Д. Дружкин, А. Орехова, А. Стюхина, В. Янченко

Билеты к зачету

Предмет: Алгем

Системы линейных уравнений

Определение системы линейных уравнений

Определение 1. *Системой линейных уравнений* (далее СЛУ) называют систему вида:

$$\begin{cases} a_1^1x_1 + a_1^2x_2 + \ldots + a_n^1x_n = b_1 \\ a_1^2x_1 + a_2^2x_2 + \ldots + a_n^2x_n = b_2 \\ \vdots \\ a_1^mx_1 + a_2^mx_2 + \cdots + a_n^mx_n = b_m, \end{cases} \tag{1}$$

где $a_j^i \in \mathbb{R}$, $b_j \in \mathbb{R}$, m — количество уравнений, n — количество переменных, x_j^i — неизвестные, a_j^i — коэффициенты, b_j — свободные члены.

$A = \begin{pmatrix} a_1^1 & \cdots & a_1^n \\ \vdots & \ddots & \vdots \\ a_1^m & \cdots & a_n^m \end{pmatrix}$ называется *матрицей коэффициентов*

$\tilde{A} = (A \mid B) = \left(\begin{array}{ccc|c} a_1^1 & \cdots & a_n^1 & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_1^m & \cdots & a_n^m & b_m \end{array}\right)$ — *расширенная матрица коэффициентов.*

Пусть $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$.

Тогда СЛУ можно переписать в матричном виде: $AX = B$.

СЛУ

совместные (есть решение) | несовместные (нет решений)

определённые (единственное решение) | неопределённые (более одного решения)

Элементарные преобразования СЛУ и строк матрицы

Определение 2. *Элементарными преобразованиями СЛУ* называются преобразования вида:

1. Прибавление к одному уравнению другое, умноженное на число,
2. Перестановка двух уравнений,
3. Умножение уравнения на число, отличное от нуля.

Метод Гаусса

Определение 3. *Ведущим* элементом ненулевой строки называется её первый ненулевой элемент

Определение 4. Матрица называется *ступенчатой*, если

1. Номера ведущих элементов её ненулевых строк образует строго возрастающую последовательность,
2. Ненулевые строки (если они есть) стоят в конце.

Пример (Ступенчатой матрицы)**.**

$$\begin{pmatrix} 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Теорема 1. *Всякую матрицу путём элементарных преобразований можно привести к ступенчатому виду.*

Определение 5. СЛУ называется *ступенчатой*, если её расширенная матрица ступенчатая

Система однородных линейных уравнений

Определение 6. Система линейных уравнений называется однородной, если все свободные члены уравнений равны нулю:

$$\begin{cases} a_1^1 x_1 + a_1^2 x_2 + \ldots + a_n^1 x_n = 0 \\ a_1^2 x_1 + a_2^2 x_2 + \ldots + a_n^2 x_n = 0 \\ \vdots \\ a_1^m x_1 + a_2^m x_2 + \cdots + a_n^m x_n = 0. \end{cases} \tag{2}$$

Однородная система всегда совместна, поскольку она всегда имеет тривиальное (нулевое) решение.

Теорема 2. *Совокупность всех решений системы однородных линейных уравнений с n неизвестными является подпространством $\mathbb{R}^n$ (в общем случае K^n).*

Совокупность всех решений произвольной совместной СЛУ есть сумма какого-либо одного решения и подпространства решений системы однородных линейных уравнений с той же матрицей коэффициентов.

$\square$ Пусть $\bar{u} = (u_1, \ldots, u_n)$ и $\bar{v} = (v_1, \ldots, v_n)$ — решения 2.
Тогда $\bar{u} + \bar{v}$ — решение 2, так как

$$\overbrace{a_1^1 u_1 + \ldots + a_n^1 u_n}^{0} + \overbrace{a_1^1 v_1 + \ldots + a_n^1 v_n}^{0} = 0.$$

Также $\lambda\bar{u}$ — решение 2, так как

$$\lambda \overbrace{(a_1^1 u_1 + \ldots + a_n^1 u_n)}^{0} = 0.$$

Пусть $\bar{t} = (t_1, \ldots, t_n)$ — решение 1, $\bar{u} = (u_1, \ldots, u_n)$ — решение 2.
Тогда $\bar{t} + \bar{u}$ — решение 1, так как

$$a_1^1(t_1 + u_1) + \ldots + a_n^1(t_n + u_n) = b_1$$
$$\underbrace{a_1^1 t_1 + \ldots + a_n^1 t_n}_{b_1} + \underbrace{a_1^1 u_1 + \ldots + a_n^1 u_n}_{0} = b_1.$$

Пусть $\bar{f}$ — решение 1. Тогда $\bar{p} = \bar{t} - \bar{f}$ — решение 2, так как

$$a_1^1(t_1 - f_1) + \ldots + a_n^1(t_n - f_n) =$$
$$= \underbrace{a_1^1 t_1 + \ldots + a_n^1 t_n}_{b_1} - \underbrace{(a_1^1 f_1 + \ldots + a_n^1 f_n)}_{b_1} = 0$$

$\blacksquare$

Векторное пространтсво

Определение 7. *Векторным пространством* над полем K называется множество V с операциями сложения и умножения на элемент поля K, обладающая следующими свойствами:

1. V — аддитивная абелева группа.
2. $\lambda(a + b) = \lambda a + \lambda b$
3. $(\lambda + \mu)a = \lambda a + \mu a$

4. $\lambda(\mu a) = (\lambda\mu)a$

5. $1 \cdot a = a$

$\lambda, \mu \in K,\ a, b \in V$.

Определение 8. Пусть $S \subset V$. Совокупность всевозможных линейных комбинаций из векторов S называется *линейной оболочкой* множества S. Обозначние: $<S>$.

Пространство V *порождается* множеством S, если $V =<S>$.

Определение 9. Векторное пространство называется *конечномерным*, если оно порождается конечным числом векторов и бесконечномерным в противном случае.

Определение 10. *Базисом* векторного пространства называется упорядоченная максимально линейно независимая система векторов, где каждый вектор пространства линейно выражается через эту систему.

Ранг

Определение 11. Рангом *системы векторов* называется размерность её линейной оболочки.

Ранг *матрицы* — это ранг системы её строк.

Определение 12. Системы векторов $\{\bar{a}_1, \ldots, \bar{a}_n\}$ и $\{\bar{b}_1, \ldots, \bar{b}_m\}$ называются *эквивалентными*, если каждый из векторов $\bar{b}_i$ линейно выражается через $\bar{a}_1, \ldots, \bar{a}_n$ и наоборот, $\bar{a}_j$ линейно выражается через $\bar{b}_1, \ldots, \bar{b}_m$, где $i = 1, \ldots, m$ и $j = 1, \ldots, n$.

Это равносильно $<\bar{a}_1, \ldots, \bar{a}_n>=<\bar{b}_1, \ldots, \bar{b}_n>$.

Теорема 3. *Ранг матрицы равен числу ненулевых строк ступенчатой матрицы, к которой она приводится элементарными преобразованиями строк.*

Линейная зависимость между столбцами матриц не меняется при элементарных преобразований строк. Ранг системы её столбцов не меняется при элементарных преобразований строк.

Ранг системы строк любой матрицы равен рангу системы столбцов этой матрицы.

Теорема 4 (Кронекера-Капелли). *СЛУ совместна* $\Leftrightarrow rk(A|B) = rk\ A$.

□ $\Rightarrow$ Пусть система 1 совместна и $(k_1, \ldots, k_n)$ — решение СЛУ.

$$\begin{pmatrix} a_1^1 \\ a_1^2 \\ \vdots \\ a_1^m \end{pmatrix} k_1 + \begin{pmatrix} a_2^1 \\ a_2^2 \\ \vdots \\ a_2^m \end{pmatrix} k_2 + \ldots + \begin{pmatrix} a_n^1 \\ a_n^2 \\ \vdots \\ a_n^m \end{pmatrix} k_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

Последний столбец расширенной матрицы есть линейная комбинация остальных столбцов с коэффициентами $(k_1, \ldots, k_n)$. Всякий другой столбец расширенной матрицы входит в матрицу A, поэтому линейно выражается через столбцы этой матрицы. Значит система столбцов расширенной матрицы $A|B$ и A эквивалентны $\implies$ $rk(A|B) = rk(A)$.

$\Leftarrow$ $rk(A|B) = rk(A)$ $\implies$ максимальная линейно независимая система столбцов A остаётся линейно независимой и в $A|B$ $\implies$ через эту систему, а значит через систему столбцов матрицы A, линейно выражается последний столбец $A|B$ $\implies$ $\exists (k_1, \ldots, k_n)$:

$$\begin{pmatrix} a_1^1 \\ a_1^2 \\ \vdots \\ a_1^m \end{pmatrix} k_1 + \begin{pmatrix} a_2^1 \\ a_2^2 \\ \vdots \\ a_2^m \end{pmatrix} k_2 + \ldots + \begin{pmatrix} a_n^1 \\ a_n^2 \\ \vdots \\ a_n^m \end{pmatrix} k_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

то есть $(k_1, \ldots, k_n)$ — решение СЛУ $\implies$ СЛУ совместна. ■

Теорема 5. *Совместная СЛУ является определённой* $\Leftrightarrow$ $rk(A)$ *равен числу неизвестных.*

Теорема 6. *Размерность пространства решений СОЛУ с* n *неизвестными и матрицей коэффициентов* A *равняется* $n - rk\ A$.

□ Приводим СОЛУ путём элементарных преобразований к ступенчатому виду.

Число ненулевых уравнений в ступенчатом виде равно $rk(A)$. Общее решение системы содержит n переменных:

$$\begin{cases} x_1 = c_1^1 x_{r+1} + c_2^1 x_{r+2} + \ldots + c_{n-r}^1 x_n \\ x_2 = c_1^2 x_{r+1} + c_2^2 x_{r+2} + \ldots + c_{n-r}^2 x_n \\ \vdots \\ x_r = c_1^r x_{r+1} + c_2^r x_{r+2} + \ldots + c_{n-r}^r x_n. \end{cases}$$

■

Частные решения:

Придавая по очереди одному из свободныъ неизвестных $x_{r+1}, \ldots, x_n$ значения 1, а остальным значения 0, получим решение системы:

$$\begin{array}{l} \bar{u}_1 = (c_1^1, c_1^2, \ldots, c_1^r, 1, 0, \ldots, 0) \\ \bar{u}_2 = (c_2^1, c_2^2, \ldots, c_2^r, 0, 1, \ldots, 0) \\ \vdots \\ \bar{u}_{n-r} = (c_{n-r}^1, c_{n-r}^2, \ldots, c_{n-r}^r, 0, 0, \ldots, 1). \end{array}$$

Докажем, что $\bar{u}_1, \ldots, \bar{u}_{n-r}$ образуют базис пространства решений (это есть ядро линейного отображения см. определение 16).

$\square$ $\bar{u} = \lambda_1\bar{u}_1 + \ldots + \lambda_{n-r}\bar{u}_{n-r}$, $\bar{u}$ — решение системы.

$\bar{0} = \lambda_1\bar{u}_1 + \ldots + \lambda_{n-r}\bar{u}_{n-r} \Leftrightarrow \lambda_1 = \ldots = \lambda_{n-r} = 0 \implies \bar{u}_1, \ldots, \bar{u}_{n-r}$ — линейно независимы.

Значит $(\bar{u}_1, \ldots, \bar{u}_{n-r})$ — базис пространства решений. $\blacksquare$

Определение 13. Всякий базис пространства решений СОЛУ называется *фундаментальной* системой решения.

Линейные оторбажения

Определение 14. Пусть U, V — действительные векторные пространства. *Линейным отображением* называется отображние $\varphi : U \to V$, удовлетворяющая свойствам:

1. $\varphi(\bar{a} + \bar{b}) = \varphi(\bar{a}) + \varphi(\bar{b})$
2. $\varphi(\lambda\bar{a}) = \lambda\varphi(\bar{a})$,

$\lambda \in \mathbb{R}$, $\bar{a}$, $\bar{b} \in U$

В таком случае векторные пространства U и V называются *изоморфными.*

Если U совпадает с V, то φ называется *линейным преобразованием.*

Вспомнив запись СЛУ через матрицы, получаем, что $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ и $\varphi(\bar{x}) = \bar{b}$, где $\bar{x} = (x_1, \ldots, x_n)$ — решение СЛУ.

Пусть A — матрица коэффициентов, тогда A_φ — *матрица линейного отображения.*

Для СОЛУ: $\varphi(\bar{x}) = \bar{0}$,где $\bar{x} = (x_1, \ldots, x_n)$ — решение СОЛУ.

Определение 15. *Образом* линейного отображения $\varphi : U \to V$ называется множество $Im\,\varphi = \{\bar{b} \in V,\ \varphi(\bar{x}) = \bar{b},\ \bar{x} \in U\}$.

Определение 16. *Ядром* линейного отображения $\varphi : U \to V$ называется множество $Ker\ \varphi = \{\bar{x} \in U : \ \varphi\bar{x} = \bar{0}\}$.

Заметим, что $Ker\ \varphi \subset U$ и $Im\ \varphi \subset V$.

Теорема 7. $\varphi(\bar{a}) = \bar{b}$, $\varphi(\bar{x}) = \bar{b}$
$\implies \bar{x} = \bar{x} + Ker\ \varphi$.

Определители и их приложения

Линейные формы

Определение 17. *Линейной функцией* или *линейной формой* на векторном пространстве V называется функция $\alpha: V \to \mathbb{R}$ (в общем виде $\alpha: V \to K$, где K — поле), обладающая следующими свойствами:

1. $\alpha(\bar{x} + \bar{y}) = \alpha(\bar{x}) + \alpha(\bar{y})$
2. $\alpha(\lambda\bar{x}) = \lambda\alpha(\bar{x})$

Определение 18. *Билинейной функцией* или *билинейной формой* на векторном пространстве V называется форма $\alpha : V \times V \to \mathbb{R}$ (паре векторов сопоставляется действительное число), линейная по каждому аргументу, то есть:

1. $\alpha(\lambda_1\bar{x}_1 + \lambda_2\bar{x}_2,\, \bar{y}) = \lambda_1\alpha(\bar{x}_1,\, \bar{y}) + \lambda_2\alpha(\bar{x}_2,\, \bar{y})$
2. $\alpha(\bar{x}, \gamma_1\bar{y}_1 + \gamma_2\bar{y}_2) = \gamma_1\alpha(\bar{x}, \bar{y}_1) + \gamma_2\alpha(\bar{x}, \bar{y}_2)$

Пример. Самый наглядный пример билинейной функции — скалярное произведение.

Для любых функций $f(x)$ и $g(x)$, интегрируемых на отрезке $[a, b]$, функция $I(f, g) = \int\limits_a^b f(x)g(x)\,\mathrm{d}x$ является билинейной функцией на $[a, b]$.

Определение 19. *Скалярным произведением* называется билинейная форма, обладающая свойствами:

1. Симметричность $(\bar{x}, \bar{y}) = (\bar{y}, \bar{x})$
2. Положительная определённость $(\bar{x}, \bar{x}) > 0$ и $(\bar{x}, \bar{x}) = 0 \Leftrightarrow \bar{x} = \bar{0}$

Определитель матрицы n-ого порядка

Пусть V — действительное пространство, функция $f\colon \underbrace{V \times \ldots \times V}_{m} \to \mathbb{R}$.

Определение 20. Функция f называется *полилинейной*, если она линейна по каждому аргументу.

Определение 21. Полилинейная функция называется *кососимметрической*, если при перестановке любых двух аргументов она умножается на -1.

Определение 22. *Определителем* квадратной матрицы $A = (a^i_j)$, $i,\ j = 1, \ldots, n$ называется число

$$det\ A = \sum_{k_1, k_2, \ldots, k_n} sgn(k_1, \ldots, k_n) \cdot a^1_{k_1}\, a^2_{k_2} \ldots a^n_{k_2},$$

где $sgn(k_1, \ldots, k_n)$ — знак перестановки.

Теорема 8. *Определитель является кососимметрической полилинейной функцией строк матрицы*

Всякая функция f на множестве квадратных матриц порядка n, являющаяся кососимметрической полилинейной функцией строк матрицы имеет вид $f(A) = f(E) \cdot det\ A$ в частности, если $f(E) = 1$, то $f(A) = det\ A$.

Определение 23. Матрица A называется *невырожденной*, если определитель матрицы A не равен нулю. ($det\ A \neq 0$).

Теорема 9 (об определителе матрицы с углом нулей)**.** *Пусть $A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix}$, где B и C квадратные матрицы. Тогда $det\ B \cdot det\ C = det\ A$.*

Лемма. $\begin{vmatrix} a^1_1 & \ldots & a^1_j & \ldots & a^1_n \\ 0 & 0 & a^i_j & 0 & 0 \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ a^n_1 & \ldots & a^n_j & \ldots & a^n_n \end{vmatrix} = A^i_j \cdot a^i_j$, *где A^i_j — алгебраическое дополнение элемента a^i_j и вычисляется $A^i_j = (-1)^{i+j} \cdot M^i_j$.*

M^i_j — минор элемента a^i_j.

□ Переставляя строки и столбцы приведем матрицу к виду:

$$\begin{pmatrix} a^i_j & 0 & \ldots & 0 \\ a^1_j & a^1_1 & \ldots & a^1_n \\ \vdots & \vdots & \ddots & \vdots \\ a^n_j & a^n_1 & \ldots & a^n_n \end{pmatrix} = det\ B \cdot det\ C = a^i_j \cdot det\ C = a^i_j A^i_j.$$

(красным отмечена матрица B, синим — C). ■

Некоторые приложения определителя

Теорема 10 (Крамера)**.** *Если определитель матрицы коэффициентов A отличен от нуля, то система*

$$\begin{cases} a_1^1x_1 + a_1^2x_2 + \ldots + a_n^1x_n = b_1 \\ a_1^2x_1 + a_2^2x_2 + \ldots + a_n^2x_n = b_2 \\ \vdots \\ a_1^nx_1 + a_2^nx_2 + \cdots + a_n^nx_n = b_n, \end{cases}$$

имеет единственное решение.

Причем $x_i = \frac{det\ A_i}{det\ A}$, $i = 1, \ldots, n$, где A_i — матрица A, в которой i столбец заменяется на $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

☐ При элементарных преобразованиях системы уравнений в матрицах A и A_i происходит элементарные преобразования строк, следовательно формула Крамера не меняется.

Рассмотрим случай, когда $A = E$. Тогда система имеет вид:

$$\begin{cases} x_1 = b_1 \\ \vdots \\ x_n = b_n \end{cases}$$

$$det\ A_i = \begin{array}{c} \text{i столбец} \\ \downarrow \\ \begin{bmatrix} 1 & 0 & \cdots & b_1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & b_2 & 0 & \cdots & 0 \\ \vdots & \ldots & \ldots & \vdots & \ldots & \ldots & \vdots \\ 0 & 0 & \cdots & b_n & 0 & \cdots & 1 \end{bmatrix} \end{array} = b_i$$

$\implies x_i = \frac{b_i}{1} = b_i \implies$ Формула Крамера верна.

Если $det\ A \implies \exists i:\ det\ A_i = 0 \implies$ система несовместна.

Если $det\ A = \ldots = det\ A_n = 0 \implies$ система несовместна или неопределена. ■

Теорема 11. *Пусть A — невырожденная квадратная матрица. Тогда*

$$A^{-1} = \frac{1}{det\ A} \begin{Vmatrix} A_1^1 & A_1^2 & \ldots & A_1^n \\ A_2^1 & A_2^2 & \ldots & A_2^n \\ \vdots & \vdots & \ldots & \vdots \\ A_n^1 & A_n^2 & \ldots & A_n^n \end{Vmatrix}$$

(обратите внимание, что матрица транспонирована).

$\square$ $A \cdot A^{-1} = A^{-1} \cdot A = E$

$$\underbrace{AX = E}_{\substack{\text{Уравнение относительно} \\ \text{столбцов матрицы } X}} \quad \Longrightarrow X = A^{-1}, \text{ то есть } A \cdot X_j = E_j$$

Эта система n линейных уравнений относительно элементов $x_j^1,\, x_j^2, \ldots,\, x_j^n$.

По формулам Крамера получим:

$$x_j^i = \frac{1}{det\ A} \begin{vmatrix} a_1^1 & \cdots & 0 & \cdots & a_n^1 \\ a_2^1 & \cdots & 0 & \cdots & a_n^2 \\ \vdots & & \vdots & & \vdots \\ a_1^j & \cdots & 1 & \cdots & a_n^j \\ \vdots & & \vdots & & \vdots \\ a_n^1 & \cdots & 0 & \cdots & a_n^n \end{vmatrix} = \frac{A_i^j}{det\ A}.$$

$\blacksquare$

Второй способ вычисления обратной матрицы: $(A|E)$ приводим через элементарные преобразования к $(E|A^{-1})$

Пример.

$$\begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{pmatrix} \cdot \begin{pmatrix} x_1^1 & x_2^1 \\ x_1^2 & x_2^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{pmatrix} \cdot \begin{pmatrix} x_1^1 \\ x_1^2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\text{Например, } \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} x_1^1 \\ x_1^2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\left(\begin{array}{cc|c} 1 & 2 & 1 \\ 3 & 4 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 2 & 1 \\ 0 & -2 & -3 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & -2 & -3 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3/2 \end{array}\right)$$

$$\begin{cases} x_1^1 = -2 \\ x_1^2 = 3/2 \end{cases}$$

Аналогично с вторым столбцом матрицы X.

Ранг матрицы

Определение 24. *Минором* k-го порядка матрицы A называется определитель порядка k, построенный из k^2 элементов этой матрицы, расположенныъ на пересечении произвольно выбранных k строк и k столбцов.

Определение 25. *Рангом* ненулевой матрицы $A_{n\times m}$ называется натуральное число $k:\ 1 \leq k \leq min(m,\, n)$, удовлетворяющая двум условиям:

1. У матрицы A существует по крайней мере один минор k-го порядка, отличный от нуля. $M_k \neq 0$.

2. Если у матрицы A существует миноры $k+1$-го порядка, то все они равны нулю. $M_{k+1} = 0$

Определение 26. Если $rk\,A = k$, то любой её $M_k \neq 0$ называется *базисным* или *ранговыми*. Строки и столбцы базисного минора называются *базисами*.

Теорема 12 (о базисном миноре)**.** *У любой матрицы A всякий столбец (строка) является линейной комбинацией базисных столбцов (строк).*

□ Пусть $rk\,A = k$ и M_k — базисный минор, расположенный в левом верхнем углу.

Построим определитель окаймляющий M_k, который получается добавлением i строки и j столбца.

$$\Delta = \begin{vmatrix} a_n^1 & \cdots & a_k^1 & a_j^1 \\ \vdots & & \vdots & \vdots \\ a_j^k & \cdots & a_k^k & a_j^k \\ a_1^i & \cdots & a_k^i & a_j^i \end{vmatrix} = 0$$

(так как $rk\,A = k,\ M_k \neq 0,\ M_{k+1} = 0$)

Раскладывая Δ по элементам последней строки получим:

$$a_1^i A_1^{k+1} + \ldots + a_k^i A_k^{k+1} + a_j^i M_k = 0$$
$$a_j^i = a_1^i \frac{-A_1^{k+1}}{M_k} + \ldots + a_k^i \frac{-A_k^{k+1}}{M_k}$$
$$a_j^i = \lambda_1 a_1^i + \ldots + \lambda_k a_k^i$$

a_j^i линейно выражается через остальные

■

Алгебра многочленов

(если выполнено домашнее задание, то раздел не нужно учить) 404

Группы

Циклические группы

Определение 27. *Группой* называется множество G с операцией умножения, обладающей следующими свойствами:

1. $(ab)c = a(bc), \ \forall \ a, b, c \in G$ (ассоциативность)

2. $\exists e \in G$ (единица): $\ ae = ea = e \ \forall a \in G$

3. $\forall a \in G \ \exists a^{-1} \in G$ (обратный элемент), $\ aa^{-1} = a^{-1}a = e$

Группа называется *абелевой* или *коммутативной*, если $ab = ba, \ \forall a, \ b \in G$.

В любой группе могжет быть определена степень элемента $g \in G$ с целыми показателями:

$$g^k = \begin{cases} \underbrace{g \cdot g \dots \ \cdot g}_{k}, & \text{если } k > 0 \\ e, & \text{если } k = 0 \ , k \in \mathbb{Z} \\ \underbrace{g^{-1} \cdot g^{-1} \dots \ \cdot g^{-1}}_{k}, & \text{если } k < 0 \end{cases}$$

Определение 28. Степени элемента g образуют подгруппу группы G. Она называется *циклической* и обозначается $<g>$

Определение 29. Наименьшее из натуральных m для которого выполняется $g^m = e$ называется *порядком* элемента.

Если m не существует, то порядок g равен $+\infty$.

Обозначение: $ord \ g = m$.

Теорема 13. *Если $ord \ g = n$, то*

1. $g^m = e \Leftrightarrow n \mid m$

2. $g^k = g^l \Leftrightarrow k \equiv l (mod \ n)$

$\square$ 1. $m = np + r, \ r < n$

$g^m = g^{np} \cdot g^r = (\underbrace{g^n}_{e})^p \cdot g^r = g^r$

$\Rightarrow \ g^m = e \implies g^r = e \implies r = 0 \Leftarrow$ так как $n \mid m$, то $r = 0$.

2. $g^k = g^l \implies g^{k-l} = e$

$$\implies \text{по первому утверждению } (k-l) \vdots n \implies k - l = np$$

■

В аддитивной группе говорят не о степенях элемента g, а о его кратных. Обозначение: $m\ g$

Порядком элемента g в *аддитивной* группе называют наименьшее из натуральных m, такое, что $\underbrace{g + g + \ldots + g}_{m} = 0$(если m существует).

Теорема 14. *Если ord* $g = n$, *то ord* $g^k = \frac{n}{(n,k)}$, $(n, k) = \gcd(n, k)$

□ Пусть $ord\ g^k = m$ и $(n, k) = d$. Тогда $n = n_1 d,\ k = k_1 d,\ (n_1, k_1) = 1$.

Так как $ord\ g = n$, то $g^n = e$. Также $(g^k)^m = e \implies km \vdots n \implies k_1 dm \vdots n_1 d \implies k_1 m \vdots n_1$

Так как $(k_1, n_1) = 1 \implies m \vdots n_1 \implies m = pn_1 = \frac{pn_1 d}{d} = \frac{pn}{d} \implies p = 1$.
$\implies ord\ g^k = \frac{n}{k} = \frac{n}{(n,k)}$. ■

Определение 30. Группа G называется *циклической*, если существует такой элемент в степени которого образует группу G.

$G =< g >$ и такой элемент называется *образующим.*

Пример. $\mathbb{Z}$ аддитивная группа целых чисел является циклической с образующим элементом 1 или -1

Z_n — циклическая группа с образующим элементом [1].

Определение 31. Число элементов конечной группы называется её *порядком.*

Обозначение: $|G|$

Пример. Всякая бесконечная циклическая группа изоморфна группе целых чисел:

$f : \mathbb{Z} \to G$,

$f : k \to g^k$.

Всякая конечная цилкическая группа порядка n изоморфна группе Z_n:

$f : Z_n \to G$.

Всякая подгруппа циклической группы является циклической.

В циклической группе порядка n порядок любой подгруппы делит n и для любого делителя p числа n существует одна подгруппа порядка n.

Разбиение на смежные классы

Определение 32. Пусть G — группа, H — подгруппа группы G. Элементы $g_1,\ g_2 \in G$ сравнимы по модулю H ($g_1 \equiv g_2\ (mod\ H)$), если $g_1^{-1}g_2 \in H$.
$g_1^{-1}g_2 = h \in H \implies g_2 = g_1 h$

Отношение сравнимости по модулю H является отношением эквивалентности:

1.

$$g_1 \equiv g_1\ (mod\ H)$$
$$(g_1^{-1}g_1) = e \in H$$

2.

$$g_1 \equiv g_2\ (mod\ H) \implies g_2 \equiv g_1\ (mod\ H)$$
$$g_1^{-1}g_2 \in H \implies (g_1^{-1}g_2)^{-1} \in H, \text{так как является обратным.}$$
$$\implies (g_2^{-1}g_1 \in H) \implies g_2 \equiv g_1\ (mod\ H).$$

3.

$$g_1 \equiv g_2\ (mod\ H) \land g_2 \equiv g_3\ (mod\ H)$$
$$\implies g_1 \equiv g_3\ (mod\ H)$$
$$g_1^{-1}g_2 \in H,\ g_2^{-1}g_3 \in H$$
$$\implies (g_1^{-1}\underbrace{g_2) \cdot (g_2^{-1}}_{e}g_3) \in H \implies g_1^{-1}g_3 \in H$$
$$\implies g_1 \equiv g_3\ (mod\ H).$$

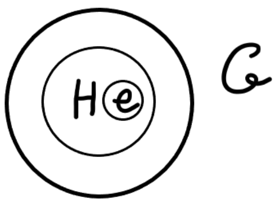


Рис. 1: Пример

Определение 33. Классы этой эквивалентности называются *левыми смежными классами* группы G подгруппы H.

Смежный класс, содержащий элемент g, имеет вид $gH = \{gh,\ h \in H\}$

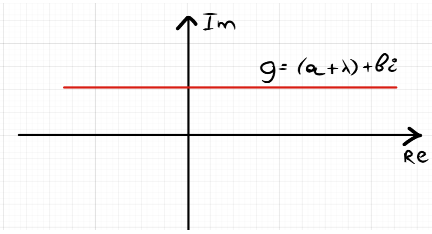
Одним из смежных классов является сама подгруппа H.

Если вместо $g_1^{-1}g_2 \in H$ взять $g_2\, g_1^{-1} \in H$, то получим другое отношение эквивалентности. Классы этой эквивалентности называются *правыми смежными классами.*

Пример. Смежные классы аддитивной группы $\mathbb{C}$ на подгруппе $\mathbb{R}$ изображаются на комплексной плоскости прямой параллельной оси Ox

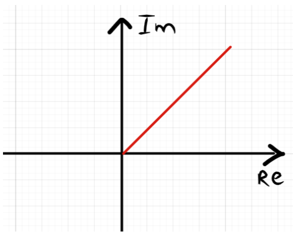
$g + \mathbb{R},\ g \in \mathbb{C}$

$g + \mathbb{R} = \{g + \lambda,\ \lambda \in \mathbb{R}\}$



Пример. Смежные классы мультипликативной групп $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ по подгруппе $\mathbb{R}_+^*$ изображаются на комплексной плоскости лучами, исходящими из начала координат.

$g\mathbb{R}_+^* = \{g\lambda,\ \lambda \in \mathbb{R}\}$



Множество левых смежных классов группы G подгруппы H обозначается G/H.

Определение 34. Число смежных классов, если оно конечно, называется *индексом* подгруппы H и обозначается $|G : H|$.

Теорема 15 (Лагранжа)**.** *Если G конечная группа, H любая её подгруппа, то $|G| = |G : H| \cdot |H|$.*

□ Все смежные классы gH содержат одно и то же количество элементов равное $|H|$. Так как эти классы образуют разбиение группы G, то порядок группы G равен произведению их числа на количество элементов подгруппы $H \implies |G| = |G : H| \cdot |H|$. ■

Определение 35. Подгруппа H группы G называется *нормальной*, если $gH = Hg$, то есть $\forall g \in G: \ gHg^{-1} = H$.

Обозначение: $H \lhd G$, $G \rhd H$.

В случае, если H — нормальная подгруппа группы G, то G/H называется *факторгруппой*. eH — единица этой группы.

Определение 36. $f: \ G_1 \to G_2$ называется *гомоморфизмом*, если $f(ab) = f(a)f(b), \ a, b \in G_1$.

Свойства:

1. $f(e) = e$

2. $f(g^{-1}) = f(g)^{-1}$
   $\square \quad f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e \implies f(a^{-1}) = f(a)^{-1}$. $\blacksquare$

3. $Im\ f = \{f(a), \ a \in G_1\}$ — образ гомоморфизма. $Im\ f \subset G_2$.

4. $Ker\ f = \{a \in G_1, \ f(a) = e\}$ — ядро.

   $Ker\ f$ есть нормальная подгруппа группа G_1.
   $\square \quad a, b \in Ker\ f$

   $f(ab) = f(a) \cdot f(b) = e \cdot e = e \implies ab \in Ker\ f$

   $a \in Ker \implies f(a^{-1}) = e^{-1} = e \implies a^{-1} \in Ker\ f \implies Kerf \subset G_1$.

   $\forall g \in G_1, \ a \in Ker\ f, \ g\,a\,g^{-1} \overset{?}{\in} Ker\ f$.

   $f(g\,a\,g^{-1}) = f(g) \cdot f(a) \cdot f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = f(g)f(g^{-1}) = e$
   $\implies g\,a\,g^{-1} \in Ker\ f$. $\blacksquare$

5. $f(g_1) = f(g_2) \implies g_1 \equiv g_2 (mod\ Ker\ f)$
   $\square \quad f(g_1) = f(g_2) \ / \cdot f(g_1^{-1})$

   $f(g_1^{-1})f(g_1) = f(g_1^{-1})f(g_2)$

   $e = f(g_1^{-1}g_2) \implies g_1^{-1}g_2 \in Ker\ f \implies g_1 \equiv g_2(mod\ Ker\ f)$ $\blacksquare$

6. $f(a^n) = (f(a))^n$

7. $f: \ G_1 \to G_2$

   $\forall g \in G_1$ порядок элемента $f(g)$ делит порядок g.
   $\square \quad$ Пусть $ord\ g = k \implies g^k = e$

   $f(g^k) = (f(g))^k \implies (f(g))^k = e \implies ord\ f(g) = k$. $\blacksquare$

Линейные операторы и квадратичные формы

404

Фигуры второго порядка на плоскости и в пространстве

404