi) + i\sin(-n\varphi)). \blacksquare$$

Извлечение корня

$$\sqrt[n]{z} = \{ \sqrt[n]{r} (\cos \frac{\varphi + 2\pi k}{n} + i\sin \frac{\varphi + 2\pi k}{n}) \}, \quad k = \overline{0, n-1}.$$

4 Определение, примеры и простейшие свойства групп

Def. (Группа)

Группа - непустое множество G , на котором задана алгебраическая операция $*$, удовлетворяющая свойствам:

1. $a, b \in G \Rightarrow a * b \in G$
2. Операция $*$ ассоциативна.
 $\forall a, b, c \in G \quad (a * b) * c = a * (b * c)$
3. В множестве существует нейтральный элемент.
 $\exists n \mid \forall a \quad a * n = n * a = a$
4. Для каждого элемента существует симметричный ему элемент.
 $\forall a \quad \exists a^{-1} \mid a * a^{-1} = n$

Def. (Алгебраическая операция)

Отображение $f : X^2 \rightarrow X$ называется алгебраической операцией на множестве X .

Th. (Единственность нейтрального и симметричного элементов)

В группе имеется лишь 1 нейтральный элемент и для каждого элемента существует ровно 1 симметричный.

Доказательство:

1. Допустим противное: пусть существует два различных нейтральных элемента n и m . Применим к ним операцию $*$: $m = n * m = n \Rightarrow$ противоречие.
2. Допустим, что для x существует два различных симметричных элемента x_1 и x_2 . Рассмотрим композицию $x_1 * x * x_2 = (x_1 * x) * x_2 = n * x_2 = x_2$. С другой стороны $x_1 * x * x_2 = x_1 * (x * x_2) = x_1 * n = x_1$. То есть $x_1 = x_2$ - противоречие. ■

Примеры

1. $\mathbb{Z}(+)$ - группа.
2. $\mathbb{Z}(-)$ - не группа, т.к. операция « $-$ » не ассоциативна.
3. $\mathbb{Z}(*)$ - не группа, т.к нет симметрии.
4. $\mathbb{R}(+)$ - группа.
5. $\mathbb{R}(*)$ - не группа, т.к нет обратного элемента для 0.
6. $\mathbb{R} \setminus \{0\}(*)$ - группа.

Свойства группы

1. Только один нейтральный элемент
2. Для каждого элемента существует обратный ему.
3. $(a^{-1})^{-1} = a$
4. $(ab)^{-1} = b^{-1}a^{-1}$
5. $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$

Th. (Правило обращения композиций)

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

$$\text{Проверка: } (a * b) * (b^{-1}a^{-1}) = a * b * b^{-1}a^{-1} = a * e * a^{-1} = e.$$

Def. (Подгруппа)

Подмножество H группы G называется подгруппой, если оно само является группой относительно имеющихся операций.

Def. (Абелева группа)

Абелева группа - группа, в которой алгебраическая операция обладает свойством коммутативности.

5 Определение, примеры и простейшие свойства колец и полей

Def. (Кольцо)

Непустое множество K называется кольцом, если выполнены условия:

1. На множестве K задана алгебраическая операция *сложение* $(+)$
2. Множество K относительно « $+$ » является *абелевой группой*.
3. На множестве K задана алгебраическая операция *умножение* $(*)$
4. Сложение и умножение связаны свойством дистрибутивности, т.е.
 $a(b + c) = ab + bc$; $(a + b)c = ac + bc$. $\forall a, b, c \in K$.

Если операция умножения в кольце K является коммутативной, то кольцо K называется **коммутативным**, если операция умножения является ассоциативной - **ассоциативное кольцо**, если есть нейтральный элемент относительно операции умножения - **кольцо с единицей**.

Def. (Делители нуля и область целостности)

Два элемента кольца $a, b \in K$ | $a, b \neq 0, ab = 0$, называются делителями нуля.

Областью целостности называется коммутативное кольцо с единицей и без делителей нуля.

Примеры

1. $\mathbb{Z}(+, *)$ - коммутативное ассоциативное кольцо с единицей, область целостности.
2. $2\mathbb{Z}(+, *)$ - коммутативное ассоциативное кольцо без единицы.

В кольце также можно ввести операцию вычитания « $-$ »: $a - b = a + (-b)$.

Свойства кольца

1. $a * 0 = 0$

Доказательство:

$$a * 0 = a * (0 + 0) = a * 0 + a * 0 = 2 * (a * 0) \Rightarrow a * 0 = 0.$$

2. $a(b - c) = ab - ac$

Доказательство:

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac.$$

3. $-1 * a = -a$

Доказательство:

$$a + (-1) * a = a * (1 + (-1)) = a * 0 = 0 \Rightarrow -1 * a = -a.$$

Def. (Поле)

Множество P ($|P| \geq 2$) называется полем, если выполнены условия:

1. На множестве P задана алгебраическая операция *сложение* $(+)$
2. Множество P относительно « $+$ » является *абелевой группой*.
3. На множестве P задана алгебраическая операция *умножение* $(*)$
4. Множество $P' = P \setminus \{0\}$ относительно операции $*$ является абелевой группой.
5. Сложение и умножение связаны свойством дистрибутивности, то есть
 $a(b + c) = ab + bc$; $(a + b)c = ac + bc$. $\forall a, b, c \in K$.

Свойства поля

1. Исходя из определения, любое поле является также и кольцом, относительно заданных операций, поэтому поле обладает свойствами кольца.
2. В поле нет делителей нуля.

Доказательство:

Предположим противное: пусть $ab = 0$; $a, b \neq 0$.

Тогда рассмотрим обратный элемент a^{-1} .

$$a^{-1}(ab) = a^{-1}0 = 0.$$

С другой стороны имеем: $a^{-1}(ab) = (a^{-1}a)b = 1 * b = b$.

Получаем $b = 0$ - противоречие. ■

6 Арифметические операции над многочленами

Def. (Многочлен)

Функция $f : P \rightarrow P$ называется многочленом над полем P , если ее значения вычисляются по формуле $f(x) = \sum_{k=0}^n a_k x^k \forall x \in P, n \in \mathbb{N}_0, a_k \in P$.

a_k - **коэффициенты** многочлена.

x - **переменная**.

Два многочлена равны тогда и только тогда, когда равны их значения при любых значениях переменной.

Многочлен, принимающий только нулевые значения, называется **нулевым многочленом**, обозначается $0(x)$.

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n = 0$$

Def. (Степень многочлена)

Степенью многочлена $\deg f(x) = n$ называется наивысшая степень x , при которой коэффициент не равен 0. У нулевого многочлена нет степени.

Сложение многочленов

Пусть есть два многочлена $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$.
 $h(x) = f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n$.

Свойства сложения:

1. Коммутативность

$$f(x) + g(x) = g(x) + f(x)$$

2. Ассоциативность

$$(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$$

3. $\forall f(x) \exists g(x) \mid f(x) + g(x) = 0$.

4. Многочлены образуют абелеву группу по сложению.

Произведение многочленов

Пусть есть два многочлена $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$.
 $h(x) = f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \dots + c_mx^m$, $c_k = \sum_{i+j=k} a_ib_j$.

Свойства произведения:

1. Коммутативность

$$f(x) \cdot g(x) = g(x) \cdot f(x)$$

2. Дистрибутивность

$$f(x) \cdot (g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x)$$

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_ib_j + \sum_{i+j=k} a_ic_j$$

3. Ассоциативность

$$(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$$

$$(a_ix^i \cdot b_jx^j) \cdot c_kx^k = a_ix^i \cdot (b_jx^j \cdot c_kx^k)$$

Th. (Степень произведения многочленов)

Степень произведения двух ненулевых многочленов равна сумме их степеней.

Доказательство:

Пусть $\deg f_1(x) = s_1$, $\deg f_2(x) = s_2$, $h(x) = f_1(x) \cdot f_2(x)$.

Тогда, исходя из определения произведения, $\deg h(x) \leq s_1 + s_2$. Достаточно доказать, что коэффициент $c_{s_1+s_2}$ при $x^{s_1+s_2}$ не равен 0. $c_{s_1+s_2} = \sum_{i+j=s_1+s_2} a_ib_j$.

Также известно, что $i \leq s_1$, $j \leq s_2 \Rightarrow c_{s_1+s_2} = a_{s_1}b_{s_2}$.

Так как $a_{s_1} \neq 0$, $b_{s_2} \neq 0$, получаем $c_{s_1+s_2} \neq 0$. ■

7 Делимость многочленов

Def. (Делимость многочленов)

Ненулевой многочлен $g(x)$ делит многочлен $f(x)$ (обозначается $g(x) \mid f(x)$), если $\exists h(x) : f(x) = g(x) \cdot h(x)$.

Свойства делимости

$$1. g(x) \mid f(x), g(x) \mid h(x) \Rightarrow g(x) \mid (f(x) + h(x))$$

Доказательство:

$$f(x) = g(x) \cdot a(x), h(x) = g(x) \cdot b(x) \Rightarrow f(x) + h(x) = g(x) \cdot (a(x) + b(x))$$

$$2. h(x) \mid f(x) \Rightarrow h(x) \mid f(x) \cdot g(x)$$

Доказательство:

$$f(x) = h(x) \cdot q(x) \Rightarrow f(x) \cdot g(x) = (h(x) \cdot q(x)) \cdot g(x) = h(x) \cdot (q(x) \cdot g(x))$$

$$3. h(x) \mid g(x), g(x) \mid f(x) \Rightarrow h(x) \mid f(x)$$

Доказательство:

$$h(x) = g(x) \cdot q(x) = f(x) \cdot p(x) \cdot q(x) = f(x) \cdot (q(x) \cdot p(x)).$$

$$4. f(x) \mid g(x), g(x) \mid f(x) \Rightarrow f(x) = \alpha \cdot g(x)$$

Доказательство:

$$f(x) = g(x)q_1(x) = f(x)q_1(x)q_2(x) \Rightarrow \deg q_1(x) = 0 \Rightarrow q_1(x) = \alpha$$

Th. (Теорема о делимости с остатком)

$\forall f(x), g(x) > 0 \exists q(x), r(x) : f(x) = g(x) \cdot q(x) + r(x), \deg g(x) > \deg r(x)$ или $r(x) = 0$.

Иными словами, два любых ненулевых многочлена можно поделить друг на друга с остатком, причем однозначно.

Доказательство:

Положим, что $\deg f(x) > \deg g(x)$, если не так, то $f(x) = g(x) \cdot 0 + f(x)$.

Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0$, $g(x) = b_m x^m + \dots + b_1 x + b_0$.

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = f_1(x), \deg f_1(x) < \deg f(x).$$

$$g - \frac{a_{n-1}}{b_{m-1}} x^{n-m-1} f_1 = f_2, \deg f_2(x) < \deg f_1(x).$$

$$f_1 - \frac{a_{n-2}}{b_{m-2}} x^{n-m-2} f_2 = f_3, \deg f_3(x) < \deg f_2(x).$$

...

$$f_k = r(x)$$

Теперь докажем единственность разложения.

Допустим противное, пусть $f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$, тогда $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x) \neq 0$. Однако такое невозможно, так как $q_1(x) - q_2(x) \neq 0$, $\deg g(x) > \deg r_1(x)$ и $\deg g(x) > \deg r_2(x)$ - противоречие. ■

8 НОД. Алгоритм Евклида

Def. (Наибольший общий делитель двух многочленов)

Пусть $f(x)$, $g(x)$ - два многочлена. Наибольшим общим делителем (НОД) двух многочленов $f(x)$, $g(x)$ называется многочлен $d(x)$, удовлетворяющий следующим условиям:

1. $d(x) \mid f(x)$, $d(x) \mid g(x)$
2. $\forall d'(x) (d'(x) \mid f(x), d'(x) \mid g(x) \Rightarrow d'(x) \mid d(x))$.
3. Старший коэффициент многочлена $d(x)$ равен 1.

НОД двух нулевых многочленов не определен.

НОД двух многочленов $f(x)$, $g(x)$ также обозначается как $(f(x), g(x))$.

Вообще говоря, многочлен $d(x)$ определен с точностью до множителя $\alpha \in P$, $\alpha \neq 0$, но г-н Матвеев решил ввести собственное правило, что старший коэффициент равен 1.

Лем. (НОД многочлена и его делителя)

Если $g(x) \mid f(x)$, то $\text{НОД}(g(x), f(x)) = g(x)$.

Доказательство:

Множитель $g(x)$ есть общий делитель $f(x)$ и $g(x)$, а любой общий делитель многочленов $f(x), g(x)$ делит $g(x)$. ■

Th. (Алгоритм Евклида)

Для любых двух многочленов $f(x)$ и $g(x)$ из $P[x]$ существует НОД, принадлежащий $P[x]$.

Доказательство:

Если $g(x) = 0$, то $f(x) \mid 0(x) \Rightarrow f(x)$ является НОДом.

Теперь положим, что $\deg f(x) \geq \deg g(x)$

Алгоритм состоит в следующей последовательности действий:

1. Делим $f(x)$ на $g(x)$ и получаем остаток $r_1(x)$, если $r_1(x) = 0$, заканчиваем алгоритм.
2. Делим $g(x)$ на $r_1(x)$ и получаем остаток $r_2(x)$, если $r_2(x) = 0$, заканчиваем алгоритм.
3. Продолжаем делить предыдущий остаток на новый, до тех пор, пока не получим нулевой остаток. Процесс точно остановится через конечное количество шагов, так как степени остатков все время понижаются.

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x) \\ g(x) &= g(x)q_2(x) + r_2(x) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x) \\ &\dots\dots\dots \\ r_{k-3}(x) &= r_{k-2}(x)q_{k-1}(x) + r_{k-1}(x) \\ r_{k-2}(x) &= r_{k-1}(x)q_k(x) + r_k(x) \\ r_{k-1}(x) &= r_k(x)q_{k+1}(x) \end{aligned}$$

Рассматривая данные равенства сверху вниз заметим, что пары многочленов $(f(x), g(x))$, $(g(x), r_1(x))$, \dots , $(r_{k-1}(x), r_k(x))$ имеют общие делители и $r_k(x)$ делит каждый из данных многочленов, поэтому $r_k(x)$ - НОД исходных многочленов. ■

Th. (Теорема о разложении НОД)

Пусть $d(x)$ - НОД многочленов $f(x)$ и $g(x)$. Тогда $d(x)$ представим в виде:

$$d(x) = f(x)u(x) + g(x)v(x)$$

Доказательство:

Если $g(x) \mid f(x)$, то $d(x) = f(x) \cdot 0 + g(x) \cdot c$.

Теперь положим $\deg f(x) \geq \deg g(x) > 0 \Rightarrow d(x) = r_k(x)$. Из предпоследнего равенства имеем $d(x) = r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_k(x) = r_{k-2}(x)u_1(x) - r_{k-1}(x)v_1(x)$, $u_1(x) = 1, v_1(x) = -q_k(x)$. Далее из равенства выше получим $r_{k-1}(x) = r_{k-3}(x) - r_{k-2}(x)q_{k-1}(x)$. Подставим в ранее полученное равенство для $d(x)$: $d(x) = r_{k-2}(x)u_1(x) + (r_{k-3}(x) - r_{k-2}(x)q_{k-1}(x))v_1(x) = r_{k-3}(x)u_2(x) + r_{k-2}(x)v_2(x)$, $u_2(x) = v_1(x), v_2(x) = u_1(x) - q_{k-1}(x)v_1(x)$. Продолжая подниматься вверх, получим требуемое разложение для $f(x)$ и $g(x)$. ■

9 Взаимно простые многочлены**Def. (Взаимно простые многочлены)**

Два многочлена называются взаимно простыми, если их НОД равен 1.

Th. (Критерий взаимной простоты)

Рассмотрим два многочлена $f(x), g(x)$.

$$(f(x), g(x)) = 1 \Leftrightarrow \exists u(x), v(x) : f(x)u(x) + g(x)v(x) = 1.$$

Доказательство:

$d(x) = (f(x), g(x)) \Rightarrow d(x) \mid f(x), d(x) \mid g(x) \Rightarrow d(x) \mid f(x)u(x) + g(x)v(x) \Rightarrow d(x) \mid 1 \Rightarrow d(x) = 1$. Доказательство в обратную сторону следует из теоремы о разложении НОД. ■

Свойства взаимно простых многочленов

1. $(f(x), g(x)) = 1, f(x) \mid g(x)\varphi(x) \Rightarrow f(x) \mid \varphi(x)$.

Доказательство:

$$f(x)u(x) + g(x)v(x) = 1 \Rightarrow f(x)u(x)\varphi(x) + g(x)v(x)\varphi(x) = \varphi(x).$$

$$f(x) \mid f(x), f(x) \mid g(x)\varphi(x) \Rightarrow f(x) \mid \varphi(x).$$

2. $(f(x), g(x)) = 1, f(x) \mid \varphi(x), g(x) \mid \varphi(x) \Rightarrow f(x)g(x) \mid \varphi(x)$

Доказательство:

$$f(x)u(x) + g(x)v(x) = 1 \Rightarrow f(x)u(x)\varphi(x) + g(x)v(x)\varphi(x) = \varphi(x).$$

$$f(x)g(x) \mid f(x)\varphi(x), f(x)g(x) \mid g(x)\varphi(x) \Rightarrow f(x)g(x) \mid \varphi(x).$$

3. $(f(x), \varphi(x)) = 1, (g(x), \varphi(x)) = 1 \Rightarrow (f(x)g(x), \varphi(x)) = 1$

Доказательство:

$$f(x)u(x) + \varphi(x)v(x) = 1 \Rightarrow f(x)u(x)g(x) + \varphi(x)v(x)g(x) = g(x) \Rightarrow (f(x)g(x)) \cdot u(x) + \varphi(x) \cdot (v(x)g(x)) = g(x).$$

Пусть $w(x) = (f(x)g(x), \varphi(x))$, тогда $w(x) \mid \varphi(x)$ и, исходя из написанного равенства, $w(x) \mid g(x)$, в то же время $(g(x), \varphi(x)) = 1$, отсюда следует, что $w(x) = 1$.

10 Корни многочлена

Def. (Корень многочлена)

Корнем многочлена $f(x) \in P[x]$ называется элемент $c \in P$, такой, что $f(c) = 0$.

Th. (Теорема Безу)

Остаток от деления многочлена $f(x) \in P[x]$ на двучлен $x - c$ равен $f(c)$.

Доказательство:

Имеем: $f(x) = (x - c)q(x) + r(x)$. Так как $\deg r(x) < \deg (x - c)$, то $\deg r(x) = 0 \Rightarrow r(x) = r \in P$. Следовательно, подставив c , получаем $f(c) = r$. ■

Схема Горнера

Алгоритм, называемый схемой Горнера, позволяет найти значение многочлена в точке c и неполное частное при делении многочлена на двучлен $x - c$.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = (x - c)(b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}) + r$. Проанализируем как найти b_i и r :

$$\begin{cases} a_0 = b_0 \\ a_1 = b_1 - cb_0 \\ a_2 = b_2 - cb_1 \\ \dots \\ a_n = r - cb_{n-1} \end{cases} \Leftrightarrow \begin{cases} b_0 = a_0 \\ b_1 = a_1 + cb_0 \\ b_2 = a_2 + cb_1 \\ \dots \\ r = a_n + cb_{n-1} \end{cases}$$

Пример: $x^4 + 2x^2 - 3x + 2 = (x - 2)(\dots) + r$

$$\begin{array}{c|c|c|c|c|c} & 1 & 0 & 2 & -3 & 2 \\ \hline 2 & 1 & 2 & 6 & 9 & 20 \end{array} \Rightarrow x^4 + 2x^2 - 3x + 2 = (x - 2)(x^3 + 2x^2 + 6x + 9) + 20 \Rightarrow f(2) = 20.$$

Def. (Кратный корень многочлена)

Число $c \in P$ называется корнем кратности k многочлена $f(x) \in P[x]$, если $(x - c)^k \mid f(x)$, $(x - c)^{k+1} \nmid f(x)$.

Корень кратности 1 называется *простым корнем*.

Th. (Теорема о простом корне и производной)

Простой корень многочлена не является корнем его производной.

Доказательство:

Пусть c - простой корень многочлена $f(x)$.

$f(x) = (x - c)q(x)$, $(x - c) \nmid q(x) \Rightarrow q(c) \neq 0$.

$f'(x) = q(x) + (x - c)q'(x) \Rightarrow f'(c) = q(c) \neq 0$. ■

Th. (Теорема о кратном корне и производной)

При $k > 1$ корень многочлена кратности k является корнем кратности $k - 1$ его производной.

Доказательство:

Пусть c - корень кратности k многочлена $f(x)$.

$f(x) = (x - c)^k q(x)$, $(x - c) \nmid q(x) \Rightarrow q(c) \neq 0$.

$f'(x) = k(x - c)^{k-1}q(x) + (x - c)^k q'(x) = (x - c)^{k-1}(kq(x) + (x - c)q'(x))$.

Отсюда видим, что, так как $(x - c) \nmid kq(x)$, то вся скобка $(kq(x) + (x - c)q'(x))$ не делится на $(x - c)$, следовательно $(x - c)$ является корнем кратности $k - 1$. ■

11 Основная теорема алгебры и ее следствия

Th. (Основная теорема алгебры)

Любой многочлен ненулевой степени с комплексными коэффициентами имеет по крайней мере один комплексный корень.

$$\forall f(x) \in \mathbb{C}[x] \exists c \in \mathbb{C} : f(c) = 0, \deg f(x) > 0$$

Следствие 1

Любой многочлен степени n с комплексными коэффициентами имеет n комплексных корней (кратные корни считаются несколько раз в соответствии с их кратностью).

Доказательство:

$f(x) = (x - x_0)g(x)$, $\deg g(x) = \deg f(x) - 1$ и так далее до 0.

Следствие 2

Любой многочлен с комплексными коэффициентами можно единственным образом (с точностью до перестановки множителей) представить в виде произведения $f(x) = a_n \prod_{i=1}^n (x - c_i)$.

Доказательство:

Используем метод математической индукции:

База: $n = 1$: $f(x) = a_1x + a_0 = a_1(x - (-\frac{a_0}{a_1}))$.

Шаг: предположим, что верно $\forall k \leq n$. Докажем, что верно для $n + 1$.

$f(x) = a_{n+1}x^{n+1} + a_nx^n + \dots + a_0 = (x - c_{n+1})\varphi(x)$, $\deg \varphi(x) = n \Rightarrow \varphi(x)$ представим в виде произведения, то есть $f(x)$ также представим в виде произведения. Все слагаемые c_i в данном случае являются корнями многочлена, то есть определены однозначно. Множитель a_n является коэффициентом при старшей степени, то есть также определен однозначно. Отсюда следует, что данное разложение единственно с точностью до перестановки множителей. ■

Следствие 3

$f(x)$, $g(x)$ - два многочлена, $\deg g(x) \leq \deg f(x) \leq n$. Если $f(x) = g(x)$ в более чем n различных точках, то эти многочлены равны как функции.

Доказательство:

Рассмотрим многочлен $\varphi(x) = f(x) - g(x)$, $\deg \varphi(x) \leq n$. То есть многочлен $\varphi(x)$ имеет не более чем n различных корней. С другой стороны, многочлены $f(x)$ и $g(x)$ совпадают минимум в $n + 1$ различной точке, следовательно, $\varphi(x)$ имеет как минимум $n + 1$ различных корней - противоречие. ■

Следствие 4

Алгебраическое и функциональное определения равенства многочленов эквивалентны.

12 Интерполяционная формула Лагранжа

Th. (Интерполяционная формула Лагранжа)

Для любых попарно различных чисел $c_1, c_2, \dots, c_{n+1} \in \mathbb{C}$ и любых $b_1, b_2, \dots, b_{n+1} \in \mathbb{C}$ существует единственный многочлен $f(x)$, $\deg f(x) \leq n$, такой, что $f(c_i) = b_i$, $i \in [1, n+1]$.

Доказательство:

Если такой многочлен существует, то, в силу следствия из основной теоремы алгебры, он определен однозначно, поэтому для доказательства достаточно привести такой многочлен.

$$f(x) = \sum_{j=1}^{n+1} b_j \varphi_j(x),$$

где

$$\varphi_j(x) = \frac{(x - c_1) \dots (x - c_{j-1})(x - c_{j+1}) \dots (x - c_{n+1})}{(c_j - c_1) \dots (c_j - c_{j-1})(c_j - c_{j+1}) \dots (c_j - c_{n+1})}.$$

Отсюда видим, что $\deg \varphi_j(x) = n$, $j \in [1; n+1] \Rightarrow \deg f(x) \leq n$.

Также имеем

$$\varphi_j(c_i) = \begin{cases} 1, & j = i, \\ 0, & j \neq i. \end{cases}$$

поэтому $f(c_i) = \sum_{j=1}^{n+1} b_j \varphi_j(c_i) = b_i$, $i \in [1, n+1]$. ■

Многочлен $\varphi_j(x)$ называется **интерполяционным многочленом Лагранжа**, а формула суммы таких многочленов - **интерполяционной формулой Лагранжа**.

13 Многочлены с вещественными коэффициентами

Лем. (Сопряженное корня многочлена)

Если $f(c) = 0$, $f(x) \in \mathbb{R}$, $c \in \mathbb{C}$, то $f(\bar{c}) = 0$

Доказательство:

$0 = \bar{0} = \overline{f(c)} = \overline{a_n c^n + \dots + a_1 c + a_0} = \overline{a_n} \cdot \overline{c^n} + \dots + \overline{a_1} \cdot \overline{c} + \overline{a_0} = a_n \cdot \overline{c^n} + \dots + a_1 \cdot \overline{c} + a_0 = f(\bar{c})$. ■

Лем. (Кратность сопряженного корня многочлена)

Если $c \in \mathbb{C}$ - k -кратный корень многочлена $f(x) \in \mathbb{R}[x]$, то \bar{c} также является k -кратным корнем $f(x)$.

Доказательство:

Допустим противное: пусть \bar{c} - m -кратный корень.

Предположим, что $m > k$, тогда имеем: $f(x) = (x - c)^k (x - \bar{c})^m g(x)$, $g(c) \neq 0$, $g(\bar{c}) \neq 0$.

Сделаем замену $a(x) = (x - c)(x - \bar{c})$, $g_1(x) = (x - \bar{c})^{m-k} g(x)$, $g_1(c) \neq 0 \Rightarrow f(x) = (a(x))^k g_1(x)$.

Многочлен $g_1(x)$ имеет вещественные коэффициенты, так как является частным двух многочленов с вещественными коэффициентами.

Таким образом получаем $g_1(c) \neq 0$, $g_1(\bar{c}) = 0$ - противоречие ранее доказанной лемме.

Случай с $m < k$ рассматривается аналогично. ■

Следствие

Любой многочлен нечетной степени с действительными коэффициентами имеет хотя бы один действительный корень.

Следствие

Любой многочлен ненулевой степени с вещественными коэффициентами единственным образом представим в виде произведения многочленов степени 1 и 2 с вещественными коэффициентами.

14 Линейные операции над матрицами

Def. (Матрица)

Матрицей размера $m \times n$ называется прямоугольная таблица чисел, состоящая из m строк и n столбцов.

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

Виды матриц

1. Квадратная матрица (матрица порядка n)

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

2. Треугольная матрица

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

3. Диагональная матрица

$$D_n = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

4. Нулевая матрица

$$O_{m,n} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

5. Единичная матрица

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

6. Скалярная матрица

$$\lambda E_n = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda \end{pmatrix}$$

Сложение матриц

Сложение матриц определено для матриц, имеющих одинаковый размер.

$$C = A + B, \quad c_{ij} = a_{ij} + b_{ij}, \quad i = \overline{1, m}, j = \overline{1, n}.$$

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

Свойства сложения матриц

1. Коммутативность

$$A + B = B + A, \quad \forall A, B \in K_{m,n}.$$

2. Ассоциативность

$$(A + B) + C = A + (B + C), \quad \forall A, B, C \in K_{m,n}.$$

3. Существует нейтральный элемент

$$A + O_{m,n} = O_{m,n} + A = A, \quad \forall A \in K_{m,n}.$$

4. Существует противоположный элемент

$$\forall A \in K_{m,n} \exists B \in K_{m,n} \mid A + B = B + A = O_{m,n}, \quad b_{ij} = -a_{ij}.$$

Матрица B обозначается $-A$

Из вышеперечисленных свойств следует, что множество $K_{m,n}$ относительно сложения образует абелеву группу.

Умножение матрицы на скаляр

Произведением элемента λ кольца K на матрицу $A \in K_{m,n}$ называется матрица $C \in K_{m,n}$, такая, что $c_{ij} = \lambda a_{ij}$, $i = \overline{1, m}$, $j = \overline{1, n}$.

Иными словами, умножение матрицы на скаляр - умножение всех элементов матрицы на данную величину. Это произведение обозначается λA .

Свойства умножения матрицы на скаляр

1. $1 \cdot A = A$.
2. $(-1) \cdot A = -A$.
3. $0 \cdot A = O_{m,n}$.
4. $\lambda(A + B) = \lambda A + \lambda B$.
5. $(A + B)\lambda = \lambda A + \lambda B$.
6. $(\lambda\varphi)A = \lambda(\varphi A)$.

15 Умножение матриц

Умножение матриц

Матрица $A_{m,k}$ может умножаться на матрицу $B_{k,n}$ по следующему правилу:

$$A_{m,k} \cdot B_{k,n} = C_{m,n}$$

$$c_{ij} = \sum_{t=1}^k a_{it}b_{tj}, \quad i = \overline{1, m}, \quad j = \overline{1, n}$$

Пример:

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 & 2 & 1 \\ 1 & 1 & 4 & 2 \\ 0 & 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 5 & 9 & 4 \\ 3 & 3 & 3 & 1 \end{pmatrix}$$

Свойства произведения матриц

1. $O_{m,k} \cdot A_{k,n} = O_{m,n}$
2. $A_{m,k} \cdot O_{k,n} = O_{m,n}$
3. $E_n \cdot A_{n,k} = A_{n,k}$
4. $A_{m,n} \cdot E_n = A_{m,n}$
5. $AB \neq BA$
6. $A_{m,n} \cdot (B_{n,k} + C_{n,k}) = A_{m,n}B_{n,k} + A_{m,n}C_{n,k}$
$$\sum_{t=1}^k a_{it}(b_{tj} + c_{tj}) = \sum_{t=1}^k a_{it}b_{tj} + \sum_{t=1}^k a_{it}c_{tj}$$
7. $(A_{n,k} + B_{n,k}) \cdot C_{k,m} = A_{n,k}C_{k,m} + B_{n,k}C_{k,m}$
8. $(A_{m,k}B_{k,n})C_{n,l} = A_{m,k}(B_{k,n}C_{n,l})$

Доказательство:

Любую матрицу можно представить в виде суммы произведений матричной единицы на скаляр. Таким образом, задача дистрибутивно сводится к перемножению матричных единиц.

Транспонирование матрицы

Транспонирование матрицы меняет местами строки и столбцы.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} \quad A^T = \begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{pmatrix}$$

Свойства транспонирования

1. $A^{TT} = A$
2. $(AB)^T = B^T A^T$
3. $(A + B)^T = A^T + B^T, (\lambda A)^T = \lambda A^T$

16 Перестановки

Def. (Перестановка)

Перестановкой называется упорядоченное расположение элементов конечного множества.

Th. (Число перестановок)

Число различных перестановок для n элементов ($n \geq 1$) равно $n!$.

Доказательство:

Докажем с помощью метода математической индукции.

База: Для $n = 1$ утверждение очевидно выполняется.

Шаг: Предположим, что для $n - 1$ число перестановок равняется $(n - 1)!$, докажем, что тогда для n элемента число перестановок будет равно $n!$. Разобьем все перестановки на n классов, в каждом из которых перестановки начинаются с одного и того же элемента. Число перестановок в каждом классе очевидно совпадает с числом перестановок на $n - 1$ элементе и равняется $(n - 1)!$. Следовательно, число перестановок равняется $n \cdot (n - 1)! = n!$. ■

Def. (Транспозиция)

Транспозицией называется преобразование перестановки, меняющее местами какие-либо два элемента.

Th. (Свойство транспозиций)

От любой перестановки можно перейти к любой другой при помощи транспозиций.

Def. (Инверсия)

Говорят, что в данной перестановке числа i, j образуют инверсию, если $i > j$, но число i стоит в перестановке левее числа j .

Число инверсий в перестановке (a_1, a_2, \dots, a_n) обозначается $\nu(a_1, a_2, \dots, a_n)$.

Перестановка называется **четной**, если в ней четное число инверсий, в противном случае - **нечетной**.

Th. (Изменение четности после применения транспозиции)

Однократное применение транспозиции меняет характер четности перестановки.

Доказательство:

Если применить транспозицию к двум рядом стоящим элементам, то очевидно, что характер четности поменяется. Далее рассмотрим общий случай и представим произвольную транспозицию в виде комбинаций транспозиций примененных к рядом стоящим элементам.

$$(\dots, i, a_1, a_2, \dots, a_s, j, \dots)$$

Пусть между произвольными элементами, к которым будем применять транспозицию, находится s элементов. Последовательно применяя транспозиции к рядом стоящим элементам, переместим i на место j , а затем j на место i . Всего будет применено $2s + 1$ транспозиций к рядом стоящим элементам \Rightarrow характер четности изменится. ■

Th. (Число четных и нечетных перестановок)

Пусть M - число четных перестановок, N - число нечетных перестановок. Тогда при $n > 1$ выполняется равенство $M = N = \frac{n!}{2}$.

Доказательство:

К каждой четной перестановке применим одну и ту же транспозицию, как следствие получим M различных нечетных перестановок, то есть $M \leq N$. Аналогично поступим с нечетными и получим $N \leq M$. Следовательно, $M = N$, $M + N = n! \Rightarrow M = N = \frac{n!}{2}$. ■

17 Определитель и его свойства

Def. (Член определителя)

Рассмотрим произвольную квадратную матрицу порядка n над множеством \mathbb{R} .

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Рассмотрим произведение элементов матрицы, взятых ровно по одному из каждой строки и каждого столбца. Любое такое произведение будет содержать n сомножителей и может быть записано в виде

$$a_{\alpha_1 \beta_1} a_{\alpha_2 \beta_2} \dots a_{\alpha_n \beta_n},$$

где $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$, если $i \neq j$. Далее умножим данное произведение на $(-1)^{\nu(\alpha_1, \alpha_2, \dots, \alpha_n) + \nu(\beta_1, \beta_2, \dots, \beta_n)}$. Теперь расположим сомножители так, чтобы первые индексы следовали в порядке возрастания. Таким образом получим **член определителя**:

$$(-1)^{\nu(\gamma_1, \gamma_2, \dots, \gamma_n)} a_{1\gamma_1} a_{2\gamma_2} \dots a_{n\gamma_n}.$$

Def. (Определитель)

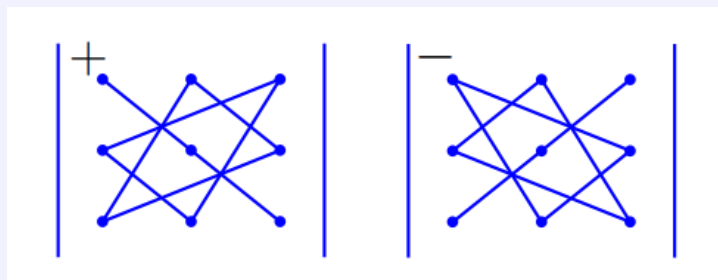
Определителем *квадратной* матрицы $A \in \mathbb{R}_{n,n}$ называется сумма всех членов определителя этой матрицы, то есть выражение

$$\sum_{(\gamma_1, \gamma_2, \dots, \gamma_n)} (-1)^{\nu(\gamma_1, \gamma_2, \dots, \gamma_n)} a_{1\gamma_1} a_{2\gamma_2} \dots a_{n\gamma_n},$$

где сумма содержит все слагаемые, для которых перестановки $(\gamma_1, \gamma_2, \dots, \gamma_n)$ различны. Определитель обозначается несколькими способами:

$$\det A = |A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Правило треугольников:



Все нижеперечисленные свойства, указанные для строк матрицы, актуальны и для ее столбцов (следует из свойства 4).

1. $|O| = 0$.
2. $|D_n| = a_{11}a_{22} \dots a_{nn}$.
3. Определитель треугольной матрицы равен произведению элементов, стоящих на главной диагонали.
4. $|A| = |A^T|$.

Доказательство:

Рассмотрим следующие члены определителей:

$(-1)^{t_1+t_2} a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n}$ - член $\det A$.

$(-1)^{t_2+t_1} b_{j_1 i_1} b_{j_2 i_2} \dots b_{j_n i_n}$ - член $\det A^T$.

И так как $a_{ij} = b_{ji}$, получаем $\det A^T = \det A$.

5. Если в определителе поменять местами две строки, то он изменит знак на противоположный.

Доказательство:

Поменяем местами соседние строки: $(-1)^t a_{1j_1} a_{2j_2} a_{3j_3} \dots a_{nj_n} \rightarrow (-1)^{t+1} a_{2j_2} a_{1j_1} a_{3j_3} \dots a_{nj_n}$ - знак поменялся.

Теперь поменяем две произвольные строки. Пусть между ними находится s строк. Будем поочередно «двигать» одну из строк к другой, поочередно меняя ее местами с соседними, затем так же в обратном направлении будем двигать другую на место первой. Таким образом мы поменяем местами соседние строки $2s + 1$ раз, следовательно, знак определителя поменяется.

6. Определитель матрицы, содержащей нулевую строку, равен 0.
7. Если элементы одной строки умножить на скаляр, то и сам определитель умножится на скаляр.
8. Определитель матрицы, содержащей две одинаковые строки, равен 0.

Доказательство:

Поменяем две одинаковые строки местами. С одной стороны матрица осталась та же, то есть ее определитель не изменился, а с другой, исходя из свойства 5, знак определителя поменялся. То есть $\det A = -\det A = 0$. ■

9. Определитель матрицы с двумя пропорциональными строками равен 0.

10.

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} + a_{j1} & \dots & a_{in} + a_{jn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{j1} & \dots & a_{jn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

11. Определитель не изменится, если к одной строке добавить другую.
12. Определитель не изменится, если к одной строке добавить другую, умноженную на скаляр.
13. Определитель не изменится, если к некоторой строке добавить линейную комбинацию других строк.

18 Теорема Лапласа

Def. (Минор матрицы)

Минором M матрицы назовем определитель, образованный элементами, стоящими на пересечении выбранных k строк и k столбцов ($k < n$). Порядком минора называется число k выбранных строк и столбцов.

Дополнительным минором M' к минору M называется определитель матрицы, образованный элементами, которые не «вычеркнуты» из матрицы после выбора k строк и столбцов для минора M .

Def. (Алгебраическое дополнение)

Алгебраическим дополнением минора M называется дополнительный к нему минор, умноженный на $(-1)^s$, где s - сумма тех номеров строк и столбцов матрицы A , на которых расположена матрица минора M .

Th. (Теорема Лапласа)

Пусть A - квадратная матрица n -ого порядка ($n > 1$). Выберем $1 \leq k < n$ строк (столбцов). Тогда $\det A$ равен сумме произведений всех различных миноров k -ого порядка, расположенных в выделенных k строках (столбцах), на их алгебраические дополнения.

Доказательство:

Рассмотрим определитель $n \times n$ и выберем $k < n$ строк. Таким образом выбрали минор, в котором $k!$ членов и дополнительный к нему минор, в котором $(n - k)!$ членов.

$$M_1 A_1 + \dots + M_s A_s, \quad s = C_n^k = \frac{n!}{k!(n-k)!}$$

Таким образом каждое слагаемое дает $k!(n - k)!$ членов, а всего слагаемых $\frac{n!}{k!(n-k)!}$, следовательно, всего членов будет $n!$ ■

Следствие

Определитель матрицы равен сумме произведений элементов строки/столбца на их алгебраическое дополнение.

$$|A| = \sum_{j=1}^n a_{ij} A_{ij}$$

Следствие

Сумма произведений элементов одной строки (столбца) на алгебраические дополнения другой строки (столбца) равна 0.

$$\sum_{j=1}^n a_{ij} A_{kj} = \delta_{ik} |A| = 0, \quad k \neq i.$$

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

19 Определитель произведения двух матриц

Th. (Определитель произведения двух матриц)

Для двух квадратных матриц A и B порядка n справедливо $|AB| = |A| \cdot |B|$.

Доказательство:

Рассмотрим матрицу D порядка $2n$:

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

С одной стороны, по теореме Лапласа имеем: $|D| = (-1)^{2 \cdot (1+2+\dots+n)} |A| \cdot |B| = |A| \cdot |B|$.

Теперь преобразуем матрицу D таким образом, чтобы в левой верхней части были записаны лишь нули.

Получим следующую матрицу D' , в которой $c_{ij} = (AB)_{ij}$:

$$D' = \begin{pmatrix} 0 & 0 & \dots & 0 & c_{11} & \dots & c_{1n} \\ 0 & 0 & \dots & 0 & c_{21} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & c_{n1} & \dots & c_{nn} \\ -1 & 0 & \dots & 0 & b_{11} & \dots & b_{1n} \\ 0 & -1 & \dots & 0 & b_{21} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & b_{n1} & \dots & b_{nn} \end{pmatrix}$$

Так как все, что мы делали, это прибавляли к строке другую, умноженную на скаляр, определитель не поменяется, поэтому $|A| \cdot |B| = |D| = |D'| = (-1)^{1+2+\dots+n+\dots+2n} |C| \cdot |-E_n| = |C| (-1)^{\frac{2n+1}{2}n} (-1)^n = |C| = |AB|$. ■

20 Обратная матрица

Def. (Обратная матрица)

Матрица X называется обратной к матрице A , если $AX = XA = E_n$.

Матрицу X обычно обозначают A^{-1} .

Th. (Единственность обратной матрицы)

Если для матрицы A существует обратная матрица, то она единственна.

Доказательство:

Предположим противное: пусть у квадратной матрицы есть две различные обратные матрицы X и Y . Тогда $Y = YE = Y(AX) = EX = X$ - противоречие.

Def. (Вырожденная матрица)

Квадратная матрица A называется **вырожденной**, если $|A| = 0$, в противном случае - **невырожденной**.

Def. (Присоединенная матрица)

Матрицей, присоединенной к матрице A , называется матрица

$$B = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix},$$

где A_{ij} - алгебраическое дополнение элемента a_{ij} матрицы A .

$$AB = BA = \det A \cdot E_n$$

Th. (Критерий существования обратной матрицы)

Для того, чтобы для матрицы A существовала обратная матрица, необходимо и достаточно, чтобы она была невырожденной.

Доказательство:

Необходимость: Пусть для матрицы A существует обратная матрица A^{-1} , тогда $|A||A^{-1}| = |E| = 1 \Rightarrow |A| \neq 0$.

Достаточность: Пусть A - невырожденная матрица. Тогда из ранее записанного выражения для присоединенной матрицы можем получить, что $A^{-1} = \frac{1}{\det A} B$, где B - присоединенная матрица к матрице A .

Способы нахождения обратной матрицы

1. Из доказательства предыдущей теоремы вытекает первый способ нахождения:

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

2. Метод Гаусса:

$$\begin{aligned} A | E &= \left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \dots & a_{1n} & 1 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 1 \end{array} \right) \sim \dots \sim \\ &\sim \left(\begin{array}{cccc|cccc} 1 & 0 & \dots & 0 & a'_{11} & a'_{12} & \dots & a'_{1n} \\ 0 & 1 & \dots & 0 & a'_{21} & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a'_{n1} & a'_{n2} & \dots & a'_{nn} \end{array} \right) = E | A^{-1} \end{aligned}$$

Свойства обратных матриц

1. $(A^{-1})^{-1} = A$
2. $(AB)^{-1} = B^{-1}A^{-1}$
3. $(A^{-1})^T = (A^T)^{-1}$

21 Правило Крамера

Def. (Невырожденная система линейных уравнений)

Система n линейных уравнений с n неизвестными называется **невырожденной**, если определитель ее матрицы не равен нулю. В противном случае система называется **вырожденной**. Соответствующее матричное уравнение также называется **невырожденным**.

Th. (Правило Крамера)

Невырожденная система n линейных уравнений с n неизвестными имеет единственное решение, которое может быть найдено по формулам

$$x_i = \frac{|A_i|}{|A|}, \quad i = \overline{1, n},$$

где матрица A_i получена из матрицы A путем замены в ней i -ого столбца на столбец свободных членов.

Доказательство:

$$AX = B \Leftrightarrow X = A^{-1}B$$

$$\begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix} = \frac{1}{|A|} \begin{pmatrix} A_{11}b_1 + A_{21}b_2 + \dots + A_{n1}b_n \\ A_{12}b_1 + A_{22}b_2 + \dots + A_{n2}b_n \\ \dots \\ A_{1n}b_1 + A_{2n}b_2 + \dots + A_{nn}b_n \end{pmatrix}$$

отсюда, исходя из определения равенства матриц, получаем

$$x_i = \frac{1}{|A|} (A_{1i}b_1 + A_{2i}b_2 + \dots + A_{ni}b_n) = \frac{1}{|A|} \begin{vmatrix} a_{11} & \dots & a_{1,i-1} & b_1 & a_{1,i+1} & \dots & a_{1n} \\ a_{21} & \dots & a_{2,i-1} & b_2 & a_{2,i+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,i-1} & b_n & a_{n,i+1} & \dots & a_{2n} \end{vmatrix} = \frac{|A_i|}{|A|}. \blacksquare$$

22 Метод Гаусса решения системы линейных уравнений

Def. (Эквивалентные системы линейных уравнений)

Рассмотрим две системы m линейных уравнений с n неизвестными. Решением системы называется упорядоченный набор чисел $(\gamma_1, \gamma_2, \dots, \gamma_n)$, удовлетворяющий всем уравнениям системы. Две системы называются эквивалентными, если у них одинаковое множество решений.

Применение элементарных преобразований к матрице системы изменяет систему на эквивалентную.

Метод Гаусса

Сначала проверяем выполняется ли, что $a_{11} \neq 0$, если нет, то элементарными преобразованиями делаем так, чтобы выполнялось.

Затем к i -ой строке прибавляем j -ую, умноженную на $-\frac{a_{ij}}{a_{jj}}$, где $j = \overline{1, n}$, $i = \overline{j+1, n}$. После всех преобразований возможны два случая:

1. $0 = 1 \Rightarrow$ система несовместна.
2. Матрица привелась к треугольному или трапецидальному виду.

В случае приведения к треугольному виду, система имеет единственное решение, которое можно получить, приведя данную матрицу к диагональной:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & b_n \end{array} \right) \sim \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b'_1 \\ 0 & a_{22} & \dots & a_{2n} & b'_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} & b'_n \end{array} \right) \sim \left(\begin{array}{cccc|c} a_{11} & 0 & \dots & 0 & B_1 \\ 0 & a_{22} & \dots & 0 & B_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} & B_n \end{array} \right)$$

То есть получаем решение: $(\frac{B_1}{a_{11}}, \frac{B_2}{a_{22}}, \dots, \frac{B_n}{a_{nn}})$.

В случае приведения к трапецидальной матрице, выделим свободные переменные, а затем опять приведем матрицу к треугольному виду:

$$\left(\begin{array}{cccccc|c} a_{11} & a_{12} & \dots & a_{1r} & \dots & a_{1n} & b_1 \\ 0 & a_{22} & \dots & a_{2r} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} & \dots & a_{rn} & b_r \end{array} \right) \sim \left(\begin{array}{cccccc|c} a_{11} & a_{12} & \dots & a_{1r} & \dots & a_{1n} & b_1 - a_{1,r+1} - \dots - a_{1,n} \\ 0 & a_{22} & \dots & a_{2r} & \dots & a_{2n} & b_2 - a_{2,r+1} - \dots - a_{2,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} & \dots & a_{rn} & b_r - a_{r,r+1} - \dots - a_{r,n} \end{array} \right) \sim$$
$$\sim \left(\begin{array}{cccccc|c} 1 & 0 & \dots & 0 & \dots & 0 & B_1 \\ 0 & 1 & \dots & 0 & \dots & 0 & B_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & B_r \end{array} \right)$$

B_i - коэффициент, зависящий от значений b_j -ых и свободных переменных.

Общее решение: $(B_1, B_2, \dots, B_r, \alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$, α_i - значение свободной переменной x_i .

Th. (Результат метода Гаусса)

Методом Гаусса система линейных уравнений приводится к одному из трех следующих видов (то есть эквивалентна им):

1. Несовместная система линейных уравнений (нет решений).
2. Определенная система линейных уравнений (ровно одно решение).
3. Неопределенная система линейных уравнений (несколько решений).

23 Определение и простейшие свойства векторных пространств

Def. (Векторное линейное пространство)

Пусть V - непустое множество с заданной на нем операцией сложения. Элементы V будем называть **векторами** и обозначать $a, b, c \dots$

\mathbb{F} - поле, элементы которого будем называть **скалярами** и обозначать $\alpha, \beta, \gamma \dots$

Множество V называется векторным линейным пространством над полем \mathbb{F} , если выполнены следующие условия:

1. Множество V является абелевой группой по сложению
 - $a + b \in V$
 - $a + b = b + a$ - коммутативность
 - $(a + b) + c = a + (b + c)$ - ассоциативность
 - $0 + a = a$ - наличие нейтрального элемента
 - $\forall a \exists (-a) \mid a + (-a) = 0$ - наличие симметричного элемента
2. $\lambda a \in V$ - определено умножение на скаляр
3. $\lambda(a + b) = \lambda a + \lambda b, (\lambda + \varphi)a = \lambda a + \varphi a$ - дистрибутивность
4. $1 \cdot a = a$ - наличие нейтрального элемента
5. $(\lambda \varphi)a = \lambda(\varphi a)$ - ассоциативность

Свойства векторного линейного пространства

1. Существует лишь один нейтральный элемент.

Доказательство:

$$o_1 = o_1 + o_2 = o_2$$

2. У каждого элемента ровно один противоположный

Доказательство:

Допустим у вектора a два противоположных элемента x и y . Тогда: $y = \bar{0} + y = (x + a) + y = x + (a + y) = x + \bar{0} = x$

3. $0 \cdot a = \bar{0}$

Доказательство:

$$x = 0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a = x + x \Rightarrow x = x + x \Rightarrow -x + x = -x + x + x \Rightarrow x = \bar{0}.$$

4. $(-1)a = -a$

Доказательство:

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

5. $\lambda \cdot \bar{0} = \bar{0}$

Доказательство:

$$\lambda \cdot \bar{0} = \lambda(a + (-a)) = \lambda(a + (-1)a) = \lambda a(1 + (-1)) = \lambda(0a) = \bar{0}$$

6. $\lambda(a - b) = \lambda a - \lambda b$

7. $(-\alpha)a = \alpha(-a) = -(\alpha a)$

24 Линейная зависимость векторов

Def. (Линейная зависимость векторов)

Определение 1:

Система векторов (a_1, a_2, \dots, a_k) называется линейно зависимой, если $\exists \alpha_1, \dots, \alpha_k \mid \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k = 0, \alpha_1^2 + \alpha_2^2 + \dots + \alpha_k^2 > 0$.

Определение 2:

Система называется линейно зависимой, если хотя бы один вектор линейно выражается через остальные.

Докажем, что данные определения эквивалентны:

#1 \Rightarrow #2:

Пусть $\alpha_1 \neq 0$, тогда можно записать $a_1 = -\frac{\alpha_2}{\alpha_1} a_2 - \frac{\alpha_3}{\alpha_1} a_3 - \dots - \frac{\alpha_k}{\alpha_1} a_k$.

#2 \Rightarrow #1:

$a_1 = \alpha_2 a_2 + \alpha_3 a_3 + \dots + \alpha_k a_k \Rightarrow (-1)a_1 + \alpha_2 a_2 + \alpha_3 a_3 + \dots + \alpha_k a_k = 0$.

Def. (Линейная независимость векторов)

Определение 1:

Система векторов (a_1, a_2, \dots, a_k) называется линейно независимой, если $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k = 0 \Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_k = 0$.

Определение 2:

Система называется линейно независимой, если ни один вектор не выражается линейно через остальные.

Свойства

1. Один вектор линейно зависим, только когда он нулевой.
2. Два вектора линейно зависимы, тогда и только тогда, когда один выражается через другой.
3. Система, содержащая нулевой вектор, линейно зависима.
4. Система, содержащая два пропорциональных вектора, линейно зависима.
5. Если подсистема системы векторов линейно зависима, то и вся система линейно зависима.

Def. (Эквивалентные системы векторов)

Системы векторов G и H называются эквивалентными, если векторы системы G линейно выражаются через векторы системы H и наоборот.

25 Основная теорема о линейной зависимости

Th. (Основная теорема о линейной зависимости)

Рассмотрим две системы векторов $A(a_1, a_2, \dots, a_m)$, $B(b_1, b_2, \dots, b_n)$, такие, что система A линейно независима и выражается через систему B .

Тогда справедливо неравенство $m \leq n$.

Доказательство:

Так как система A линейно выражается через систему B , то можно записать вектор a_1 в виде $a_1 = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n$, то есть система $(a_1, b_1, b_2, \dots, b_n)$ линейно зависима. Не нарушая общности, положим, что $\beta_1 \neq 0$, тогда справедливо равенство

$b_1 = -\frac{\alpha_1}{\beta_1} a_1 - \frac{\beta_2}{\beta_1} b_2 - \dots - \frac{\beta_n}{\beta_1} b_n$, то есть b_1 линейно выражается через систему $B'(a_1, b_2, \dots, b_n)$.

Если систему B заменить на систему B' , то условие теоремы не нарушается, так как во всех линейных комбинациях, которые выражают векторы системы A через векторы системы B можно заменить b_1 на $-\frac{\alpha_1}{\beta_1} a_1 - \frac{\beta_2}{\beta_1} b_2 - \dots - \frac{\beta_n}{\beta_1} b_n$, таким образом в системе B векторы каждый вектор b_i можно заменить на $a_i \forall i \in [1; m]$, следовательно $m \leq n$. ■

Def. (Линейная оболочка)

$$L(a_1, a_2, \dots, a_n) = \{v \mid v = \sum_{i=1}^n \alpha_i a_i, \alpha_i \in \mathbb{R}\}$$

Любые $n + 1$ векторов из линейной оболочки n векторов линейно зависимы.

26 Базис и размерность векторного пространства

Def. (Базис векторного пространства)

Векторы e_1, e_2, \dots, e_n называются базисом векторного пространства, если выполняется:

1. Система e_1, e_2, \dots, e_n линейно независима
2. Через данные векторы можно выразить любой вектор пространства

Для векторного пространства V возможны три случая:

1. V - нулевое пространство.
2. V имеет базис.
3. V - ненулевое пространство, не имеющее базиса.

В первых двух случаях пространство называют *конечномерным*, а **размерностью пространства** называют количество векторов в базисе. Пространство V размерности n называется n -мерным, $\dim V = n$.

В третьем случае пространство называют бесконечномерным. $\dim V = \infty$.

Th. (Количество векторов в базисе)

Все базисы одного векторного пространства содержат одинаковое количество векторов.

Доказательство:

Рассмотрим два различных базиса (e_1, e_2, \dots, e_m) и $(e'_1, e'_2, \dots, e'_n)$. Исходя из основной теоремы о линейной зависимости получаем, что, с одной стороны, $m \geq n$, а, с другой стороны, $n \geq m$. Следовательно, $m = n$. ■

Координаты вектора в базисе

Координатами вектора x в базисе (e_1, \dots, e_n) называются коэффициенты разложения данного вектора по базису.

Вектор раскладывается по базису единственным образом.

Доказательство:

Пусть $x = x_1 e_1 + \dots + x_n e_n = x'_1 e_1 + \dots + x'_n e_n \Rightarrow (x_1 - x'_1) e_1 + \dots + (x_n - x'_n) e_n = 0$.

Так как система векторов (e_1, \dots, e_n) является базисом, то она линейно независима, следовательно $x_i = x'_i, i = \overline{1, n}$.

Свойства:

1. При сложении векторов, их координаты складываются.
2. При умножении вектора на скаляр его координаты умножаются на скаляр.

Свойства базиса

1. В n -мерном пространстве любые $n + 1$ векторов линейно зависимы.
2. В n -мерном пространстве любая система из n л.н.з векторов является базисом.

Доказательство:

Рассмотрим л.н.з систему (a_1, \dots, a_n) и вектор x , который не выражается через эту систему. Тогда система (a_1, \dots, a_n, x) также линейно независима. Однако она состоит из $n + 1$ вектора, значит по свойству 1 она линейно зависима - противоречие.

3. Любую линейно независимую систему можно дополнить до базиса.

Доказательство:

Рассмотрим линейно независимую систему (a_1, a_2, \dots, a_m) векторного пространства V_n . Если $m = n$, то данная система уже является базисом. Случай $m > n$ невозможен по свойству 1. В случае $m < n$ данная система не является базисом, значит найдется вектор, который не выражается через данную систему, добавим его в систему. Будем продолжать дополнять систему таким образом, пока в системе будет меньше n векторов.

4. Если в пространстве V_n для системы (e_1, \dots, e_n) выполняется $L(e_1, \dots, e_n) = V$, то данная система является базисом.

27 Ранг матрицы

Def. (Базис системы векторов)

Подсистема A' системы векторов $A = (a_1, a_2, \dots, a_n)$ называется **базисом**, если:

1. A' - линейна независима.
2. Любой вектор системы A линейно выражается через векторы из A' .

Базис системы обладает теми же свойствами, что и базис векторного пространства:

1. Любые два базиса равномощны.
2. Любую линейно независимую систему можно дополнить до базиса.

Def. (Ранг системы и ранг матрицы)

Ранг системы векторов - количество векторов в базисе.

Ранг матрицы - ранг системы ее строк.

Th. (Теорема о ранге матрицы)

Ранг матрицы равен наивысшему порядку отличных от нуля миноров.

Доказательство:

Не нарушая общности, будем считать, что базисный минор расположен в левом верхнем углу матрицы (перестановка строк или столбцов не влияет на зависимость строк).

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2r} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} & \dots & a_{rn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mr} & \dots & a_{mn} \end{pmatrix}$$

Необходимо доказать, что данные r строк линейно независимы и что любую другую строку матрицы A можно выразить через эти базисные строки.

Рассмотрим наибольший минор M , отличный от нуля:

$$M = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix} \neq 0$$

Допустим противное: пусть данные r строк линейно зависимы, но тогда части этих строк в миноре M также зависимы. То есть при преобразовании минора, можно получить нулевую строку, следовательно, $M = 0$ - противоречие.

Теперь докажем, что любая строка линейно выражается через первые r строк матрицы. Данное утверждение очевидно для строк с номерами от 1 до r . Рассмотрим строку с номером $s > r$ и вспомогательный минор R .

$$R = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} & a_{1j} \\ a_{21} & a_{22} & \dots & a_{2r} & a_{2j} \\ \dots & \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} & a_{rj} \\ a_{s1} & a_{s2} & \dots & a_{sr} & a_{sj} \end{vmatrix} = 0, \quad 1 \leq j \leq n.$$

Данный определитель равен 0, так как, при $j < r$ найдутся 2 повторяющихся столбца, а при $j \geq r$, получим систему с $r + 1$ элементами (причем известно, что минор M порядка r наибольший, отличный от нуля).

По теореме Лапласа имеем: $a_{1j}A_{1j} + a_{2j}A_{2j} + \dots + a_{rj}A_{rj} + a_{sj}A_{sj} = 0 \Rightarrow a_{sj} = -\frac{A_{1j}}{M}a_{1j} - \frac{A_{2j}}{M}a_{2j} - \dots - \frac{A_{rj}}{M}a_{rj}$, $1 \leq j \leq n$. То есть все строки матрицы линейно выражаются через строки минора. ■

Следствия из теоремы о ранге матрицы

1. Ранг матрицы равен рангу системы ее столбцов.
2. Ранг матрицы не меняется при транспонировании.

28 Вычисление ранга матрицы с помощью элементарных преобразований

Th. (Ранг эквивалентных систем)

Ранги эквивалентных систем равны.

Доказательство:

Рассмотрим эквивалентные системы G и Q и их базисы G_1 и Q_1 размера g_1 и q_1 соответственно. Системы G_1 и Q_1 являются базисом системы $G \cup Q$, так как они линейно независимы и векторы системы $G \cup Q$ выражаются через них, так как системы G и Q эквивалентны. Отсюда получаем $g_1 = \text{rank}(G \cup Q) = q_1$. ■

Th. (Влияние элементарных преобразований на ранг матрицы)

Элементарные преобразования не меняют ранг матрицы.

Доказательство:

Рассмотрим систему строк (a_1, a_2, \dots, a_n) матрицы A и докажем, что элементарные преобразования приводят к эквивалентной системе, что равносильно сохранению ранга.

1. Умножение строки на ненулевой скаляр.

Очевидно, что системы (a_1, a_2, \dots, a_n) и $(\lambda a_1, a_2, \dots, a_n)$ эквивалентны.

2. Прибавление одной строки, умноженной на скаляр, к другой.

Аналогично системы (a_1, a_2, \dots, a_n) и $(a_1 + \lambda a_2, a_2, \dots, a_n)$ эквивалентны.

3. Изменение взаимного расположения строк

Содержимое системы строк не изменилось, следовательно она эквивалентна исходной системе строк. ■

Данные рассуждения справедливы и для столбцов матрицы.

Элементарные преобразования симметричны, рефлексивны, транзитивны \Rightarrow определено бинарное отношение эквивалентности.

Преобразование матрицы

Алгоритм заключается в приведении матрицы к единичному виду с помощью элементарных преобразований.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \sim \begin{pmatrix} 1 & a'_{12} & \dots & a'_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \sim \begin{pmatrix} 1 & a'_{12} & \dots & a'_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix} \sim \\ \sim \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix} \sim \dots \sim \begin{pmatrix} E_r & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{pmatrix}$$

По теореме о ранге матрицы, рассмотрев минор r -ого порядка в левом верхнем углу матрицы, получаем, что ранг матрицы равен r .

29 Подпространства векторного пространства

Def. (Подпространство векторного пространства)

Непустое подмножество W векторного пространства V над полем \mathbb{F} называется подпространством векторного пространства V , если оно само является векторным пространством относительно имеющихся операций.

Th. (Критерий подпространства)

Подмножество W является подпространством V тогда и только тогда, когда выполняются две следующие аксиомы:

$$\begin{cases} w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W \\ w \in W \Rightarrow \lambda w \in W \end{cases}$$

Доказательство:

\Rightarrow : в силу того, что W само является векторным пространством, то данные аксиомы выполняются по определению.

\Leftarrow : так как мы не переопределяли операции, то коммутативность, ассоциативность, дистрибутивность и иные свойства, накладывающие ограничения непосредственно на операции, уже выполнены. Необходимо доказать, что выполнение двух вышестоящих аксиом влечет существование нулевого вектора и существование противоположного элемента для каждого элемента подмножества.

Нулевой вектор существует, так как подмножество W непустое, следовательно, взяв произвольный вектор w получаем, что $0 \cdot w = \bar{0} \in W$. Противоположный элемент получается аналогично умножением на -1 . ■

Общее условие

$$w_1, w_2 \in W \Rightarrow \lambda_1 w_1 + \lambda_2 w_2 \in W, \forall \lambda \in \mathbb{F}$$

Th. (Размерность подпространства)

Если W - подпространство векторного пространства V , то

$$\dim W \leq \dim V$$

Th. (Дополнение базиса)

Базис подпространства можно дополнить до базиса пространства.

Доказательство:

Базис подпространства является также линейно независимой системой векторов в самом пространстве, следовательно, как было доказано ранее, может быть дополнен до базиса. ■

Def. (Сумма и пересечение подпространств)

Рассмотрим два подпространства $W_1, W_2 \subset V$.

Пересечением подпространств называется множество $W_1 \cap W_2 = \{w \mid w \in W_1, w \in W_2\}$.

Суммой подпространств называется множество $W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$.

Th. (Размерность суммы подпространств)

$$\dim (W_1 + W_2) = \dim W_1 + \dim W_2 - \dim (W_1 \cap W_2)$$

31 Однородные системы линейных уравнений

Def. (Однородная система линейных уравнений (ОСЛУ))

Однородной системой линейных уравнений называется система вида

[illegible]

В матричном виде: $AX = 0$.

Свойства ОСЛУ

1. ОСЛУ всегда совместна.
2. Система будет определенной $\Leftrightarrow r = n$.
3. Множество решений однородной системы образует векторное пространство.

Доказательство:

Пусть X_1 и X_2 - решения ОСЛУ.

Тогда $AX_1 = O$ и $AX_2 = O$. $A(X_1 + X_2) = AX_1 + AX_2 = O + O = O \Rightarrow X_1 + X_2$ - решение ОСЛУ.

$$A(\lambda X_1) = \lambda AX_1 = \lambda O = O \Rightarrow \lambda X_1 - \text{решение ОСЛУ.} \blacksquare$$

Взаимодействие однородных и неоднородных систем

Рассмотрим неоднородную систему линейных уравнений и соответствующую ей однородную: $AX = B$, $AX = O$

1. Сумма решений однородной и неоднородной системы является решением неоднородной системы.

Доказателство:

$$A(X_1 + X_2) = AX_1 + AX_2 = B + O = B$$

2. Разность решений неоднородной системы является решением однородной системы.

Доказателство:

$$A(X_1 - X_2) = AX_1 - AX_2 = B - B = O$$

3. Любое решение неоднородной системы можно получить из фиксированного решения неоднородной, добавляя некое решение однородной.

Поиск базисного пространства решений

Выберем базисный минор матрицы системы. Считаем, что он расположен в левом верхнем углу (перестановки строк не изменяют решение). Обозначим $r = \text{rank} A$. Перепишем систему:

[illegible]

x_1, x_2, \dots, x_r - базисные переменные, x_{r+1}, \dots, x_n - свободные переменные.

Придадим свободным переменным значения:

- 1) $1, 0, \dots, 0$

- 2) $0, 1, \dots, 0$

• • •

- $$n-r) \ 0, 0, \dots, 1$$

Для каждого набора свободных переменных найдем значения базисных переменных:

$$c_1 = (\alpha_{11}, \alpha_{12}, \dots, \alpha_{1r}, 1, 0, \dots, 0)$$

$$c_2 = (\alpha_{21}, \alpha_{22}, \dots, \alpha_{2r}, 0, 1, \dots, 0)$$

• • •

$$c_{n-r} = (\alpha_{n-r\ 1}, \alpha_{n-r\ 2}, \dots, \alpha_{n-r\ r}, 0, 0, \dots, 1)$$

Th. (Фундаментальная система решений)

Система $(c_1, c_2, \dots, c_{n-r})$ является базисом пространства решений ОСЛУ.

Доказательство:

Требуется доказать:

1. Система $(c_1, c_2, \dots, c_{n-r})$ линейно независима.

2. Любое решение линейно выражается через $(c_1, c_2, \dots, c_{n-r})$.

1. Система $(c_1, c_2, \dots, c_{n-r})$ линейно независима, так как очевидно, что значения свободных переменных не выражаются через другие.

2. Пусть $c = (\gamma_1, \gamma_2, \dots, \gamma_n)$ - произвольное решение ОСЛУ. Заметим, что $c - \gamma_{r+1}c_1 - \gamma_{r+2}c_2 - \dots - \gamma_n c_{n-r} = (0, \dots, 0, 0, \dots, 0) \Rightarrow c = \gamma_{r+1}c_1 + \gamma_{r+2}c_2 + \dots + \gamma_n c_{n-r}$. Так как совпали свободные переменные, то совпадут и базисные. Таким образом получаем, что произвольное решение c линейно выражается через $(c_1, c_2, \dots, c_{n-r})$. ■

Следствие

Размерность пространства решений ОСЛУ равна $n - r$, где n - число переменных, $r = rank A$.

32 Линейные преобразования векторного пространства

Def. (Линейное преобразование векторного пространства)

Отображение $\varphi : V_n \rightarrow V_n$ называется линейным преобразованием (оператором), если выполняются следующие условия:

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(\lambda a) = \lambda \varphi(a)$

Примеры

1. $\varphi(v) = \bar{0}$ - нулевое преобразование.
2. $\varphi(v) = v$ - тождественное преобразование.
3. $D(f) = f'$ - дифференцирование (на множестве бесконечно дифференцируемых функций на отрезке).

Свойства линейного преобразования

1. $\varphi(\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n) = \lambda_1 \varphi(a_1) + \lambda_2 \varphi(a_2) + \dots + \lambda_n \varphi(a_n)$ - образ линейной комбинации равен такой же линейной комбинации образов.
2. $\varphi(\bar{0}) = \bar{0}$.
 $\varphi(\bar{0}) = \varphi(0 \cdot \bar{a}) = 0 \cdot \varphi(\bar{a}) = \bar{0}$
3. Линейное преобразование сохраняет линейную зависимость векторов.
 $\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n = \bar{0} \Rightarrow \varphi(\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n) = \varphi(\bar{0}) \Rightarrow \lambda_1 \varphi(a_1) + \lambda_2 \varphi(a_2) + \dots + \lambda_n \varphi(a_n) = \bar{0}$.

Th. (Единственность линейного преобразования)

Пусть (e_1, e_2, \dots, e_n) - базис векторного пространства V_n , а (a_1, a_2, \dots, a_n) - произвольная система векторов. Тогда существует единственное линейное преобразование, такое что

$$\begin{cases} \varphi(e_1) = a_1 \\ \varphi(e_2) = a_2 \\ \dots\dots\dots \\ \varphi(e_n) = a_n \end{cases}$$

Доказательство:

Возьмем произвольный вектор x и разложим его по базису: $x = x_1 e_1 + \dots + x_n e_n \Rightarrow \varphi(x) = x_1 a_1 + \dots + x_n a_n$. Требуется доказать, что данное отображение является линейным преобразованием.

Рассмотрим два вектора $x = x_1 e_1 + \dots + x_n e_n$ и $y = y_1 e_1 + \dots + y_n e_n$.

$$\varphi(x + y) = (x_1 + y_1) a_1 + \dots + (x_n + y_n) a_n = \varphi(x) + \varphi(y).$$

$$\varphi(\lambda x) = x_1 \lambda a_1 + \dots + x_n \lambda a_n = \lambda \varphi(x).$$

Теперь докажем, что данное преобразование единственно. Предположим противное: пусть существует еще одно преобразование ψ , для которого выполняется вышепречисленное свойство.

Тогда $\varphi(x) = x_1 a_1 + \dots + x_n a_n = x_1 \psi(e_1) + \dots + x_n \psi(e_n) = \psi(x)$ - противоречие, т.к. они получились равными. ■

33 Ядро и образ линейного преобразования

Def. (Ядро и образ линейного преобразования)

Ядром преобразования φ называется множество векторов $\ker \varphi = \{v \mid \varphi(v) = \bar{0}\}$.

Образом преобразования φ называется множество векторов $Im \varphi = \{\varphi(v) \mid v \in V\} = \varphi(V)$.

Th. (Свойство ядра и образа)

Ядро и образ векторного пространства V так же являются его подпространствами.

Доказательство:

1. $w_1, w_2 \in \ker \varphi$

- $\varphi(w_1 + w_2) = \varphi(w_1) + \varphi(w_2) = \bar{0} + \bar{0} = \bar{0} \Rightarrow w_1 + w_2 \in \ker \varphi$.
- $\varphi(\lambda w_1) = \lambda \varphi(w_1) = \lambda \cdot \bar{0} = \bar{0} \Rightarrow \lambda w_1 \in \ker \varphi$.

2. $w_1, w_2 \in Im \varphi \Rightarrow w_1 = \varphi(v_1), w_2 = \varphi(v_2)$.

- $w_1 + w_2 = \varphi(v_1) + \varphi(v_2) = \varphi(v_1 + v_2) \Rightarrow w_1 + w_2 \in Im \varphi$.
- $\lambda w_1 = \lambda \varphi(v_1) = \varphi(\lambda v_1) \Rightarrow w_1 \in Im \varphi$. ■

Def. (Дефект и ранг линейного преобразования)

Дефектом линейного преобразования называется размерность ядра $d = \dim(\ker \varphi)$.

Рангом линейного преобразования называется размерность образа $r = \dim(Im \varphi)$.

Th. (Сумма дефекта и ранга линейного преобразования)

Сумма ранга и дефекта линейного преобразования φ векторного пространства V_n равна размерности пространства, то есть $d + r = n$.

Доказательство:

Рассмотрим базис $E(e_1, e_2, \dots, e_n)$ пространства V_n . Пусть оператор φ имеет в базисе E матрицу A . Обозначим через X координатный столбец произвольного вектора $x \in V_n$, а через Y - координатный столбец вектора $y = \varphi(x)$.

Тогда имеем: $Y = AX$. Рассмотрев вектор из ядра преобразования, получим $O = AX$. Данное уравнение является однородным, поэтому размерность пространства решений данного уравнения равна $n - \text{rank}(A)$. С другой стороны, размерность этого подпространства также равна $\dim(\ker \varphi) = d$. И, так как ранг линейного оператора равен рангу его матрицы, записанной в некотором базисе оператора, получаем, что $d + r = n$. ■

Th. (Свойство биективного линейного преобразования)

φ - биекция $\Leftrightarrow \dim(\ker \varphi) = 0$

\Rightarrow : в таком случае ядром будет лишь нулевой вектор, а он линейно зависим.

\Leftarrow : Базис ядра имеет размерность 0, следовательно ядро состоит только из нулевого вектора, в ином случае базис состоял хотя бы из одного вектора.

Необходимо доказать, что преобразование инъективно и сюръективно. Допустим оно неинъективно, тогда найдутся два различных вектора v_1, v_2 , такие, что $\varphi(v_1) = \varphi(v_2)$, но тогда $\varphi(v_1 - v_2) = \bar{0} \Rightarrow (v_1 - v_2) \in \ker \varphi \Rightarrow v_1 = v_2$ - противоречие.

Если преобразование пространства V_n не сюръективно, то $\text{rank}(\varphi) < n \Rightarrow d > 0$ - противоречие. ■

34 Матрица линейного преобразования

Def. (Матрица линейного преобразования)

Пусть $\varphi : V_n \rightarrow V_n$ - линейное преобразование. Применим отображение к каждому вектору базиса V_n :

[illegible]

Матрицей линейного преобразования называется транспонированная матрица данной системы линейных уравнений:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Столбцы матрицы линейного преобразования - координатные столбцы образов базисных векторов.

Примеры

1. $\varphi(v) = \bar{0}$ - нулевая матрица.
2. $\varphi(v) = v$ - единичная матрица.
3. $\varphi(i) = 1 \cdot i + 0 \cdot j + 0 \cdot k$, $\varphi(j) = 0 \cdot i + 1 \cdot j + 0 \cdot k$, $\varphi(k) = 0 \cdot i + 0 \cdot j + 0 \cdot k$ - проекция на плоскость.

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

Биекция между матрицами и преобразованиями

Пусть у нас есть базисная строка и строка образов: (e_1, e_2, \dots, e_n) , $(\varphi(e_1), \varphi(e_2), \dots, \varphi(e_n))$. Как мы помним, $\varphi(e) = eA$.

Теперь рассмотрим произвольный вектор x и его координатный столбец X в базисе e .
 $x = eX \Rightarrow \varphi(x) = \varphi(e)X = eAX \Rightarrow \varphi(X) = AX$ при условии, что координатный столбец и матрица рассматриваются в одном базисе.

Th. (Ранг матрицы линейного преобразования)

Ранг линейного преобразования равен рангу его матрицы.

$$\text{rank}(\varphi) = \text{rank}(A)$$

Доказательство:

$$rank(\varphi) = \dim \varphi(V_n) = \dim L(\varphi(e_1), \varphi(e_2), \dots, \varphi(e_n)) = rank(\varphi(e_1), \varphi(e_2), \dots, \varphi(e_n)) = rank(A). \blacksquare$$

Th. (Арифметические операции с преобразованиями)

При сложении двух преобразований их матрицы складываются, при перемножении - перемножаются, при умножении преобразования на скаляр, матрица также умножается на скаляр.

Доказательство:

Пусть $\varphi(e) = eA$, $f(e) = eB$ в базисе e .

$(\varphi + f)(e) = \varphi(e) + f(e) = eA + eB = e(A + B)$.

$\varphi(f(e)) = \varphi(eB) = e(BA)$.

$\lambda\varphi(e) = \lambda eA = e(\lambda A)$. ■

35 Подобные матрицы

Def. (Подобные матрицы)

Квадратные матрицы A и B порядка n над полем P называются подобными, если существует невырожденная матрица S размера $n \times n$ над полем P , что выполняется равенство:

$$B = S^{-1}AS$$

Матрица S в данном случае называется **трансформирующей матрицей**.

Th. (Подобие матриц линейного преобразования)

Матрицы одного и того же линейного преобразования в двух различных базисах подобны.

Доказательство:

Рассмотрим линейное преобразование φ в двух базисах $U = (u_1, u_2, \dots, u_n)$ и $V = (v_1, v_2, \dots, v_n)$.

Имеем: $\varphi(U) = UA$, $\varphi(V) = VB$, - где A и B матрицы линейного преобразования в базисах U и V соответственно. Через S обозначим матрицу перехода от одного базиса к другому: $V = US$.

С одной стороны имеем $\varphi(V) = \varphi(U) \cdot S = UAS$, с другой стороны же $\varphi(V) = VB = USB$. То есть получаем $USB = UAS \Rightarrow U(SB - AS) = 0 \Rightarrow SB = AS \Rightarrow B = S^{-1}AS$. ■

Th. (Связь с линейным преобразованием)

Если различные матрицы A и B порядка n подобны, то существует линейный оператор, для которого A и B являются матрицами линейного оператора в разных базисах.

Доказательство:

Пусть матрица S - трансформирующая матрица для матриц A и B .

Как известно, для каждой невырожденной матрицы существует линейное преобразование, для которого она является матрицей линейного преобразования. Рассмотрим линейное преобразование $\varphi : V_n \rightarrow V_n$ и базис $U = (u_1, u_2, \dots, u_n)$, такой что $\varphi(U) = UA$.

Теперь рассмотрим базис $V = US$, данная строка также будет базисом, т.к. получена умножением базисной строки на невырожденную матрицу. Пусть $\varphi(V) = VX$. Докажем, что $X = B$. Для этого аналогично прошлой теореме распишем $\varphi(V) = \varphi(U) \cdot S = UAS$, с другой стороны $\varphi(X) = VX = USX \Rightarrow U(AS - SX) = 0 \Rightarrow A = SXS^{-1} \Rightarrow X = B$. ■

1. Отношение подобия симметрично, рефлексивно и транзитивно.

Доказательство:

$$1.1 \ A = SBS^{-1}$$

$$1.2 \ A = E^{-1}AE$$

$$1.3 \ B = S^{-1}AS, \ C = T^{-1}BT \Rightarrow C = T^{-1}S^{-1}AST = (ST)^{-1}A(ST).$$

2. Определители подобных матриц равны.

Доказательство:

$$|B| = |S^{-1}AS| = |S^{-1}| \cdot |A| \cdot |S| = |S^{-1}S| \cdot |A| = |E| \cdot |A| = |A|.$$

3. Единичная матрица подобна лишь самой себе.

Доказательство:

$$S^{-1}ES = S^{-1}SE = E \cdot E = E \text{ (Единичная матрица перестановочна).}$$

4. Скалярная матрица подобна лишь самой себе.

5. Ранги подобных матриц равны.

Доказательство:

$$\text{rank}(A) \geq \text{rank}(S^{-1}A) \geq \text{rank}(S^{-1}AS) = \text{rank}(B)$$

$$\text{rank}(B) \geq \text{rank}(SB) \geq \text{rank}(SBS^{-1}) = \text{rank}(A)$$

$$\text{rank}(B) \geq \text{rank}(A) \text{ и } \text{rank}(A) \geq \text{rank}(B), \text{ то есть } \text{rank}(A) = \text{rank}(B).$$

6. Характеристические многочлены подобных матриц равны.

Доказательство:

$$\text{Пусть } B = S^{-1}AS. \text{ Тогда } |B - \lambda E| = |S^{-1}AS - \lambda E| = |S^{-1}AS - S^{-1}\lambda ES| = |S^{-1}S(A - \lambda E)| = |S^{-1}| \cdot |A - \lambda E| \cdot |S| = |A - \lambda E|.$$

36 Характеристическая матрица и характеристический многочлен

Def. (Характеристическая матрица и характеристический многочлен)

Рассмотрим линейное преобразование $\varphi : V_n \rightarrow V_n$ с матрицей линейного преобразования A в базисе $e = (e_1, e_2, \dots, e_n)$. Обозначим через U координатный столбец собственного вектора u преобразования φ в базисе e .

Тогда получаем $AU = \lambda U \Rightarrow (A - \lambda E_n)U = 0$.

Матрица $(A - \lambda E_n)$ называется **характеристической матрицей** линейного оператора φ (матрицы A).

Понятно, что уравнение относительно собственного вектора $(A - \lambda E_n)U = 0$ имеет ненулевое решение тогда и только тогда, когда $|A - \lambda E_n| = 0$.

Многочлен $f(\lambda) = |A - \lambda E_n|$ называется **характеристическим многочленом** оператора f (характеристическим многочленом матрицы A).

Иногда характеристическим многочленом называют многочлен $|\lambda E_n - A|$.

1. Характеристический многочлен всегда отличен от нуля, а его степень равна n .

$$\deg f(x) = \dim V = n.$$

2. $f(0) = \pm |A|$.

3. $|A| \neq 0 \Leftrightarrow f(0) \neq 0$

4. Характеристические многочлены подобных матриц равны.

Доказательство:

Пусть $B = S^{-1}AS$. Тогда $|B - \lambda E| = |S^{-1}AS - \lambda E| = |S^{-1}AS - S^{-1}\lambda ES| = |S^{-1}S(A - \lambda E)| = |S^{-1}| \cdot |A - \lambda E| \cdot |S| = |A - \lambda E|$.

5. Для квадратной матрицы A порядка $k + m$ выполняется $|A - \lambda E_{k+m}| = |A_{k \times k} - \lambda E_k| \cdot |A_{m \times m} - \lambda E_m|$

$$A = \left(\begin{array}{c|c} A_{k \times k} - \lambda E_k & O \\ \hline B & A_{m \times m} - \lambda E_m \end{array} \right)$$

Доказательство:

По теореме Лапласа имеем: $|A - \lambda E_{k+m}| = |A_{k \times k} - \lambda E_k| \cdot |A_{m \times m} - \lambda E_m| - \underbrace{|O| \cdot |B|}_{=0} = |A_{k \times k} - \lambda E_k| \cdot |A_{m \times m} - \lambda E_m|$.

37 Собственные векторы и собственные значения линейного преобразования

Def. (Собственный вектор линейного преобразования)

Пусть задано линейное преобразование $\varphi : V_n \rightarrow V_n$.

Ненулевой вектор x называется собственным вектором линейного преобразования φ , отвечающим собственному значению λ , если $\varphi(x) = \lambda x$.

Примеры собственных векторов

1. $\varphi = e, e(V) = 1 \cdot V$.

2. φ - нулевой, $\varphi(V) = 0 = 0 \cdot V$.

Def. (Собственное значение линейного преобразования)

Собственные значение линейного преобразования φ - корни характеристического многочлена, принадлежащие основному полю.

Собственные векторы, отвечающие данному собственному значению, образуют ядро преобразования $\ker(\varphi - \lambda e)$ (является решением ОСЛУ $(A - \lambda E)X = 0$).

Алгоритм нахождения собственных векторов

1. Находим корни λ : $|A - \lambda E| = 0$.

2. Решаем ОСЛУ $(A - \lambda E)X = 0$ при найденных ранее значениях λ .

Th. (Критерий диагональности матрицы)

Матрица линейного преобразования в базисе E будет диагональной тогда и только тогда, когда базис E состоит из собственных векторов этого преобразования.

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \Leftrightarrow \begin{cases} \varphi(e_1) = \lambda_1 e_1 \\ \varphi(e_2) = \lambda_2 e_2 \\ \dots \\ \varphi(e_n) = \lambda_n e_n \end{cases}$$

Следствие

Квадратная матрица подобна диагональной \Leftrightarrow у соответствующего матрице линейного преобразования существует базис, состоящий из собственных векторов.

Th. (Линейная независимость собственных векторов)

Собственные векторы, отвечающие попарно различным собственным значениям, линейно независимы.

Доказательство:

Рассмотрим собственные векторы v_1, v_2, \dots, v_n , отвечающие попарно различным собственным значениям. Допустим противное: пусть они линейно зависимы. Тогда v_1 линейно выражается через остальные векторы: $v_1 = \alpha_2 v_2 + \dots + \alpha_n v_n$.

С одной стороны, $\lambda_1 v_1 = \lambda_1 \alpha_2 v_2 + \dots + \lambda_1 \alpha_n v_n$.

С другой стороны, $\lambda_1 v_1 = \varphi(v_1) = \varphi(\alpha_2 v_2 + \dots + \alpha_n v_n) = \alpha_2 \varphi(v_2) + \dots + \alpha_n \varphi(v_n) = \alpha_2 \lambda_2 v_2 + \dots + \alpha_n \lambda_n v_n$.

Тогда рассмотрим разность полученных представлений $\lambda_1 v_1$: $0 = \alpha_2(\lambda_1 - \lambda_2)v_2 + \dots + \alpha_n(\lambda_1 - \lambda_n)v_n \Rightarrow \alpha_2(\lambda_1 - \lambda_2) = \alpha_3(\lambda_1 - \lambda_3) = \dots = \alpha_n(\lambda_1 - \lambda_n) = 0$, и, так как существует $\alpha_i > 0$, то получим $\lambda_1 = \lambda_i$ - противоречие. ■

Следствие

Если матрица $A_{n \times n}$ содержит n характеристических чисел, то она подобна диагональной.

38 Основные свойства делимости в кольце целых чисел

Def. (Делимость целых чисел)

Говорят, что число $b \in \mathbb{Z} \setminus \{0\}$ делит число $a \in \mathbb{Z}$ (a делится на b), если существует число $c \in \mathbb{Z}$ такое, что $a = bc$.

b делит a обозначается $b \mid a$.

a делится на b обозначается $a : b$.

Th. (Деление с остатком)

$\forall (a \in \mathbb{Z}, b \in \mathbb{N}) \exists! q, r \mid a = bq + r, 0 \leq r < b$.

Доказательство:

Возьмем максимальный q такой, что $bq \leq a$, тогда $r = a - bq \Rightarrow 0 \leq a - bq < b$.

Докажем, что данное представление единственно.

Пусть $a = bq_1 + r_1 = bq_2 + r_2$. Тогда $b(q_1 - q_2) = r_2 - r_1 \Rightarrow |b||q_1 - q_2| = |r_2 - r_1|$. Если $q_1 \neq q_2$, то $|q_1 - q_2| \geq 1 \Rightarrow |r_2 - r_1| \geq b$ - противоречие, тогда $q_1 = q_2, r_1 = r_2$. ■

Свойства делимости

1. $a \mid b, a \mid c \Rightarrow a \mid (b \pm c)$

Доказательство:

$$b = aq_1, c = aq_2 \Rightarrow b \pm c = a(q_1 \pm q_2).$$

2. $a \mid b \Rightarrow a \mid bc$

Доказательство:

$$b = aq \Rightarrow bc = a(qc).$$

3. $a \mid b, b \mid a \Rightarrow a = \pm b$

Доказательство: $b = aq_1, a = bq_2 \Rightarrow b = bq_1q_2 \Rightarrow q_1q_2 = 1 \Rightarrow q_1 = q_2 = \pm 1$.

Def. (Наибольший общий делитель)

Наибольшим общим делителем (НОД) чисел a_1, a_2, \dots, a_n называется наибольшее из чисел, делящих одновременно каждое из чисел a_1, a_2, \dots, a_n . НОД обозначается (a_1, a_2, \dots, a_n) .

Свойства:

1. $(0, 0, \dots, 0)$ не определен.

2. $(a, 0, \dots, 0) = |a|, a \neq 0$.

3. $a \mid b \Rightarrow (a, b) = a$.

4. $a = bq + r \Rightarrow (a, b) = (b, r)$

Доказательство:

$$d \mid a, d \mid b \Rightarrow d \mid r; d \mid b, d \mid r \Rightarrow d \mid a.$$

Def. (Наименьшее общее кратное)

Наименьшим общим кратным (НОК) чисел a_1, a_2, \dots, a_n называется наименьшее положительное число, которое делится на каждое из чисел a_1, a_2, \dots, a_n .

Алгоритм Евклида

Алгоритм основан на последнем свойстве НОД.

$$d = (a, b) = (b, r) = (r, r_1) = \dots = (r_{n-1}, r_n) = (r_n, 0) \Rightarrow d = r_n.$$

$$a = bq + r, b = rq_1 + r_1, r = r_1q_2 + r_2, \dots, r_{n-1} = r_nq_{n+1} + r_{n+1}, r_n = r_{n+1}q_{n+2}.$$

Алгоритм продолжается до тех пор, пока не поделится нацело, НОДом будет последний ненулевой остаток.

Th. (Представление НОД)

Пусть $d = (a, b)$. Тогда существуют $u, v \in \mathbb{Z}$ такие, что $d = au + bv$.

Доказательство:

Рассмотрим множество $M = \{ax + by, x, y \in \mathbb{Z}\}$. Данное множество не пусто в силу того, что $a, b \in M$.

Заметим, что остаток от деления любых двух чисел этого множества также принадлежит этому множеству. Пусть $k = a\alpha_1 + b\beta_1, l = a\alpha_2 + b\beta_2, k = lq + r$.

Тогда $r = a(\alpha_1 - \alpha_2q) + b(\beta_1 - \beta_2q) \Rightarrow r \in M$. Рассмотрим наименьший положительный элемент d_0 множества M . Из вышеописанных рассуждений получаем, что любой элемент из M , в частности a и b , делится на d_0 без остатка. То есть $d_0 = d$. ■

Данное разложение получается при помощи обратного алгоритма Евклида.

39 Основные свойства сравнений

Def. (Сравнение чисел по модулю)

Говорят, что $a, b \in \mathbb{Z}$ сравнимы по модулю $m \in \mathbb{N}$, $m > 1$, если a и b имеют одинаковые остатки при делении на m . Записывается так: $a \equiv b \pmod{m}$.

Свойства сравнений

1. $a \equiv a \pmod{m}$ - **рефлексивность**.
2. $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$ - **симметричность**.
3. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ - **транзитивность**.
4. Сравнения по фиксированному модулю можно почленно складывать.
 $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$.

Доказательство:

Достаточно доказать, что $m \mid (a + c) - (b + d)$.

$$m \mid (a - b), m \mid (c - d) \Rightarrow m \mid (a + c) - (b + d) = (a - b) + (c - d).$$

5. Сравнения по фиксированному модулю можно почленно перемножать.
 $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Доказательство:

Пусть $a = mq_1 + r_1, b = mq_2 + r_1, c = mq_3 + r_2, d = mq_4 + r_2$.

$$\text{Тогда } ac = m(mq_1q_3 + r_1q_3 + r_2q_1) + r_1r_2, bd = m(mq_2q_4 + q_2r_2 + q_4r_1) + r_1r_2 \Rightarrow ac \equiv bd.$$

6. Обе части сравнения можно умножать на одно и то же число.
 $a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{m}$. Следует из 1) и 5)
7. Обе части сравнения и модуль можно умножать на одно и то же число.
 $a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{mk}$.
8. Обе части сравнения и модуль можно сокращать на одно и то же число.
 $ak \equiv bk \pmod{mk} \Rightarrow a \equiv b \pmod{m}$. Следует из 7)
9. К обеим частям сравнения можно добавлять одно и то же число.
 $a \equiv b \pmod{m} \Leftrightarrow a + k \equiv b + k \pmod{m}$. Следует из 1) и 4)
10. Обе части сравнения можно сокращать на число, взаимно простое с модулем.
 $ak \equiv bk \pmod{m}, (m, k) = 1 \Rightarrow a \equiv b \pmod{m}$.

Доказательство:

$$m \mid (ak - bk) \Rightarrow m \mid k(a - b), (m, k) = 1 \Rightarrow m \mid (a - b) \Rightarrow a \equiv b \pmod{m}.$$

11. $a \equiv b \pmod{m}, d \mid a, d \mid m \Rightarrow d \mid b$.

Доказательство:

$$m \mid a - b \Rightarrow d \mid a - b, \text{ в то же время } d \mid a, \text{ поэтому } d \mid b.$$

12. $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

Доказательство:

$a - b = qt \Rightarrow a = b + qt, b = a - qt$, следовательно, всякий делитель b и m также является делителем a , аналогично любой делитель a и m является делителем b .

40 Классы вычетов

Def. (Класс вычетов)

Классом вычетов по модулю m называется множество всех чисел, дающих одинаковый остаток при делении на m .

Класс вычетов называется **взаимно простым с модулем**, если любой его вычет взаимно прост с модулем.

Для m классы вычетов записывают так: $\overline{0}, \overline{1}, \dots, \overline{m-1}$.

Свойства вычетов

1. $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \pmod{m}$.

2. Классы вычетов либо равны, либо не пересекаются.

$$\overline{a} \cap \overline{b} = \emptyset \text{ либо } \overline{a} = \overline{b}.$$

3. $a \not\equiv b \Rightarrow \overline{a} \cap \overline{b} = \emptyset$

Def. (Полная система вычетов)

Полной системой вычетов по модулю m называют набор из m чисел, попарно несравнимых по модулю m .

Полная система вычетов по модулю m называется **наименьшей неотрицательной**, если она состоит из чисел $0, 1, \dots, m-1$.

Def. (Приведенная система вычетов)

Приведенной системой вычетов по модулю m называется система вычетов, полученная из полной вычеркиванием вычетов, не взаимно простых с m .

Def. (Пробегание)

Говорят, что переменная x пробегает по множеству X , если она принимает каждое значение из множества X ровно по одному разу.

Th. (Первая лемма о пробегании)

Пусть x пробегает полную систему вычетов по модулю m и $(a, m) = 1$. Тогда $ax + b$ также пробегает полную систему вычетов по модулю m .

Доказательство:

Допустим противное: пусть в системе вычетов $ax + b$ есть сравнимые числа:

$$ax_1 + b \equiv ax_2 + b \pmod{m}.$$

Тогда, учитывая, что $(a, m) = 1$, следует, что $x_1 \equiv x_2 \pmod{m}$ - противоречие в силу того, что x принимает значения из системы вычетов по одному разу.

Th. (Вторая лемма о пробегании)

Пусть $(a, m) = 1$. Величина x пробегает приведенную систему вычетов по модулю m тогда и только тогда, когда ax пробегает эту же систему.

Доказательство:

Для каждого значения x_i можем поставить в соответствие значение ax_i , так как в силу взаимной простоты коэффициента a и модуля m выполняется $x_i \equiv ax_i \pmod{m}$. ■

41 Функция Эйлера, RSA-криптосистема

Def. (Функция Эйлера)

Функцией Эйлера называется функция $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, такая, что $\varphi(m) = M$, где M - число классов вычетов по модулю m , взаимно простых с m .

Свойства:

1. $\varphi(p) = p - 1$, p - простое.
2. $\varphi(p^k) = p^k - p^{k-1}$.

Th. (Мультипликативность функции Эйлера)

$$(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$$

Доказательство:

Рассмотрим произвольное $z \leq ab$. Обозначим через x и y остатки от деления z на a и b соответственно. Так как $(a, b) = 1$, то z взаимнопросто с ab тогда и только тогда, когда оно взаимнопросто с a и b по отдельности, что равносильно взаимной простоте a с x и b с y . Из китайской теоремы об остатках следует, что каждой паре (x, y) взаимно однозначно соответствует число $z \leq ab$.

Число различных x и y взаимно простых с a и b соответственно равняется $\varphi(a)$ и $\varphi(b)$. Поэтому искомое число различных z равняется $\varphi(a)\varphi(b)$. ■

Th. (Теорема Эйлера)

$$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

Доказательство:

Рассмотрим приведенную систему вычетов по модулю $m : (x_1, x_2, \dots, x_{\varphi(m)})$. Теперь рассмотрим все произведения вида $x_i a$. Заметим, что $x_i a$ также взаимнопросто с m , так как $(a, m) = 1$. Поэтому каждому произведению вида $x_i a$ можем поставить в соответствие x_j , причем данное соответствие взаимно однозначно, так как в противном случае нашлись бы такие $i_1 \neq i_2$, что $x_{i_1} a \equiv x_j \equiv x_{i_2} a \Rightarrow x_{i_1} \equiv x_{i_2}$, а данное равенство не может быть выполнено, так как мы рассматриваем приведенную систему вычетов.

Перемножим все различные ранее рассматриваемые произведения: $x_1 x_2 \times \dots \times x_{\varphi(m)} a^{\varphi(m)} \equiv x_1 x_2 \times \dots \times x_{\varphi(m)} \pmod{m} \Rightarrow x_1 x_2 \times \dots \times x_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$. ■

RSA-криптосистема

Выберем число $n = pq$ такое, что p и q - два больших простых числа. Факторизацию знает только дилер. Для такого n функция Эйлера принимает значение $c = \varphi(n) = (p-1)(q-1)$. Открытый ключ шифрования e генерируется такой, что $(e, c) = 1$.

Закрытый ключ шифрования d берется такой, что $d \equiv e^{-1} \pmod{\varphi(n)}$.

Вычислить закрытый ключ, зная открытый, можно лишь решив задачу о факторизации числа n , что занимает огромное время при достаточно больших p и q .

Процесс шифрования: $x \rightarrow x^e \pmod{n}$.

Процесс дешифрования: $x^e \rightarrow x^{ed} \equiv x^{1+kc} \equiv x \cdot (x^{\varphi(n)})^k \equiv x \pmod{n}$.

42 Сравнения и системы сравнений первой степени

Th. (Разрешимость сравнения первой степени)

Сравнение $ax \equiv b \pmod{m}$ разрешимо и имеет единственное решение по модулю $\frac{m}{d}$ тогда и только тогда, когда $d \mid b$, где $d = (a, m)$.

Доказательство:

$m \mid (ax - b)$, $d \mid m$, $d \mid ax \Rightarrow d \mid b$ - необходимость доказана.

Пусть $d \mid b$, тогда сократим обе части сравнения и модуль на d .

Получим $a'x \equiv b' \pmod{m'}$, $(a', m') = 1$.

Это сравнение разрешимо и имеет единственное решение по первой лемме о пробегании. ■

Алгоритмы решения

1. Перебор по полной системе вычетов по модулю m .

2. **Теорема Эйлера**

Умножим обе части на a^{c-1} , где $c = \varphi(m)$. $a^c x \equiv a^{c-1} b \pmod{m} \Rightarrow x \equiv a^{c-1} b \pmod{m}$.

3. **Теорема Евклида**

Найдем такие u и v , что $au + mv = 1 \Rightarrow au \equiv 1 \pmod{m} \Rightarrow a(ub) \equiv b \pmod{m}$.

Алгоритм решения системы сравнений

Рассмотрим произвольную систему сравнений первой степени от одной переменной.

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ a_n x \equiv b_n \pmod{m_n} \end{cases} \Leftrightarrow \begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv c_n \pmod{m_n} \end{cases}$$

Алгоритм заключается в последовательном рассмотрении пары уравнений из системы и сведением их к одному уравнению.

Рассмотрим следующие уравнения: $x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$.

$$\begin{cases} x = c_1 + m_1 t \\ x = c_2 + m_2 t \end{cases} \Rightarrow m_1 t \equiv c_2 - c_1 \pmod{m_2} \Rightarrow (m_1, m_2) \mid (c_2 - c_1).$$

Находим единственное решение по этому модулю $t = t_0 + \frac{m_2}{(m_1, m_2)}$ и подставляем в уравнение:

$$x = \underbrace{c_1 + m_1 t_0}_{= x_0} + \frac{m_1 m_2}{(m_1, m_2)} \Rightarrow x = x_0 \pmod{[m_1, m_2]}.$$

Таким образом вся система постепенно сведется к одному уравнению по модулю НОК при выполнении всех условий разрешимости.

Китайский алгоритм

Имея систему с попарно взаимно простыми модулями, составим вспомогательную систему:

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv c_n \pmod{m_n} \end{cases} \quad \begin{cases} x_1 m_2 \cdot \dots \cdot m_n \equiv 1 \pmod{m_1} \\ m_1 x_2 \cdot \dots \cdot m_n \equiv 1 \pmod{m_2} \\ \dots\dots\dots \\ m_1 m_2 \cdot \dots \cdot m_{n-1} x_n \equiv 1 \pmod{m_n} \end{cases}$$

Ясно видно, что условие разрешимости выполняется для каждого сравнения, тогда

$$x = x_1 m_2 \cdot \dots \cdot m_n c_1 + m_1 x_2 \cdot \dots \cdot m_n c_2 + \dots + m_1 m_2 \cdot \dots \cdot x_n c_n \equiv x_0 \pmod{m_1 m_2 \cdot \dots \cdot m_n}.$$

Th. (Китайская теорема об остатках)

Система сравнений первой степени с попарно взаимно простыми модулями имеет единственное решение по модулю произведения.

43 Первообразные корни

Def. (Первообразный корень)

Число g называется первообразным корнем по модулю m , если

$$g^{\varphi(m)} \equiv 1 \pmod{m}, \quad g^i \not\equiv 1 \pmod{m} \quad \forall i < \varphi(m),$$

где φ — функция Эйлера.

Иными словами, первообразным корнем по модулю m называется такое число g , что все его степени по модулю m пробегает по всем числам, взаимно простым с m .

Th. (Критерий существования первообразных корней)

Первообразные корни могут существовать только по следующим модулям: $2, 4, p^k, 2p^k$, где $p \in \mathbb{P}, p > 2, k \in \mathbb{N}$.

Доказательство:

Любой модуль не из вышеуказанного списка (случай 2^k будет рассмотрен отдельно) можно разложить на два множителя m_1, m_2 так, что $(m_1, m_2) = 1$, $\varphi(m_1), \varphi(m_2)$ — четные числа. Теперь покажем, что первообразного корня существовать не может.

Заметим, что $g^{\varphi(m)/2} = (g^{\varphi(m_1)})^{\varphi(m_2)/2} \equiv 1 \pmod{m_1} \Rightarrow g^{\varphi(m)/2} \equiv 1 \pmod{m}$ — условие минимальности не выполнено.

Теперь докажем, что по модулю $2^k, k > 2$ тоже не существует первообразных корней. Для этого докажем по индукции, что $a^{\frac{\varphi(2^k)}{2}} \equiv a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Несложно убедиться, что при $k = 3$ данное сравнение выполняется.

Предположим, что $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Докажем, что $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

Рассмотрим это сравнение:

$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \Leftrightarrow a^{2^{k-1}} - 1 \equiv 0 \pmod{2^{k+1}} \Leftrightarrow (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1) \equiv 0 \pmod{2^{k+1}}$. Из предположения получаем, что либо $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$, либо $a^{2^{k-1}} \equiv 2^k \pmod{2^{k+1}}$.

В первом случае сразу получаем желаемое, во втором же случае получаем, что $a^{2^{k-2}} + 1 \equiv 2^k + 2 \pmod{2^{k+1}}$. Используем это в неравенстве и получим $(a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1) \equiv 2^k(2^k + 2) \equiv 2^{2k} + 2^{k+1} \equiv 0 \pmod{2^{k+1}}$, что и требовалось доказать. ■

Th. (Критерий для поиска первообразного корня)

Число g является первообразным корнем по модулю $m \Leftrightarrow g^{\varphi(m)} \equiv 1 \pmod{m}$ и $\forall p \mid \varphi(m)$ выполняется $g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$.

Доказательство:

Если g — первообразный корень, то по определению все выполняется. Теперь покажем, что выполнение данных сравнений для числа g означает, что оно является первообразным корнем.

Допустим противное: пусть условия выполнены для g , но оно не является первообразным корнем. Рассмотрим $k = \text{ord}_m(g)$ — показатель (порядок) числа g по модулю m . По определению, $g^k \equiv 1 \pmod{m}$, также $k \mid \varphi(m)$. Получаем, что существует p делитель $\varphi(m)$, для которого $g^p \equiv 1 \pmod{m}$ — противоречие. ■

44 Показатели и их свойства

Def. (Показатель числа)

Показателем (порядком) числа a по модулю m называется наименьшее натуральное число δ такое, что $a^\delta \equiv 1 \pmod{m}$.

$$a^k \equiv 1 \pmod{m} \Rightarrow k \geq \delta = \text{ord}_m(a).$$

Свойства показателя

1. $a^c \equiv 1 \pmod{m} \Rightarrow \delta \mid c$

Доказательство:

Пусть $c = \delta \cdot q + r$, $0 \leq r < \delta$. $a^c = (a^\delta)^q \cdot a^r \equiv 1 \cdot a^r \equiv 1 \pmod{m} \Rightarrow r = 0 \Rightarrow \delta \mid c$.

2. $\delta \mid \varphi(m)$

Доказательство:

$a^{\varphi(m)} \equiv 1 \pmod{m}$ - теорема Эйлера. Далее аналогично 1)

3. Числа $(a^1, a^2, \dots, a^{\delta-1})$ попарно не сравнимы по модулю m .

Доказательство:

Допустим противное: пусть $a^i \equiv a^j \pmod{m}$, $j < i < \delta$.

В таком случае $a^{i-j} \equiv 1 \pmod{m} \Rightarrow$ условие минимальности не выполняется.

4. $\text{ord}_m(a) = \delta_1$, $\text{ord}_m(b) = \delta_2$, $(\delta_1, \delta_2) = 1 \Rightarrow \text{ord}_m(ab) = \delta_1 \delta_2$

Доказательство:

Пусть $\text{ord}_m(ab) = \delta$. Тогда должно выполняться $\delta_1 \mid \delta$ и $\delta_2 \mid \delta$.

Учитывая, что $(\delta_1, \delta_2) = 1$, получаем $\delta = \delta_1 \delta_2$.

$$ab^{\delta_1 \delta_2} = (a^{\delta_1})^{\delta_2} \cdot (b^{\delta_2})^{\delta_1} \equiv 1^{\delta_2} \cdot 1^{\delta_1} \pmod{m} \equiv 1 \pmod{m}.$$

5. $\text{ord}_m(a) = \delta_1$, $\text{ord}_m(b) = \delta_2 \Rightarrow \text{ord}_m(ab) = [\delta_1, \delta_2]$

6. $\text{ord}_m(a) = \delta \Rightarrow \text{ord}_m(a^k) = \frac{\delta}{(\delta, k)}$

Доказательство:

Рассмотрим произвольное $k \in \mathbb{Z}$.

Нужно найти минимальное l , при котором $(a^k)^l \equiv 1 \pmod{m}$.

Пусть $(a^k)^l = a^{kl} \equiv 1 \pmod{m}$. В то же время $\delta \mid kl$ и $a^{\frac{kl}{\delta}} \equiv 1 \pmod{m}$. Сократим числитель и знаменатель дроби на (δ, k) . Необходимо, чтобы $\frac{\frac{k}{(\delta, k)} l}{\frac{\delta}{(\delta, k)}}$ было целым числом, тогда $l \geq \frac{\delta}{(\delta, k)}$. Отсюда минимальное $l = \frac{\delta}{(\delta, k)}$.

1. $f \sim f$ - рефлексивность.
2. $f \sim g \Rightarrow g \sim f$ - симметричность.
 $X = SY \Rightarrow Y = S^{-1}X, |S| \neq 0 \Rightarrow |S^{-1}| \neq 0.$
3. $f \sim g, g \sim h \Rightarrow f \sim h$ - транзитивность.
 $X = SY, Y = KZ \Rightarrow X = (SK)Z.$

Th. (Теорема Лагранжа)

Любая квадратичная форма эквивалентна канонической.

Доказательство:

Будем строить доказательство по индукции. Очевидно, что при $n = 1$ форма каноническая. Сделаем индукционное предположение, что данное утверждение верно для всех $k < n$. Рассмотрим три случая:

1. Все коэффициенты нулевые.

В таком случае матрица является нулевой, а форма, как следствие, канонической.

2. Среди коэффициентов a_{ii} есть хотя бы один отличный от нуля.

Не нарушая общности, пусть $a_{11} \neq 0$. Перепишем форму в виде $f(x_1, x_2, \dots, x_n) = (a_{11}x_1^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + \dots + 2a_{1n}x_1x_n) + f_1(x_2, \dots, x_n) = \frac{1}{a_{11}}(a_{11}x_1 + \dots + a_{1n}x_n)^2 + f_2(x_2, \dots, x_n).$

По индукционному предположению все формы порядка меньше n эквивалентны канонической, поэтому $f_2(x_2, \dots, x_n) \sim g_2(y_2, \dots, y_n)$, где $g_2(y_2, \dots, y_n)$ - каноническая квадратичная форма, $Y = XS$.

Тогда переменные (x_2, \dots, x_n) заменим согласно преобразованию S , а x_1 заменим на выражение $a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$. После такого преобразования форма примет канонический вид.

3. Все коэффициенты a_{ii} равны 0.

Пусть $a_{ij} \neq 0$. Если все равны 0, то сводится к первому случаю.

Применим следующее преобразование:

$$\begin{cases} y_i = x_i + x_j \\ y_j = x_i - x_j \\ y_k = x_k, \quad k = \overline{1, n}, \quad k \neq i, \quad k \neq j \end{cases}$$

В таком случае форма будет представима в виде $\dots + a_{ij}(y_i^2 - y_j^2) + \dots \Rightarrow$ данная квадратичная форма содержит квадраты переменных, а значит, в силу второго случая, она эквивалентна канонической. ■

46 Квадратичные вычеты и криптосистема Рабина

Def. (Квадратичный вычет)

Число a называется квадратичным вычетом по модулю $p \in \mathbb{P}$, $p > 2$ если разрешимо сравнение $x^2 \equiv a \pmod{p}$.

Записывают $\left(\frac{a}{p}\right) = 1$, если a - квадратичный вычет по модулю p , в противном случае $\left(\frac{a}{p}\right) = -1$. Запись вида $\left(\frac{a}{p}\right)$ называется **символом Лежандра**.

Th. (Количество квадратичных вычетов)

Количество квадратичных вычетов в приведенной системе вычетов по модулю p равно количеству неквадратичных в этой же системе и равняется $\frac{p-1}{2}$.

Доказательство:

Заметим, что $x^2 \equiv (p-x)^2 \pmod{p}$. Отсюда следует, что квадратичных вычетов не более, чем $\frac{p-1}{2}$. Осталось доказать, что среди чисел $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ нет сравнимых по модулю p . Допустим противное: пусть $x^2 \equiv y^2 \pmod{p} \Rightarrow (x+y)(x-y) \equiv 0 \pmod{p}$. Однако $x \neq y$ и $x+y < p$, поэтому данное равенство невозможно. ■

Th. (Критерий Эйлера)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Доказательство:

Докажем, что если сравнение $x^2 \equiv a \pmod{p}$ разрешимо, то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и наоборот. $x^2 \equiv a \pmod{p} \Rightarrow x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$.

По малой теореме Ферма получаем: $x^{p-1} \equiv 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Также имеем, что уравнение $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ имеет минимум $\frac{p-1}{2}$ различных корней. В то же время данное уравнение не может иметь более $\frac{p-1}{2}$ различных корней. То есть всякий квадратичный вычет является решением уравнения $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и наоборот, что и требовалось доказать. ■

Квадратичный закон взаимности

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}$$

Криптосистема Рабина

Берется два больших простых числа p, q . Желательно, чтобы выполнялось $p \equiv q \equiv 3 \pmod{4}$, так как сильно ускоряет процесс дешифровки.

Вычисляется открытый ключ $N = pq$.

Закрытым ключом является разложение N - сами числа p, q .

Процесс шифрования: $x \rightarrow x^2 \pmod{N}$.

Процесс дешифрования заключается в извлечении квадратного корня.

Взлом системы Рабина эквивалентен факторизации RSA.

47 Индексирование и протокол Диффи-Хеллмана

Def. (Индекс)

Пусть m - модуль, по которому существует первообразный корень g .
Рассмотрим приведенную систему вычетов по модулю m : $(1, g, g^2, \dots, g^{\varphi(m)-1})$.

Индексом числа a по модулю m при основании g называется такое число i , что $a \equiv g^i \pmod{m}$, то есть $i = \text{ind}_g a \pmod{m} = DL a \pmod{m}$ - дискретный логарифм от a .

Свойства индекса

$$1. \text{ind}_g ab \pmod{c} = \text{ind}_g a \pmod{c} + \text{ind}_g b \pmod{c}$$

Доказательство:

$$a \equiv g^i \pmod{c}, b \equiv g^j \pmod{c} \Rightarrow ab \equiv g^{i+j} \pmod{c}.$$

$$2. \text{ind}_g a^n \pmod{c} \equiv n(\text{ind}_g a \pmod{c}) \pmod{c}$$

Протокол Диффи-Хеллмана

Данный протокол генерирует общий секретный ключ для двух пользователей.
Пусть есть два пользователя: Алиса и Боб.

1. Берется большое простое число p и первообразный корень g по модулю p .
2. Алиса выбирает число α , а Боб число β .
3. Алиса отправляет Бобу число $A = g^\alpha \pmod{p}$, а Боб отправляет ей число $B = g^\beta \pmod{p}$.
4. Алиса вычисляет $B^\alpha \pmod{p} \equiv g^{\alpha\beta} \pmod{p}$, а Боб вычисляет $A^\beta \pmod{p} \equiv g^{\alpha\beta} \pmod{p}$.

Алиса и Боб получили одинаковое число, оно и будет закрытым ключом.

Злоумышленник не может за разумное время вычислить ключ шифрования, зная числа, которые отправляли Алиса и Боб, если p, α, β выбраны достаточно большими.

48 Процесс ортогонализации

Def. (Евклидово пространство)

Пространство V_n называется евклидовым, если $\forall a, b \in V_n$ поставлено в соответствие $ab \in \mathbb{R}$, называемое скалярным произведением, и выполнены аксиомы:

1. $ab = ba$
2. $(a + b)c = ac + bc$
3. $(\lambda a)b = \lambda(ab)$
4. $a^2 \geq 0, \quad a^2 = 0 \Leftrightarrow a = \bar{0}$

Th. (Евклидовость пространств)

Любое n -мерное пространство над \mathbb{R} евклидово.

Доказательство:

Пусть (e_1, e_2, \dots, e_n) - базис пространства V_n .

Разложим векторы a и b пространства V_n по базису:

$$a = a_1 e_1 + \dots + a_n e_n, \quad b = b_1 e_1 + \dots + b_n e_n.$$

Зададим скалярное произведение $ab = \sum_{i=1}^n a_i b_i$.

Покажем, что данное произведение удовлетворяет аксиомам:

1. $ab = \sum_{i=1}^n a_i b_i = \sum_{i=1}^n b_i a_i = ba.$
2. $(a + b)c = \sum_{i=1}^n (a_i + b_i) c_i = \sum_{i=1}^n a_i c_i + \sum_{i=1}^n b_i c_i = ab + bc.$
3. $(\lambda a)b = \sum_{i=1}^n (\lambda a_i) b_i = \lambda \sum_{i=1}^n a_i b_i = \lambda(ab).$
4. $a^2 = \sum_{i=1}^n a_i^2 \geq 0, \quad \sum_{i=1}^n a_i^2 = 0 \Leftrightarrow a = \bar{0}.$

Свойства скалярного произведения

1. $c(a + b) = ca + cb$
 $c(a + b) = (a + b)c = ac + bc = ca + cb.$
2. $a(\lambda b) = \lambda(ab)$
 $a(\lambda b) = (\lambda b)a = \lambda(ba) = \lambda(ab).$
3. $\bar{0}a = \bar{0}$
 $\bar{0}a = (0 \cdot a)a = 0 \cdot (aa) = \bar{0}.$

Def. (Модуль вектора)

Число $|a| = \sqrt{a^2}$ называется модулем вектора a , где a - вектор евклидова пространства V_n .

Свойства модуля

1. $|a| \geq 0, \quad |a| = 0 \Leftrightarrow a = \bar{0}$
2. $|\lambda a| = |\lambda| \cdot |a|$
 $|\lambda a| = \sqrt{\lambda^2 a^2} = \sqrt{\lambda^2} \sqrt{a^2} = |\lambda| \cdot |a|.$

Def. (Угол между векторами)

Углом между векторами a, b евклидова пространства V_n называется число $\varphi \in R$ такое, что $\cos \varphi = \frac{ab}{|a| \cdot |b|}$.

Th. (Свойство евклидова пространства)

Для любых векторов a, b из евклидова пространства V_n выполняется

$$|ab| \leq |a| \cdot |b|$$

Доказательство:

$$|ab| = \left| \sum_{i=1}^n a_i b_i \right| \leq \sum_{i=1}^n (|a_i| \cdot |b_i|) = |a| \cdot |b|. \blacksquare$$

Th. (Неравенство треугольника)

Для любых векторов a, b из евклидова пространства V_n выполняется

$$|a + b| \leq |a| + |b|$$

Доказательство:

$$|a + b|^2 = (a + b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2. \blacksquare$$

Def. (Ортогональность и векторы)

Векторы u и v евклидова пространства называются **ортогональными** (перпендикулярными), если их скалярное произведение $\langle u, v \rangle$ равно 0.

Ортогональность векторов обозначается знаком \perp .

Система векторов называется **ортогональной**, если все её векторы попарно ортогональны, то есть $\langle u_i, v_j \rangle = 0$ при $i \neq j$.

Ортогональная система векторов также называется **ортонормированной**, если длина каждого вектора системы равна 1.

Говорят, что вектор v **ортогонален** (перпендикулярен) системе векторов M , если он ортогонален каждому вектору из M .

Свойства ортогональных векторов

1. $a \perp b \Leftrightarrow b \perp a$
2. $\bar{0} \perp a$
3. $a \perp a \Rightarrow a = \bar{0}$.
 $a^2 = 0 \Rightarrow a = \bar{0}$
4. $b \perp (a_1, a_2, \dots, a_n) \Rightarrow b \perp \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$.
 $(\alpha_1 a_1 + \dots + \alpha_n a_n) b = \alpha_1 (a_1 b) + \alpha_2 (a_2 b) + \dots + \alpha_n (a_n b) = 0.$

Th. (Линейная независимость ортогональной системы)

Ортогональная система векторов (без $\bar{0}$) линейно независима.

Доказательство:

(a_1, a_2, \dots, a_n) - ортогональная система векторов $\Rightarrow a_i a_j = 0, i \neq j; a_i \neq 0, i = \overline{1, n}$.

Допустим, что существуют такие $\alpha_1, \dots, \alpha_n (\sum_{i=1}^n \alpha_i^2 > 0)$, что $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n = 0$.

Пусть $\alpha_i \neq 0$, тогда домножим равенство на a_i и в силу ортогональности системы получим, что $\alpha_i a_i^2 = 0, \alpha_i \neq 0 \Rightarrow a_i = 0$ - противоречие.

Процесс ортогонализации Грама-Шмидта

Дана линейно независимая система векторов (v_1, v_2, \dots, v_n) конечномерного евклидова пространства. Необходимо построить такую ортогональную систему векторов (w_1, w_2, \dots, w_n) , чтобы $L(v_1, v_2, \dots, v_n) = L(w_1, w_2, \dots, w_n)$.

Алгоритм состоит из двух шагов:

1. Положить $w_1 = v_1$.

2. Рекуррентно вычислить векторы по формуле $w_k = v_k - \sum_{i=1}^{k-1} (\alpha_{ki} w_i)$, где $\alpha_{ki} = \frac{\langle v_k, w_i \rangle}{\langle w_i, w_i \rangle}$.

На k -ом шаге мы подбираем коэффициент α_{ki} для каждого вектора w_i такой, чтобы вектор w_k был ортогонален всем ранее записанным векторам.

$$0 = \langle w_k, w_i \rangle = \langle v_k, w_i \rangle - \alpha_{ki} \cdot \langle w_i, w_i \rangle \Rightarrow \alpha_{ki} = \frac{\langle v_k, w_i \rangle}{\langle w_i, w_i \rangle}.$$

Следствие

В евклидовом пространстве V_n всегда можно выбрать ортонормированный базис.

Достаточно выбрать любой базис, ортогонализировать его, затем заменить каждый вектор ортонормированным.

49 Факторизация RSA-модуля с известной секретной экспонентой

Извлечение квадратного корня из 1 по RSA-модулю

$$x^2 \equiv 1 \pmod{pq} \Leftrightarrow x^2 \equiv 1 \pmod{p}, x^2 \equiv 1 \pmod{q}$$

В итоге получаем 4 системы уравнений:

$$\begin{cases} x \equiv 1 \pmod{p} \\ x \equiv 1 \pmod{q} \end{cases} \quad \begin{cases} x \equiv -1 \pmod{p} \\ x \equiv 1 \pmod{q} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{p} \\ x \equiv -1 \pmod{q} \end{cases} \quad \begin{cases} x \equiv -1 \pmod{p} \\ x \equiv -1 \pmod{q} \end{cases}$$

В итоге получаем 4 решения: $x = \pm 1, x = \pm c$.

Th. (Факторизация RSA-модуля)

Зная корень из 1 по RSA-модулю можно факторизовать RSA-модуль.

Доказательство:

$N = pq$ - RSA-модуль, $x^2 \equiv 1 \pmod{N}$ - 4 решения, $x = \pm 1, x = \pm c$.

$c^2 \equiv 1 \pmod{N} \Rightarrow (c-1)(c+1) \equiv 0 \pmod{N} \Rightarrow pq \mid (c-1)(c+1)$. Так как p, q - простые числа, то одно из них делит $c-1$, а другое $c+1$. Не нарушая общности, пусть $p \mid c-1$. Тогда $p = (c-1, N)$. ■

Th. (Алгоритм факторизации)

При известном секретном ключе d существует эффективный алгоритм факторизации RSA-модуля.

Доказательство:

Введем обозначения:

$N = pq$ - модуль.

$p - 1 = 2^{v_1} u_1$, u_1 - нечетное.

$q - 1 = 2^{v_2} u_2$, u_2 - нечетное.

$ed - 1 = S$.

Имеем, что $x^{ed} \equiv x \pmod{pq} \Rightarrow x^{ed-1} \equiv 1 \pmod{pq} \Rightarrow (x^{\frac{S}{2}})^2 \equiv 1 \pmod{pq}$

$x^{\frac{S}{2}} \equiv \pm 1 \pmod{pq}$ - плохо, не дает s .

Если знаем d и e , то знаем корень из 1 \Rightarrow знаем факторизацию. ■

(Плохих x не больше половины - доказывается в следующей лемме)

Лем. (Мощность множества «плохих» x)

Обозначим множество B плохих x :

$$B = \left\{ \begin{array}{l} x : x^u \equiv 1 \pmod{pq} \\ x : x^{2^j u} \equiv -1 \pmod{pq} \end{array} \right.$$

$$|B| \leq \frac{1}{2} \varphi(pq) = \frac{(p-1)(q-1)}{2}.$$

Доказательство:

$$x^u \equiv 1 \pmod{pq} \Leftrightarrow \begin{cases} x^u \equiv 1 \pmod{p} \\ x^u \equiv 1 \pmod{q} \end{cases} \Leftrightarrow \begin{cases} u \cdot \text{ind } x \equiv 0 \pmod{p-1} \\ u \cdot \text{ind } x \equiv 0 \pmod{q-1} \end{cases}$$

Количество решений первого уравнения: $(u, 2^{v_1} u_1) = (u, u_1)$, аналогично количество решений второго уравнения $(u, 2^{v_2} u_2) = (u, u_2)$. По CRT получаем, что всего $K = (u, u_1) \cdot (u, u_2)$ решений для первого уравнения полученной системы множества B .

$$x^{2^j u} \equiv -1 \pmod{pq} \Leftrightarrow \begin{cases} x^{2^j u} \equiv -1 \pmod{2^{v_1} u_1 + 1} \\ x^{2^j u} \equiv -1 \pmod{2^{v_2} u_2 + 1} \end{cases}$$

Ищем $t = \text{ind}(-1)$:

$$g^{p-1} \equiv 1 \pmod{p} \Rightarrow p \mid (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1).$$

Если $p \mid (g^{\frac{p-1}{2}} - 1)$, то $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ - противоречие. Тогда $p \mid (g^{\frac{p-1}{2}} + 1) \Rightarrow g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Получаем $t = \text{ind}(-1) \leq \frac{p-1}{2}$

Пусть $2t < p - 1$, тогда $g^t \equiv -1 \pmod{p} \Rightarrow g^{2t} \equiv 1 \pmod{p} \Rightarrow 2t \geq \frac{p-1}{2}$ - противоречие.

Значит $t = \frac{p-1}{2}$.

Таким образом получаем, что решений первого уравнения системы $(2^j u, 2^{v_1} u_1)$, $j < v_1$, чтобы были решения, аналогично решений второго уравнения системы $(2^j u, 2^{v_2} u_2)$.

Положим, $v_1 \leq v_2$, тогда решений всей подсистемы не больше чем $4^j K$.

Оценим мощность множества B : $|B| = K + 4^j K \leq K + K + 4K + 16K + \dots + 4^{v_1-1} K = (1 + \frac{4^{v_1}-1}{3})K = \frac{4^{v_1}+2}{3} K$.

Покажем, что $(u, u_1) \cdot (u, u_2)(1 + \frac{4^{v_1}-1}{3}) < \frac{1}{2} 2^{v_1} 2^{v_2} u_1 u_2$.

Достаточно показать, что $\frac{4^{v_1}+2}{3} \leq \frac{1}{2} 4^{v_1}$. Для этого умножим обе части неравенства на 6 и получим $2 \cdot 4^{v_1} + 4 \leq 3 \cdot 4^{v_1}$, что очевидно выполняется. ■

50 Сумма и пересечение подпространств

Def. (Сумма и пересечение подпространств)

Рассмотрим два подпространства $W_1, W_2 \subset V$.

Пересечением подпространств называется множество $W_1 \cap W_2 = \{w \mid w \in W_1, w \in W_2\}$.

Суммой подпространств называется множество $W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$.

Th. (Размерность суммы подпространств)

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$$

Th. (Свойство суммы и пересечения подпространств)

Сумма и пересечение подпространств сами являются подпространствами.

Доказательство:

Необходимо доказать 2 аксиомы для суммы и пересечения.

Начнем с пересечения: докажем, что $x_1, x_2 \in W_1 \cap W_2 \Rightarrow x_1 + x_2 \in W_1 \cap W_2$.

$x_1, x_2 \in W_1 \Rightarrow x_1 + x_2 \in W_1$, аналогично $x_1 + x_2 \in W_2 \Rightarrow x_1 + x_2 \in W_1 \cap W_2$.

Теперь докажем, что $x \in W_1 \cap W_2 \Rightarrow \lambda x \in W_1 \cap W_2$.

$x \in W_1 \Rightarrow \lambda x \in W_1$, аналогично $\lambda x \in W_2 \Rightarrow \lambda x \in W_1 \cap W_2$.

Перейдем к сумме: рассмотрим $s_1, s_2 \in W_1 + W_2$.

Докажем, что $s_1 + s_2 \in W_1 + W_2$. По определению суммы можем расписать $s_1 = x_1 + x_2, s_2 = y_1 + y_2, x_1, y_1 \in W_1, x_2, y_2 \in W_2$. Тогда $s_1 + s_2 = x_1 + x_2 + y_1 + y_2 = \underbrace{(x_1 + y_1)}_{\in W_1} + \underbrace{(x_2 + y_2)}_{\in W_2} \Rightarrow$

$s_1 + s_2 \in W_1 + W_2$.

Далее докажем, что $s \in W_1 + W_2 \Rightarrow \lambda s \in W_1 + W_2$. Снова распишем $s = x_1 + x_2, x_1 \in W_1, x_2 \in W_2$. Тогда получаем: $\lambda s = \lambda(x_1 + x_2) = \underbrace{\lambda x_1}_{\in W_1} + \underbrace{\lambda x_2}_{\in W_2} \Rightarrow \lambda s \in W_1 + W_2$. ■

Def. (Прямая сумма подпространств)

Сумма двух подпространств W_1, W_2 называется прямой, если $W_1 \cap W_2 = \bar{0}$.

Прямая сумма обозначается: $W_1 \oplus W_2$.

Th. (Размерность прямой суммы подпространств)

$$\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2)$$

Доказательство:

По теореме о размерности суммы подпространств имеем: $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$. Так как, по определению прямой суммы, $W_1 \cap W_2 = \bar{0}$, получаем, что $\dim(W_1 \cap W_2) = 0$. То есть получаем, что $\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2)$. ■

Следствие

$$\dim(W_1 \oplus W_2 \oplus \dots \oplus W_n) = \dim(W_1) + \dim(W_2) + \dots + \dim(W_n)$$

Th. (Разложение на одномерные подпространства)

Всякое пространство раскладывается на сумму одномерных подпространств.

Доказательство:

Пусть пространство V_n имеет базис (e_1, e_2, \dots, e_n) .

Тогда несложно догадаться, что $V_n = L(e_1) \oplus L(e_2) \oplus \dots \oplus L(e_n)$. Данная сумма является и прямой, так как базис линейно независим по определению, также любой вектор пространства V_n линейно выражается через пространство, выраженное прямой суммой, так как сам вектор расписывается по базису (e_1, e_2, \dots, e_n) . ■

Th. (Дополнение подпространства)

У любого подпространства есть прямое дополнение.

$$\forall W \subset V_n \exists U \subset V_n \mid V_n = U \oplus W$$

Доказательство:

Пусть W имеет базис (e_1, e_2, \dots, e_r) . Как известно, базис подпространства можно дополнить до базиса всего пространства. Тогда рассмотрим дополнение базиса (e_{r+1}, \dots, e_n) данного подпространства и соответствующее данному базису подпространство $U = L(e_{r+1}, \dots, e_n)$. Заметим, что $W \cap U = \bar{0}$, так как ни один вектор из U не выражается линейно через векторы w .

$W = L(e_1, e_2, \dots, e_r) = L(e_1) \oplus L(e_2) \oplus \dots \oplus L(e_r)$. В то же время имеем, что $V_n = L(e_1) \oplus L(e_2) \oplus \dots \oplus L(e_n)$. То есть можем заключить, что $V_n = W \oplus U$. ■