

Конспект по алгебре за I семестр бакалавриата
Чебышёва СПбГУ (лекции Степанова Алексея
Владимировича)

November 19, 2019

Contents

1	Линейная алгебра. Векторные пространства	2
1.1	Лекция 1	2
1.2	Лекция 2	4
1.3	Лекция 3	5
1.3.1	Произведение матриц	6
1.4	Лекция 4	6
1.5	Лекция 5	9
1.6	Лекция 6	9
1.7	Лекция 7	9
1.8	Лекция 8	9
1.9	Лекция 9	11
1.10	Лекция 10	14
1.11	Лекция 11	15
1.12	Лекция 12	17
1.13	Лекция 13	20
1.14	Лекция 14	20
2	Начала теории групп	23
2.1	Лекция 15	23
2.2	Лекция 16	24
2.3	Лекция 17	26
2.4	Лекция 18	28
2.5	Лекция 19	30
2.5.1	Поговорим о коммутаторах	30
2.5.2	Возвращаемся к матрицам	31
2.6	Лекция 20	32
2.6.1	Симметрическая группа	32
2.7	Лекция 21	33
2.7.1	Продолжаем возиться с перестановками. Четность.	33
2.8	Лекция 22	36

Chapter 1

Линейная алгебра. Векторные пространства

1.1 Лекция 1

X - множество

$*$: $X \times X \rightarrow X$

$(x, y) \mapsto x * y$

Аксиомы:

1. $\forall x, y, z \in X : x * (y * z) = (x * y) * z$ (ассоциативность)
2. $\exists e \in X \forall a \in X : e * a = a * e = a$ (нейтральный элемент)
3. $\forall a \in X \exists a' \in X : a * a' = a' * a = e$ (обратный элемент)
4. $\forall a, b \in X : a * b = b * a$ (коммутативность)

Определение 1. Множество X с операцией $*$, удовлетворяющее аксиоме 1, называется **полугруппой**

Определение 2. Множество X с операцией $*$, удовлетворяющее аксиомам 1-2, называется **моноидом**

Определение 3. Множество X с операцией $*$, удовлетворяющее аксиомам 1-3, называется **группой**

Определение 4. Множество X с операцией $*$, удовлетворяющее аксиомам 1-4, называется **коммутативной** или **абелевой группой**

Примеры.

1. $(\mathbb{Z}, +)$ – группа
2. $(\mathbb{N}, +)$ – полугруппа

3. $(\mathbb{N}_0, +)$ – моноид

4. $(\mathbb{R} \setminus \{0\}, \cdot)$ – группа

5. Пусть A – множество

$X :=$ множество биективных отображений $A \rightarrow A$

id_A – нейтральный элемент

Если $f(x) = y$, то $\tilde{f}(y) = x$ – обратная функция ($f \circ \tilde{f} = \tilde{f} \circ f = id_A$).

$f(x) = x + 1$, $g(x) = 2x$, $id_A(x) = x$

$f \circ g(x) = f(g(x)) = f(2x) = 2x + 1$

$g \circ f(x) = g(f(x)) = g(x + 1) = 2x + 2 \neq 2x + 1$

Следовательно, (X, \circ) – не коммутативная группа

Обозначение.

- \cdot – мультипликативность, 1 , x^{-1}
- $+$ – аддитивность, 0 , $-x$
- \circ – относительно композиции, id , x^{-1}
- $*$ – абстрактная операция, e , x^{-1}

Пусть $(R, +)$ – абелева группа

Определим отображение

$$\cdot : R \times R \rightarrow R$$

$$(a, b) \mapsto a \cdot b$$

Для $(R, +, \cdot)$ могут быть верны следующие аксиомы:

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

$(b + c)a = ba + ca$ (дистрибутивность)

6. $a(bc) = (ab)c$ (ассоциативность)

7. $\exists 1_R \forall a \in R : 1_R \cdot a = a \cdot 1_R = a$ (нейтральный элемент)

8. $ab = ba$ (коммутативность)

9. $0_R \neq 1_R$

10. $\forall a \neq 0_R \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ (обратный элемент)

Определение 5. $(R, +, \cdot)$, удовлетворяющее аксиоме 5, называется **не ассоциативным кольцом без единицы**.

Определение 6. $(R, +, \cdot)$, удовлетворяющее аксиомам 5-6, называется **ассоциативным кольцом без единицы**.

Определение 7. $(R, +, \cdot)$, удовлетворяющее аксиоме 5-7, называется **ассоциативным кольцом с единицей**.

Определение 8. $(R, +, \cdot)$, удовлетворяющее аксиомам 5-8, называется **коммутативным кольцом**.

Примеры.

1. \mathbb{Z} – коммутативное кольцо

2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля

3. Рассмотрим $\mathbb{Z}_n = 0, \dots, n-1$ с операциями $+_n, \cdot_n$:

$$a +_n b = (a + b) \% n$$

$$a \cdot_n b = (a \cdot b) \% n$$

Обратимые элементы:

$$ax = 1 + ny$$

$$ax - ny = 1$$

Если $(a, n) = 1$, есть решение, иначе – нет. \mathbb{Z}_p – поле $\Leftrightarrow p \in \mathbb{P}$

1.2 Лекция 2

Определение 9. V – векторное пространство над полем F , если $(V, +)$ – абелева группа, задано отображение $V \times F \rightarrow V$

$(x, \alpha) \mapsto x \cdot \alpha$, удовлетворяющее аксиомам $\forall x, y \in V, \forall a, b \in F$:

$$5. x \cdot (\alpha \cdot \beta) = (x \cdot \alpha) \cdot \beta$$

$$6. (x + y) \cdot \alpha = x \cdot \alpha + y \cdot \alpha$$

$$x \cdot (\alpha + \beta) = x \cdot \alpha + x \cdot \beta$$

$$7. x \cdot 1_F = x$$

$$A \in M_n(F), \alpha \in F$$

$$(A, \alpha)_{ij} = a_{ij} \cdot \alpha$$

$$(AB)\alpha = A(B\alpha)$$

Примеры.

1. Множество векторов в \mathbb{R}^3

$$2. F^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in F \right\}$$

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

3. X - множество, $F^X = \{f \mid f : X \rightarrow F\}$
 $f, g : X \rightarrow F$
 $(f + g)(x) = f(x) + g(x)$
 $(f\alpha)(x) = f(x)\alpha$
4. $F[t]$ - многочлены от одной переменной t
5. V - абелева группа, в которой $\forall a \in V : \underbrace{a + a + \dots + a}_{p \in \mathbb{P}} = 0$ Тогда V - векторное пространство над \mathbb{Z}_p $k \cdot a = \underbrace{a + \dots + a}_k$

1.3 Лекция 3

Определение 10. Алгебра A над полем F – кольцо, являющееся векторным пространством над F ("+" - операция в кольце и в векторном пространстве), такое что $(ab)\alpha = a(b\alpha)$ $a, b \in A, \alpha \in F$

Пример. $(\mathbb{R}^3, +, \times)$ - не ассоциативная алгебра на \mathbb{R}

Определение 11. Матрица размера $I \times J$ (I, J - множества индексов) над множеством X - это функция

$$A : I \times J \rightarrow X, \quad (i, j) \rightarrow a_{ij}.$$

Пусть определено умножение $X \times Y \rightarrow Z, \quad (x, y) \rightarrow xy$
(Z - коммутативный моноид относительно "+")

Определение 12. Строка - матрица размера $\{1\} \times J$
Столбец - матрица размера $J \times \{1\}$

A - строка длины J над X

B - строка длины J над Y

Тогда произведение $AB = \sum_{j \in J} a_{1j} b_{j1} \in Z$

$x \rightarrow x_e$ - координаты вектора x

$$\underbrace{x \cdot y}_{\text{скалярное произведение}} = x_e^T \cdot y_e$$

Определение 13. Транспонирование матрицы.

D - матрица $I \times J$ над X

D^T - матрица $J \times I$ над $X : (D^T)_{ij} = (D)_{ji}$

Замечание. Пусть в X есть элемент $0 : 0 \cdot y = 0 \quad \forall y \in Y$. Все кроме конечного числа $a_j = 0$. Тогда AB имеет смысл, даже когда $|J| = \infty$.

"почти все" = кроме конечного количества

Обозначение.

a_{i*} - i -я строка матрицы A

a_{*j} - j -й столбец матрицы A

1.3.1 Произведение матриц

A - матрица $I \times J$ над X .

B - матрица $J \times K$ над Y .

AB - матрица $I \times K$ над $Z = X \cdot Y$, $(AB)_{ik} = a_{i*} \cdot b_{*k} = \sum_{j \in J} a_{ij} \cdot b_{jk}$.

$$(x_1, \dots, x_n) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = va, \quad v \in V, a \in F.$$

1.4 Лекция 4

Определение 14. $(G, *)$, $(H, \#)$ - группа

$\varphi : G \rightarrow H$ - гомоморфизм, если:

$$\varphi(g_1 * g_2) = \varphi(g_1) \# \varphi(g_2)$$

Определение 15. R, S -кольца

$\varphi : R \rightarrow S$ - гомоморфизм, если:

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$$

$$\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$$

Для колец с 1: $\varphi(1) = 1$

Определение 16. U, V - векторные пространства над F

$\varphi : U \rightarrow V$ - линейное отображение, если:

$$\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$$

$$\varphi(u\alpha) = \varphi(u)\alpha$$

Замечание. Изоморфизм – биективный гомоморфизм.

Определение 17. V - векторное пространство над полем F

v - строка элементов "длины" I над V

a - столбец "высоты" I , почти все элементы которого равны 0.

Тогда va - линейная комбинация набора v с коэффициентами .

Замечание. $U \subset V$

U является векторным пространством относительно тех же операций, которые заданы в V . Тогда U - подпространство V

Лемма. $U \subseteq V$

$\forall u_1, u_2 \in U, \alpha \in F :$

$u_1 + u_2 \in U, u_1 \alpha \in U$ Тогда U - подпространство. Если U - подпространство в V , то пишут $U \subseteq V$.

Определение 18. $v = \{v_i | i \in I\}$, где $v_i \in V \forall i \in I$

$\langle v \rangle$ - наименьшее подпространство, содержащее все v_i

Лемма. $\langle v \rangle = \{va | a - \text{столбец высоты } I \text{ над } F, \text{ где почти всюду элементы равны нулю}\} = U$

Доказательство. $v_i \in \langle v \rangle \Rightarrow v_i a_i \in \langle v \rangle$

$\Rightarrow v_{i_1} a_{i_1} + \dots + v_{i_k} a_{i_k} \in \langle v \rangle$

$\Rightarrow \langle v \rangle$ содержит все варианты комбинаций. $va + vb = v(a + b) \in U$

$(va)\alpha = v(a\alpha) \in U$

\Rightarrow множество линейных комбинаций – подпространство U - подпространство, содержащее $v_i \forall i \in I$

$\langle v \rangle$ – наименьшее подпространство, содержащее v_i

$\Rightarrow \langle v \rangle \subseteq U$ тогда $\langle v \rangle = U$

□

Определение 19. Если $\langle v \rangle = V$, то v – система образующих пространство V
Базис – система образующих.

Обозначение. F^I – множество функций из I в F = множество столбцов высоты I
 ${}^I V$ – множество строк длины I

Набор элементов из V , заиндексированных множеством I – это функция $f : I \rightarrow V$
 $i \mapsto f_c$

Определение 20. $v \in {}^I V$

v – линейно независим, если $\forall a \in F^I, a \neq 0 \Rightarrow va \neq 0$

Теорема 1.4.1. $v \subseteq V$ (можно считать, что v – строка длины v)
Следующие утверждения эквивалентны:

1. v – линейно независимая система образующих
2. v – максимальная линейно-независимая система
3. v – минимальная система образующих
4. $\forall x \in V \exists! a \in F^v : x = va = \sum_{t \in v} t \cdot a_t$ (почти все элементы равны 0)

Доказательство. (1) \Rightarrow (4) – доказали ранее (1) \Rightarrow (2)

$$x \in V \setminus v$$

$$x = va(a \in F^v)$$

$$va = x \cdot 1 = 0 - \text{линейная зависимость набора } v \cup x$$

Т.о. любой набор, строго содержащий v , линейно зависим $\Rightarrow v$ – максимальный.

$$(1) \Rightarrow (2)$$

$$x \in V \setminus$$

$$v \subseteq V \cup x - \text{линейно зависим}$$

$$va + xa_x = 0$$

$$a \neq 0$$

$$\text{Если } a_x = 0 \Rightarrow va = 0 \Rightarrow a = 0 \text{ ?!}$$

$$\text{Значит } a_x \neq 0$$

$$va = c \cdot (-a_x)$$

$$x = v \cdot \frac{a}{-a_x} \Rightarrow v - \text{система образующих.}$$

□

Лемма. (Цорн) Пусть \mathbb{A} – набор подмножеств (не всех) множества X .

Если объединение любой цепи из \mathbb{A} , принадлежащей \mathbb{A} , то в \mathbb{A} существует максимальный элемент.

$$M \in \mathbb{C} - \text{максимальная, если } M \subseteq M' \subseteq \mathbb{A} \Rightarrow M = M'$$

Теорема 1.4.2. (о существовании базиса) V – векторное пространства

X – линейное независимое подмножество V

Y – система образующих V

$$X \leq Y$$

Тогда существует базис Z пространства $V : X \leq Z \leq Y$

Доказательство. \mathbb{A} – множество всех линейно независимых подмножеств, лежащих между X и Y . $X \in \mathbb{A}$

$$\mathbb{C} \leq \mathbb{A}$$

$$X \leq \cup C \in \mathbb{C} \leq Y$$

Пусть $\cup C \in \mathbb{C}$ – линейно зависимый. То есть $\exists u_1, \dots, u_2 \in / \dots$

...

Пусть v – базис V .

$$\forall x \in V \exists! x_v \in F^v : x = v \cdot x_v$$

$$v = (v_1, \dots, v_n), x_v = \text{матрица столцов альфа;}$$

$$x = v_1 \alpha_1 + \dots = v \cdot x_v$$

□

1.5 Лекция 5

1.6 Лекция 6

1.7 Лекция 7

Утверждение.

$$U \leq W \iff \exists V \leq W : W = U \oplus V$$

Доказательство. Выберем базис u в U . Дополним до базиса $u \cup v$ пространства W и положим $V = \langle v \rangle$.

$$\langle u \rangle = U \quad \langle v \rangle = V \quad \langle u \cup v \rangle = \langle u \rangle + \langle v \rangle = U \oplus V = W$$

$$x \in U \cap V \Rightarrow x = ua = vb \Leftrightarrow ua - vb = 0 \Rightarrow a = 0, b = 0 \quad (u \cup v - \text{линейно независимый})$$

□

Следствие.

$$u - \text{базис } U, v - \text{базис } V, U, V \leq W$$

$$u \cup v - \text{базис } W \Leftrightarrow U \oplus V$$

25.09.2019

1.8 Лекция 8

$$v = (v_1, v_2, \dots, v_n) \in n^V$$

$$M_n(F) - \text{алгебра матриц размера } n \times n \text{ над } F$$

$$GL_n(F) = M_n(F)^* - \text{полная линейная группа степени } n \text{ над } F$$

Лемма.

$$v \in n^V, A \in GL_n(F)$$

$$v - \text{линейно независимый} \Leftrightarrow vA - \text{линейно независимый}$$

$$\langle v \rangle = \langle vA \rangle$$

Доказательство. $(vA)A^{-1} = v(AA^{-1}) = vE = v$, поэтому можно доказывать только в одну сторону.

v - линейно независимый.

$vAb = 0 \Rightarrow A^{-1}Ab = 0 \Rightarrow b = 0$, т.е. vA - линейно независимый.

$$(vA)b = v(Ab) \in \langle v \rangle, \langle vA \rangle \leq \langle v \rangle$$

□

Утверждение. u, v - два разных базиса пространства V .

Тогда $\exists!$ матрица $A \in GL_n(F) : u = vA$

При этом $a_{*k} = (u_k)_v \quad \forall k = 1, \dots, n$. Такая матрица обозначается $C_{v \rightarrow u}$ и называется матрицей перехода от v к u .

$$C_{v \rightarrow u} C_{u \rightarrow v} = C_{v \rightarrow u} C_{u \rightarrow v} = E$$

Доказательство. Положим $a_{*k} = (a_k)_v \Rightarrow u_k = va_{*k} \Rightarrow u = vA$.

$vA = vB \Leftrightarrow A = B$ то есть A - единственно.

Далее:

$$\left. \begin{aligned} u &= vC_{v \rightarrow u} \\ v &= uC_{u \rightarrow v} \end{aligned} \right\}$$

$$uE - uC_{v \rightarrow u}C_{v \rightarrow u}$$

$$E = C_{u \rightarrow v}C_{v \rightarrow u}$$

□

Следствие. v - базис V

$f : GL_n(F) \rightarrow$ множество базисов пространства V

$f(A) = vA$ - биекция.

Доказательство.

$$|F| = q \quad \dim V = u$$

$$(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) - \text{количество базисов}$$

\mathbb{F} - поле из q элементов.

□

Утверждение. Если матрица двусторонне обратима, то она квадратная.

Следствие. u, v - базисы V

$$x = C_{u \rightarrow v} x_v$$

Доказательство.

$$x = ux_u = vx_v$$

$$v = uC_{u \rightarrow v}$$

$$ux_u = uC_{u \rightarrow v}x_v \Rightarrow x_u = C_{u \rightarrow v}x_v$$

□

Следствие. (Матричные линейные отображения)

$$L : U \rightarrow V, \quad u - \text{базис } U, v - \text{базис } V$$

Тогда $\exists!$ матрица $L_{v,u}(L_u^v : \forall x \in UL(x)_v = L_u^v x_u$

При этом $(L_u^v)_{*k} = L(u_k)_v$

Замечание.

$$u = (u_1, \dots, u_n) \in n^U$$

$$L : U \rightarrow V$$

$$L(a) := (L(u_1), \dots, L(u_n))$$

$$L(ua) = L(u)a \quad a \in F^n$$

$$\varphi_v : V \rightarrow F^n$$

$$\varphi_v(g) = y_v \quad \forall g \in V$$

$$\varphi_v - \text{линейно} \Rightarrow (L(u)a)_v = L(u)_v a$$

$$L(u)_v := (L(u_1)_v, \dots, L(u_n)_v)$$

Доказательство.

$$x = ux_u$$

$$L(x) = L(u)x_u$$

$$L(x)_v = L(u)_v x_u$$

Положим $L_u^v := L(u)_v$.

$$\forall x \in U : L(x)_v = L_u^v x_u$$

$$\text{При } x = u_k : L(u_k)_v = L_u^v(u_k)_u = (L_u^v)_k$$

□

Замечание. Если $Ax = Bx \quad \forall x \in F^n$, то $A = B$

26.09.2019

1.9 Лекция 9

Примеры.

1. $V = \mathbb{R}[t]_3$ - многочлены степени не более 3

$$D(p) = p' \quad V \rightarrow V$$

$$v = (1, t, t^2, t^3).$$

$$D(1) = 0, D(t) = 1, D(t^2) = 2t.$$

$$D_v = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$v^{(1)} = (1, \frac{t}{1!}, \frac{t^2}{2!}, \frac{t^3}{3!}).$$

2. $V = \mathbb{R}[t]$

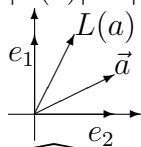
$$v = (1, t, \frac{t^2}{2}, \dots, \frac{t^n}{n!}, \dots).$$

$$D(v_0) = 0, D(v_k) = v_{k-1}.$$

$$\begin{pmatrix} 0 & 1 & \cdots \\ & 0 & 1 & \cdots \\ & & 0 & 1 \\ \vdots & \vdots & & \ddots \end{pmatrix}$$

3. $V = \mathbb{R}^3$

$$|L(a)| = |a|$$



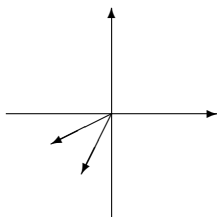
$$a, L(a) = \varphi$$

$e = (e_1, e_2)$ - базис

$$L(e_1)_e = \begin{pmatrix} \cos \varphi \\ \sin \varphi \end{pmatrix}$$

$$L(e_2)_e = \begin{pmatrix} -\sin \varphi \\ \cos \varphi \end{pmatrix}$$

$$L_e = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}.$$



$$a_e = \begin{pmatrix} \cos \psi \\ \sin \psi \end{pmatrix}$$

$$L(a)_e = \begin{pmatrix} \cos(\psi + \varphi) \\ \sin(\psi + \varphi) \end{pmatrix}.$$

$$L(a)_e = L_e \cdot a_e = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix} \cdot \begin{pmatrix} \cos \psi \\ \sin \psi \end{pmatrix} = \begin{pmatrix} \cos \varphi \cos \psi - \sin \varphi \sin \psi \\ \cos \varphi \sin \psi + \sin \varphi \cos \psi \end{pmatrix}.$$

Утверждение. $L : U \rightarrow V$

$u, u' - \text{базис } U$

$v, v' - \text{базис } V$

Тогда $L_{u'}^{v'} = C_{v' \rightarrow v} L_u^v C_{u \rightarrow u'}$

Доказательство.

$$L(x)_v = L_u^v x_u.$$

$$C_{v' \rightarrow v} L(x)_v = L(x)_{v_1} = L_{u'}^{v'} x_{u'} = L_{u'}^{v'} C_{u' \rightarrow u} x_u.$$

$$\forall x_u \in F^{\dim U}$$

$$L(x)_v = C_{v \rightarrow v'} L_{u'}^{v'} C_{u' \rightarrow u} x_k.$$

$$L_u^v = C_{v \rightarrow v'} L_{u'}^{v'} C_{u' \rightarrow u}.$$

□

Замечание.

$$\text{Если } U = V \quad u = v, u' = v'.$$

$$L_{u'}^{v'} = C_{u' \rightarrow u} L_u^v C_{u \rightarrow u'}.$$

Утверждение. *Линейное отображение однозначно определяется образом базисных векторов.*

$u = (u_1, \dots, u_n) - \text{базис } U$

Для любого векторного пространства V :

$$\forall v_1, \dots, v_n \in V$$

$$\exists! \text{ линейное отображение } (*) L : U \rightarrow V : L(u_k) = v_k \quad \forall k$$

Доказательство.

$$L(ua) := va$$

$$\forall L^* : L(ua) = L(u)a = va$$

□

При этом L - инъективно тогда и только тогда, когда v - линейно независимый
 L - сюръективно тогда и только тогда, когда v - система образующих
 L - изоморфизм тогда и только тогда, когда v - базис.

Утверждение. $V, \quad v, v' - \text{базис } V$

$L : V \rightarrow V - \text{линейно}$

$$L(v_k) = v'_k \quad \forall k$$

$$(L_v)_k = L(v_k)_v = (v'_k)_v$$

$$L_v = C_{v \rightarrow v'}.$$

по другому

$$(Id_{v'}^v)_k = Id(v'_k)_v = (v'_k)_v.$$

$$\text{Тогда } L_v = C_{v \rightarrow v'} = Id_{v'}^v.$$

Определение 21. $f : X \rightarrow Y$

$$Im f = \{f(x) \mid x \in X\}$$

$L : U \rightarrow V$ - линейное отображение

$$Im L = \{L(x) \mid x \in U\}$$

$$Ker L = L^{-1}(0) = \{x \in U \mid L(x) = 0\}$$

Лемма.

$$Im L \leq V$$

$$Ker L \leq U$$

Пусть $L(x) = y$

$$\begin{aligned}\forall y \in V : L^{-1} = x + Ker L \\ L^{-1}(y) = \{z \in U \mid L(z) = y\} \\ x + Ker L = \{x + z \mid z \in Ker L\}\end{aligned}$$

1.10 Лекция 10

Теорема 1.10.1. $L : U \rightarrow V$

$$\dim U = \dim Ker L + \dim Im L.$$

Доказательство. $u = (u_1, \dots, u_k)$ - базис $Ker L$

$v = (v_1, \dots, v_m)$ Дополним базис ядра до базиса U : $u \cup v$ - базис U

$L(v) = (L(v_1), L(v_2), \dots, L(v_m))$ - базис образа. $\forall x \in Im L \exists y \in U : L(y) = x$.

$$y = ua + vb, \quad a \in F^k, b \in F^m$$

$$x = L(y) = \underbrace{L(u)}_{(L(u_1), \dots, L(u_k)) = (0, \dots, 0)} + L(v).$$

Следовательно, $L(v)$ - система образующих.

$$L(v)c = 0, \quad c \in F^m.$$

$$L(vc) = 0 \Rightarrow vc \in Ker L \Rightarrow vc = ud \quad \text{для некоторого } d \in F^k.$$

Тогда $vc - ud = 0$, но v и u - два базисных вектора. Следовательно, $c = d = 0$ и $L(v)$ - линейно независимый. \square

Теорема 1.10.2. (формула Грассмана о размерности суммы и пересечения)

$$U, V \leq W$$

$$\dim U \cap V + \dim U + V = \dim U + \dim V.$$

Доказательство. \hookleftarrow внешнюю сумму $U \oplus V$, $L(u, v) = u + v$

Тогда $Im L = U + V$. $(u, v) \in Ker L \Leftrightarrow u + v = 0 \Leftrightarrow u = -v \subset U \cap V$

$$Ker L = (u, -u) \mid u \in U \cap V \cong U \cap V$$

$$\dim(U \oplus V) = \dim Ker L + \dim Im L = \dim U \cap V + \dim U + V \quad \square$$

08.10.2019

1.11 Лекция 11

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} \cdot x_1 + \dots + \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix} \cdot x_n = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Простейший базис:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

$$x = vx_v, \quad x = ex_e = Ex_e$$

$$eC_{e \rightarrow v} = v - \text{из столбцов } v.$$

$$C_{e \rightarrow v} = v - \text{матрица из столбцов } (v_1, \dots, v_n).$$

$$L : F^m \rightarrow F^n, \quad A \in M_{n \times m}(F) \quad L(x) = Ax$$

$$L(x)_e = L_0^e x_e, \quad L(x)_e = L(x) = Ax = L_e^e x_e.$$

$\text{Hom}(F^n, F^m) \cong M_{m \times n}(F)$ - изоморфизм векторных пространств. В дальнейшем A отождествляется с L , пишем A_u^v вместо L_u^v (A в базисе $u - v$).

Определение 22. Линейный оператор из V в V называется эндоморфизмом V . Множество эндоморфизмов $V = \text{End}(V)$ - ассоциативная алгебра над f

$+, * \alpha$ - поточечные операции, $*$ - композиция.

$L, M, N \in \text{End}(V) : \quad L \circ (M + N) = L \circ M + L \circ N$ - следует из линейности L

v - базис V , $u = \dim V$

$$\theta_v : \text{End}(V) \rightarrow M_n(F)$$

$$\theta_v = L_v$$

Утверждение. θ_v - биективно.

Упражнение. Построить обратное θ_v

$$\text{Лемма. } (M \circ L)_v = M_v \circ L_v$$

Утверждение. θ_v - изоморфизм

F - алгебра

$$\text{End} V \cong M_n(F)$$

—

Теорема 1.11.1. $U \leq V$

$\forall L : V \rightarrow W, \quad U \leq \text{Ker} L, \exists! \tilde{L} : V \setminus U \rightarrow W$

$$\tau : \begin{array}{ccc} V \setminus U & \longrightarrow & W \\ \uparrow \pi_U & & \\ V & \xrightarrow{L} & W \end{array}.$$

$$\tau \circ \pi_U = L$$

L - эпиморфизм $\Rightarrow \tau$ - эпиморфизм

$\text{Ker} L = U \Rightarrow \tau$ - мономорфизм

Доказательство. Диаграмма коммутативна, следовательно, \tilde{L} строится однозначно. Пусть $\tilde{L}(x+U) := L(x).y \in U \in \text{Ker} L : L(x+y) = L(x)+L(y) = L(x) \tilde{L}$ задано корректно (легко проверить, что оно линейно, единственность следует из коммутативности диаграммы). $\tilde{L}(x+U) = L(x)$ - необходимо и достаточно коммутативности диаграммы. $\tilde{L}(x+U) = 0_W \Leftrightarrow L(x) = 0 \Leftrightarrow x \in \text{Ker} L = U \Leftrightarrow x+U = 0+U = 0_{V \setminus U}$
Для инъективности : $\text{Ker} \tilde{L} = 0_{V \setminus U}$ □

Теорема 1.11.2 (О гомоморфизме). $L : V \rightarrow W$

$$V/\text{Ker} L \cong \text{Im} L.$$

Доказательство. Возьмем $U = \text{Ker} L$ и заменим W на $\text{Im} L$ $n = \dim \langle a_{*1}, \dots, a_{*n} \rangle \leq \dim F^m = m$. Из линейной независимости строк следует, что $m \leq n$ Таким образом $m = n$.

n линейно независимых столбцов (строк) в n -мерном пространстве - базис и матрица A - матрица перехода $C_{e \rightarrow a}$, где $a = (a_{*1}, \dots, a_{*n})$ - набор столбцов A . Следовательно, $A \in GL_n(F)$ - множество обратных матриц. □

Определение 23. Ранг:

$$rk(v_1, v_2, \dots, v_n) = \dim \langle v_1, \dots, v_n \rangle,$$

$$rk L = \dim \text{Im} L$$

$$u_1, \dots, u_n - \text{базис } U, L : U \rightarrow V$$

$$rk L = rk((L(u))) = \dim \langle L(u_1), \dots, L(u_n) \rangle$$

$$A \in M_{m \times n}(F)$$

$$\text{Столбцовый ранг } A : rk A = rk(a_{*1}, \dots, a_{*m})$$

$$\text{Строчный ранг} : rk A = rk(a_{1*}, \dots, a_{n*})$$

или наибольшее количество независимых столбцов (строк).

Лемма. $A \in M_{m \times n}$

1. столбцы A линейно независимы \Leftrightarrow столбцовый $rk A = n$
2. столбцы A - система образующих в $F^m \Leftrightarrow$ столбцовый $rk A = m$
3. строки A линейно независимы \Leftrightarrow строчной $rk A = m$

4. строки A - система образующих в ${}^mF \Leftrightarrow$ строчной $rkA = n$
5. столбцы являются базисом $F^n \Leftrightarrow m = n =$ строчной rkA
6. если столбцы и строки A линейно независимы $\Leftrightarrow n = m$, строки и столбцы - базисы, A - обратима.

Доказательство. (6)

из (1) $\Rightarrow c.rkA = n$

$$n = \dim \langle a_{*1}, \dots, a_{*n} \rangle$$

□

10.10.2019

1.12 Лекция 12

Лемма. $L : U \rightarrow V$ - линейное отображение.

$$rkL = c.L_U^V$$

Для любых базисов u, v пространств U, V .

Доказательство.

$$\begin{array}{ccc} U & \xrightarrow{L} & V \\ \downarrow \varphi_u & & \downarrow \varphi_v \\ F^n & \xrightarrow{L_U^V} & F^m \end{array}$$

$$A \in M_{m \times n}(F)$$

$$ImA = \{Ax \mid x \in F^n\} = \{a_{*1}x_1 + \dots + a_{*n}x_n \mid x_i \in F\} = \langle a_{*1}, \dots, a_{*n} \rangle.$$

$rkA = c.rkA$ - ранг оператора умножения на A . Из диаграммы $ImL \cong ImL_U^V \Rightarrow rkL = c.rkL_U^V$ □

Лемма. $A \in M_{m \times n}(F)$

$$B \in GL_m(F), C \in GL_n(F)$$

$rkA = rkBAC$ - строчной или столбцовый.

Доказательство. $L : F^n \rightarrow F^m$ - оператор умножения на A . $A = L_e^e$.

$B = C_{e \rightarrow v}, C = C_{e \rightarrow u}$, где u, v - базисы пространств F^m, F^n .

$BAC = L_v^u$ Тогда $c.rkA = c.rkBAC = rkL$. Со столбцами все хорошо. Теперь со строками: $r.rkA^T = c.rkA$

$$r.rk(BAC)^T = r.rk(A^T B^T C^T) \quad r.rk(BAC)^T = c.rkBAC$$

Тогда $r.rkA^T = r.rkC^T A^T B^T$. (Заметим, что $(B^T)^{-1} = ((B^{-1})^T)$ Следовательно, B^T, C^T - произвольные обратимые матрицы. □

$$\text{Упражнение. } (AB)^T = B^T A^T$$

Теорема 1.12.1 (PDQ - разложение, равенство базисов). $L : U \rightarrow V$ - линейное отображений,

1. Существуют базисы u, v пространств U, V такие что

$$L_u^v = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}.$$

Размер $E = rkL$.

2. $\forall A \in M_{m \times n}(F) \exists P \in GL_m(F), Q \in GL_n(F) : A = PDQ$, где $D = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$

3. $crkA = r.rkA$

Доказательство. (f_1, \dots, f_k) - базис $Ker L$. Дополним до базиса на пространства $U : g \cup f = u$. Тогда (см. Теорему о ядре и о,разе). $L(g)$ - базис $Im L$. Дополним его до базиса v пространства V .

$$v = (L(g_1), \dots, L(g_l), v_{l+1}, \dots, v_n).$$

$$\begin{aligned} L(g_1)_v &= \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\ &\vdots \\ L(g_l)_v &= \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \\ &\vdots \end{aligned}$$

$$L(f_i) = 0 \text{ таким образом } L_u^v = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$$

□

Определение 24. W - множество матриц-перестановок (группа Вейля).

$$a_{*i} = e_{\sigma(k)}, \quad \text{где } \sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ - биекция.}$$

$B =$ - множество обратимых верхнетреугольных матриц. (борелевская подгруппа) B^- - множество обратимых нижнетреугольных матриц.

Теорема 1.12.2 (разложение Брюа).

$$GL_n(F) = BWB = \{b_1 w b_2 \mid b_1, b_2 \in B, w \in W\}.$$

$w \in W : BwB$ - клетка Брюа.

Доказательство. $a \in GL_n(F)$

$$\exists b, c \in B : bac \in W.$$

Индукция по n

В первом столбце a выберем низший ненулевой элемент.

$$\begin{pmatrix} 1 & & * \\ 0 & 1 & \end{pmatrix}.$$

$$ua = ()$$

Пусть a' - матрица, полученная из uav вычеркиванием i -ого столбца и j -строки. Легко видеть, что ее столбцы линейно независимы. Следовательно, a' - обратима. Тогда по ПИ $\exists b', c' : b'a'c' \in W_{n-1}$. Все получилось!

□

Доказательство. см конспект $GL_n(F) = BWB$

$a \in GL_n(F)$

□

Теорема 1.12.3 (разложение Гаусса).

$$GL_n(F) = WB^-B.$$

$w \in W : wB^-B$ - клетка Гаусса.

Доказательство. Докажем, что $\forall w \in W : BwB \subset wB^-B$

$$BWB = \bigcup_{w \in W} BwB \subset \dots$$

Лемма (1). $D = D_n(F)$ - множество обратимых диагональных матриц. $U = U_n(F)$ - множество унитарных матриц. Тогда $B = DU = UD$.

Упражнение. $a = \begin{pmatrix} \alpha_i & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & 0 \end{pmatrix}, \quad \alpha_i \neq \alpha_j, \text{ если } i \neq j \Rightarrow ab = ba \Rightarrow b \in D$

Доказательство.

$$\begin{pmatrix} \frac{1}{b_{11}} & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & \frac{1}{b_{nn}} \end{pmatrix}$$

□

Лемма (2). $U = \prod_{i < j} X_{ij}$, причем произведение берется в любом наперед заданном порядке.

Доказательство. Будет в теории групп

□

Обозначение. $w \in W : U_w := \prod_{i < j, \sigma(i) > \sigma(j)} X_{ij}$, где σ - перестановка соответствующая w . То есть $w^{-1}X_{ij}w = X_{\sigma(i)\sigma(j)}$.

Теорема 1.12.4 (Приведенной разложение Брюа). $B = \bigcup_{w \in W} U_w w D U$ При этом w, a также элементны из U_w, D, U определены по элементам из B из единственным образом.

Доказательство. □

Следствие. $BwB \subset wB^{-1}B = w(w^{-1}U_w w)B \subset wU^{-}B \subset wB^{-}B$

Доказательство. $BwB = U_w w B$ □

□

Утверждение.

$$BwB \cap Bw'B = \emptyset, \forall w \neq w'.$$

1.13 Лекция 13

15.10.2019 Доказательство теорем

1.14 Лекция 14

17.10.2019

Разложение Гаусса. Идея доказательства: $a \in GL_n(F)$, $wa \in U^{-}B$. Найдем такое w .

Определение 25. Главная подматрица матрицы A - подматрица $k \times k$ стоящая в левом верхнем углу матрицы A .

Лемма. Обратимость любой главной подматрицы не зависит от умножения на U^{-} слева и на U справа.

Доказательство. $a^{(k)}$ - главная подматрица $k \times k$ в a .

$$\begin{pmatrix} b & 0 \\ c & d \end{pmatrix} \begin{pmatrix} a^{(k)} & * \\ * & * \end{pmatrix} = \begin{pmatrix} ba^{(k)} & * \\ * & * \end{pmatrix}.$$

Где $b \in U^{-}F$ Обратимость $a^{(k)}$ равносильно обратимости $ba^{(k)}$, так как b - обратима. □

Лемма. $a \in U^{-}B \Leftrightarrow$ все главные подматрицы обратимы.

Доказательство. Доказываем следствие влево. Индукция по n . База: $n = 1$ - очевидно
Переход:

$$a = \begin{pmatrix} a^{(n-1)} & * \\ * & a_{nn} \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 \\ -xa^{(n-1)} & 1 \end{pmatrix} \begin{pmatrix} a^{(n-1)} & * \\ x & a_{nn} \end{pmatrix} = \begin{pmatrix} a^{(n-1)} & * \\ 0 & * \end{pmatrix}.$$

Дальше применим предположение индукции к $a^{(n-1)}$. Она раскладывается в произведение верхне- и нижнетреугольной.

В обратную сторону следует из прошлой леммы. Действительно, у обратимой верхнетреугольной матрицы все главные подматрицы обратимы, а умножение слева на обратимые нижнетреугольные не меняет их обратимость. \square

Лемма. $\forall a \in GL_n(F) \exists w \in W$: все подматрицы в wa обратимы. По условию $a^{(n-1)}$ обратима,

Доказательство. Индукция по k . Докажем, что существует перестановка $a \in GL_n(F)$ такая, что главные подматрицы размера не более $k \times k$ обратимы.
 $k = 1$

$$a_{*1} = 0 \Rightarrow \exists i : a_{ij} \neq 0.$$

Меняем i - строку с первой.

Переход:

$$a = \begin{pmatrix} a^{(k)} & * \\ * & * \end{pmatrix}.$$

По индукционному предположению все главные подматрицы в $a^{(k)}$ обратимы. Все столбцы линейно независимы, следовательно, ранг матрицы $\begin{pmatrix} a_{11} & \cdots & a_{1k+1} \\ & \ddots & \\ a_{n1} & \cdots & a_{nk+1} \end{pmatrix} =$

$k+1$ $k+1$ - мерное подпространство U в ^{k+1}F . А первые k строк этой матрицы линейно независимы. $X = b_1, \dots b_k, Y = b_1, \dots b_n, \quad b_i = (a_{i1}, \dots a_{ik+1})$.

X - линейно независимый, $\langle y \rangle = U, \dim U = k+1$.

$$\exists Z : X \geq X \geq Y, \text{ где } Z - \text{ базис } U..$$

$$|Z| = k+1 \Rightarrow Z = b_1, \dots b_k, b_i, i > k..$$

Переставляем i -ю строку на $k+1$ место. У получившейся матрицы первые k главных подматриц равны главным подматрицам в a , а строки $k+1$ -й строки главной подматрицы линейно независимы. Следовательно, она независима. \square

$wa \in B^- B$. Домножая на B, B^- , получим, что хотели. \square

Теорема 1.14.1 (Кронекера-Капелли). Система линейных уравнений $Ax = b$ имеет хотя бы одно решение тогда и только тогда, когда $rk A = rk(Ab)$, где (Ab) - расширенная матрица.

Доказательство.

$$rk A = rk(Ab) \Leftrightarrow \langle a_{*1}, \dots \rangle = \langle a_{*1}, \dots, a_{*n}, b \rangle \Leftrightarrow b \in \langle a_{*1}, \dots, a_{*n} \rangle \Leftrightarrow \text{система имеет решение.}$$

□

Chapter 2

Начала теории групп

2.1 Лекция 15

Определение 26. Подмножество $H \subset G$ называется подгруппой, если H – группа относительно операции, заданной в G .

$$H \leq G.$$

Лемма. $H \subset B$ H - подгруппа $\Leftrightarrow \forall h, g \in H : gh, g^{-1} \in H$.

Утверждение. G, H - группы.

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

$$(g, h) \cdot (g', h') := (g \cdot g', h \cdot h').$$

Определение 27. $\varphi: X \rightarrow Y, (X, *), (Y, \dots) -$

φ - гомоморфизм групп, если:

$$\varphi(x_1 * x_2) = \varphi(x_1) \cdot \varphi(x_2), \quad \forall x_1, x_2 \in X.$$

Изоморфизм - биективный гомоморфизм.

Лемма. $G, H \leq F$

1. $G \cap H = \{1\}$

2. $G \cdot H = F$

3. $\forall g \in G, h \in H : gh = hg$

Тогда $F \cong G \times H$.

Доказательство. $\varphi : G \times H \rightarrow F$

$$\varphi(g, h) = g \cdot h$$

$$\varphi((g, h) \cdot (g', h')) = \varphi(gg', hh') = gg'hh'.$$

$$\varphi(g, h) \cdot \varphi(g', h') = ghg'h'.$$

(1) $\Leftrightarrow \varphi$ - сюръективно.

$$\varphi(g, h) = \varphi(g', h') \Leftrightarrow gh = g'h' \Leftrightarrow g'^{-1}g = h'h^{-1} = 1 \Rightarrow g' = g, h' = h.$$

□

2.2 Лекция 16

22.10.2019

Пример. $\ln : \mathbb{R}_{>0}^* \rightarrow (\mathbb{R}, +)$

$\ln ab = \ln a + \ln b$ - гомоморфизм.

Определение 28.

$\varphi G \rightarrow H$ - гомоморфизм.

$$Im\varphi = \{\varphi(g) \mid g \in G\}.$$

$$Ker\varphi = \varphi^{-1}1 = \{g \in G \mid \varphi(g) = 1\}.$$

Лемма. $Im\varphi$ и $Ker\varphi$ - подгруппы.

Доказательство.

$$a, b \in Ker\varphi.$$

$$\varphi(ab) = \varphi(a)\varphi(b) = 1 \Leftrightarrow ab \in Ker\varphi.$$

$$\varphi(a^{-1}) = \varphi(a)^{-1} = 1 \Rightarrow a^{-1} \in Ker\varphi.$$

□

Лемма.

$\varphi(g) = h, \quad \varphi : G \rightarrow H$ - гомоморфизм.

$$\varphi^{-1} = \underbrace{gKer\varphi}_{\text{левый смежный класс по ядру } \varphi} = \underbrace{Ker\varphi g}_{\text{правый}}.$$

Доказательство. $\varphi(x) = h = \varphi(g) \Leftrightarrow \varphi\varphi^{-1} = 1 \Leftrightarrow \varphi(xy^{-1}) = 1 \Leftrightarrow xy^{-1} \in Ker\varphi \Leftrightarrow x \in Ker\varphi g$

□

Определение 29. $H \leq G$

H называется нормальной подгруппой, если $gH = Hg \quad g \in G. (H \trianglelefteq G)$

Замечание. $g^{-1}Hg = H \quad \forall g \in G \Leftrightarrow g^{-1}Hg \subseteq H \quad \forall g \in G$

Лемма. $H \leq G$

$$g_1H \cap g_2H \neq \emptyset \Leftrightarrow g_1H = g_2H.$$

Доказательство. $x \in g_1H \cap g_2H \Rightarrow x = g_1h_1 = g_2h_2, \quad h_1, h_2 \in H.$ Тогда $g_1 = g_2(h_2h_1^{-1}) \Rightarrow g_1H = g_2(h_2h_1^{-1})H.$ \square

Следствие. $G = \bigsqcup_{g \in X} gH$, где X - множество представителей левых смежных классов

по H .

$$g_1 \stackrel{H}{\sim} g_2 \Leftrightarrow g_1^{-1}g_2 \in H$$

Лемма.

$$|g_1H| = |g_2H|, \quad \forall g_1, g_2 \in G, H \leq G.$$

Доказательство.

$$\left(\begin{array}{l} g_1H \rightarrow g_2H \\ x \mapsto g_2g_1^{-1}x \end{array} \right).$$

Обратная $y \mapsto g_1g_2^{-1}y$ \square

Теорема 2.2.1 (Лагранж). G - конечна группа. Тогда $|G| = |H||G : H|$, где $|G : H|$ - количество левых смежных классов G по H . $|G : H|$ - индекс H в G .

Доказательство. Из прошлой леммы и следствия \square

Следствие. Если $p = |G| \in \mathbb{P}$, то $\forall g \in G \setminus 1 : G = \{1, g, \dots, g^{p-1}\} \cong \mathbb{Z}_p$

Доказательство. $\{g^n \mid n \in \mathbb{Z}\} \leq G = \langle g \rangle.$

$|\langle g \rangle|$ делит p и больше единицы, так как содержит единицу и $g \neq 1$. Следовательно, $|\langle g \rangle| = p.$

Докажем, что все элементы $1, g, \dots, g^{p-1}$ различны. Рассмотрим $0 \leq k, l \leq p-1$. Пусть $g^k = g^l \Rightarrow g^{k-l} = 1$. При $k-l \neq 0$, $g^n = g^{m(k-l)+r} = g^r, \quad r < k-l \leq p-1$. Тогда бы $\{1, g, \dots, g^{k-l-1}\} = \langle g \rangle$. Из чего следует $|\langle g \rangle| < p$. Противоречие.

Рассмотрим $k \in [0, p-1]$. $g^p = g^k \Leftrightarrow g^{p-k} = 1 \Rightarrow k = 0 \Rightarrow g^p = 1$.

Теперь проверим изоморфность. $\varphi : \mathbb{Z}_p \rightarrow G, \varphi(k) = g^k$ \square

Определение 30. Группа, порожденная одним элементом, называется циклической.

Утверждение. Любая циклическая группа изоморфна \mathbb{Z} или \mathbb{Z}_n .

Доказательство. $G = \{g^m \mid m \in \mathbb{Z}\}$. Разберем два случая:

1. $g^m \neq 1 \forall m \in \mathbb{N} \Rightarrow g^m \neq 1 \forall m \neq 0.$

$$\varphi \mathbb{Z} \rightarrow G, \quad \varphi(m) = g^m.$$

$$\varphi(m+k) = g^{m+k} = g^m g^k = \varphi(m)\varphi(k).$$

2. Пусть n - наименьшее натуральное число, такое что $g^n = 1$.

$$\varphi : \mathbb{Z} \rightarrow G, \quad \varphi(m) = g^m \text{ сюръективно ..}$$

$$g^m = 1 \Leftrightarrow g^{nk+r} = 1 \Leftrightarrow g^r = 1 \Rightarrow r = 0$$

$$\text{Ker}\varphi = \{m \mid g^m = 1\} = n\mathbb{Z}.$$

□

Определение 31. Порядок $g \in G$ - наименьшее натуральное число, такое что $g^n = 1$. $\text{ord}(g) = |\langle g \rangle|$

Утверждение (из теоремы Силова). $|G| = p^m$, $p \nmid m$. Тогда $\exists H \leq G : |H| = p^k \forall h \in H \setminus 1$.

$\text{ord}(h \mid p^k)$, следовательно, $h^{p^l} = 1 \Rightarrow (h^{p^{l-1}})^p = 1$

2.3 Лекция 17

24.10.2019

G - группа.

Определение 32. $S \subseteq G$

$\langle S \rangle$ - наименьшая подгруппа содержащая S .

Утверждение. $\langle S \rangle = \{S_1^{n_1} \cdot \dots \cdot S_k^{n_k} \mid k \in \mathbb{N}, S_i \in S, n_i \in \mathbb{Z}\}$, для абелевой $:s_i \neq s_j$ при $j \neq i$.

Определение 33. $s^g := g^{-1}sg$

Замечание. $(s^g)^h = s^{g^h}$
 $h(gS) = {}^h g S$

Свойства.

$$1. (s_1 s_2)^g = s_1^g s_2^g$$

$$2. (s^g)^{-1} = (s^{-1})^g$$

$s \mapsto s^g$ - автоморфизм G .

Определение 34. $H \leq G$

$$H^G = \langle h^g \mid h \in H, g \in G \rangle - \text{нормальное замыкание } H \text{ в } G.$$

Нормальное замыкание равно наименьшей нормальной подгруппе в G , содержащей H .

$\langle S \rangle^G$ - наименьшая нормальная подгруппа, содержащая S .

$s^g = g^{-1}sg$ - сопряженный с s при помощи g .

$$H^g = \langle h^g \mid h \in H \rangle - \text{подгруппа, сопряженная с } H \text{ при помощи } g.$$

Определение 35. $aba^{-1}b^{-1} = [a, b]$ – коммутатор элементов a, b .

Замечание. $ab = ba \Leftrightarrow aba^{-1}b^{-1} = 1$

Утверждение. $\varphi : G \rightarrow A$ – гомоморфизм в абелеву группу.

$$\varphi([g, h]) = 1$$

Тогда $[G, G] = \langle [g, h] \mid h, g \in G \rangle \subseteq \text{Ker} \varphi$ – коммутант G .

$$[g, h]^f = [g^f, h^f]$$

Утверждение. $[a, b]^{-1} = [a, b]$

Определение 36. Центр группы – $\text{Center}(G) = Z(G) := \{c \in G \mid cg = gc \forall g \in G\}$

Обозначение.

$G/H = \{gH \mid g \in G\}$ – множество левых смежных классов.

$H \setminus G = \{Hg \mid g \in G\}$ – множество левых смежных классов.

$$H \trianglelefteq G \quad (H^g = H \forall g \in G)$$

Определение 37. Фактор-группа G/H – множество смежных классов по H с операцией $(g_1H)(g_2H) = g_1g_2H$.

корректность определения.

$$g'_1 \in g_1H \Rightarrow g'_1h_1.$$

$$g'_2 \in g_2H \Rightarrow g'_2h_1.$$

$$g_1 \mid + g_2 \mid = g_1h_1g_2h_2 = g_1g_2g_2^{-1} = (g_1g_2)(g_2^{-1}h_1g_2)h_2 \in g_1g_2H.$$

□

Определение 38. $\pi_H : G \rightarrow G/H, g \mapsto gH$

π_H – эпиморфизм, $\text{Ker} \pi_H = H$

Теорема 2.3.1 (универсальное свойство факторгруппы). $H \trianglelefteq G$

Для любого гомоморфизма $\varphi : G \rightarrow F$, такого что $H \leq \text{Ker} \varphi \exists! \bar{\varphi} : G/H \rightarrow F$ коммутативна для диаграммы

$$\begin{array}{ccc} G & \xrightarrow{\pi_H} & G/H \\ \downarrow \varphi & & \downarrow \exists! \bar{\varphi} \\ F & & F \end{array}$$

Теорема 2.3.2. $\varphi G \rightarrow F$

$$G/\text{Ker} \varphi \cong \text{Im} \varphi.$$

Доказательство. Заменяем F на $Im\varphi$.

$$\varphi' \rightarrow Im\varphi \quad Ker\varphi' = Ker\varphi.$$

По прошлой теореме существует единственное:

$$\hat{\varphi}: \begin{array}{ccc} G/Ker\varphi & \rightarrow & Im\varphi \\ \uparrow \pi & & \uparrow \varphi' \\ G & & G \end{array}.$$

φ - сюръективно. Следовательно, φ' - сюръективно.

□

$gKer\varphi \in Ker\hat{\varphi} \Leftrightarrow \hat{\varphi}(gKer\varphi) = 1 \Leftrightarrow \varphi(g) = 1 \Leftrightarrow gKer\varphi = Ker\varphi = 1_{G/Ker\varphi}$. Следовательно, $\hat{\varphi}$ - инъективно .

Пример. $\mathbb{Z} \rightarrow \mathbb{Z}_n, \quad \varphi(x) = x \bmod n$.

$$Ker\varphi = n\mathbb{Z}$$

$$\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

2.4 Лекция 18

Пример.

$$U_n(F) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}.$$

Обозначим

$$U_n(k) = \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & * \\ 0 & 1 & 0 & \dots & & * \\ 0 & 0 & 1 & 0 & \dots & \\ \vdots & & & & & \\ 0 & 0 & \dots & 0 & & 1 \end{pmatrix} \right\} = \{a \mid a_{ij} = 1, a_{ij} = 0, \forall i \neq j, j - i < k\}.$$

Матрица трансвекций:

$$t_{ij}(\alpha) = \begin{pmatrix} 1 & \dots & \alpha & \dots & 0 \\ 0 & & \ddots & & 0 \\ 0 & & 0 & & 1 \end{pmatrix}.$$

Тогда $U_n^{(k)}(F) = U_n^{(k)} = \langle t_{ij}(\alpha) \mid j - i \geq k, \alpha \in F \rangle$ - группа.

Лемма. $U_n^{(k)} \setminus U_n^{(k-1)} \cong \underbrace{F \times \dots \times F}_{n-k}, \quad F = (F, +)$. Проверим, что есть гомоморфизм,

и применим теорему о гомоморфизме.

Доказательство.

$$\varphi : U_n^k \rightarrow F^{n-k}, \quad \varphi(a) = (a_{i-k+1}, \dots, a_{n-k+1})^T.$$

Заметим, что φ - сюръективна, $\varphi^{-1}(e) = U_n^{k+1}$.

$$a, b \in U_n^{(k)}, \quad (a, b)_{i-k+1} = \sum_{j=1}^n a_{ij} \cdot b_{i-k+1+j} = b_{i-k+1} + a_{i-k+1}.$$

Тогда $\varphi(a \cdot b) = \varphi(a) + \varphi(b)$. Следовательно, φ - гомоморфизм. □

Определение 39. $[a, b] = aba^{-1}b^{-1}$ - коммутатор.

$H, K \leq G$, $[H, K] := \langle [h, k] \mid h \in H, k \in K \rangle$ - коммутант.

Утверждение. $[h, k]^g = [h^g, k^g] \Rightarrow [G, G] \trianglelefteq G$.

Утверждение. $\varphi : G \rightarrow A$ - гомоморфизм.

A - абелева $\implies [G, G] \subseteq \text{Ker} \varphi$.

Доказательство.

$$\varphi([g, h]) = [\varphi(g), \varphi(h)] = 1.$$

Тогда

$$[g, h] \in \text{Ker} \varphi, \quad \forall g, h \in G.$$

Из этого следует, что $[G, G] \subseteq \text{Ker} \varphi$. □

Следствие. $[U_n^{(k)}, U_n^{(k)}] \leq U_n^{(k+1)}$

Лемма. $[U_n^{(k)}, U_n^{(m)}] = U_n^{(m+k)}$, (если $l \geq n$, то $U_n^l := e$).

Доказательство.

$$[t_{ij}(\alpha), t_{jh}(\beta)] = t_{ih}(\alpha\beta), \quad i, j, h \text{ - различны.}$$

$\forall i, h : h - i \geq m :$

$$\exists j : j - i \geq k, h - j \geq m.$$

Следовательно, любая образующая (и сама группа) содержится: $U_n^{(m+k)} \subseteq [U_n^{(m)}, U_n^{(k)}]$.

В обратную сторону:

$$\begin{aligned} [xy, z] &= xyz y^{-1} x^{-1} z^{-1} = x(yzy^{-1} z^{-1} z x^{-1} z^{-1}) = \\ &= x[y, z] x^{-1} z x^{-1} z^{-1} = [y, z]^{x^{-1}} \cdot [x, z] \end{aligned}$$

Заметим, что

$$[t_{ij}(\alpha), t_{lh}(\beta)] = e, \text{ если } j \neq l, h \neq i.$$

Тогда

$$t_{ij}(\alpha) \in U_n^{(k)}, \quad t_{lh}(\beta) \implies [t_{ij}(\alpha), t_{lh}(\beta)] \in U^{(m+k)n}.$$

Посчитаем

$$\underbrace{[t_{ij}(\alpha), t_{li}(\beta)]}_{j \neq l} = [t_{li}(\beta), t_{ij}(\alpha)]^{-1} = t_{lj}(\beta\alpha)^{-1} = t_{lj}(-\beta\alpha).$$

Так как $U_n^{(k+m)}$ - нормальная подгруппа, то есть трансвекцию во включении 2.4 можно заменить на произведение трансвекций, то есть на любые элементы $U_n^{(k)}, U_n^{(m)}$. Доказали обратное утверждение. \square

2.5 Лекция 19

2.5.1 Поговорим о коммутаторах

Лемма.

$$H = \langle X \rangle \leq G = \langle Y \rangle.$$

Тогда

$$H \trianglelefteq G \iff x^y \in H \quad \forall x \in X, y \in Y.$$

Доказательство. В правую сторону очевидно (по определению), обратно: нужно доказать, что $h^g \in H \quad \forall h \in H, g \in G$. Разложим $g = y_1 \cdot \dots \cdot y_m$, $y_i = U \cup Y^{-1}$.

Индукция по m . При $m = 0 : g = 1 \wedge h^1 = h \in H$.

Переход: $m \geq 1$. По ИП $h^{y_1 \dots y_{m-1}} \in H$, $h = x_1 \dots x_n$, $x_i \in X \cup X^{-1}$.

$$h^y = (h^{y_1 \dots y_{m-1}})^y_m = x_1^{y_m} \dots x_n^{y_m}.$$

$x_i \in X \Rightarrow x_i \in H$ по условию.

$$x_i \in X^{-1} \Rightarrow ((x_i)^{-1})^{y_m} = ((x^{-1})^{y_m})^{-1} \in H.$$

\square

Замечание. В определении нормальной подгруппы вместо h^g также можно написать $[g, h]$, так как для $h \in H, g \in G$

$$[g, h] = ghg^{-1}h^{-1} = h^{g^{-1}}h \in H \iff h^{g^{-1}} \in H.$$

g^{-1} можно заменить на g .

Аналогично в лемме можно заменить x^y на $[x, y]$.

Свойства (Формулы для коммутаторов). 1. $[x, y] = [y, x]^{-1}$

$$2. [xy, z] = {}^x[y, z] \cdot [x, z]$$

$$3. [x, y]^z = [x^z, y^z]$$

Лемма. $H, K \leq G$, $[H, K] \trianglelefteq \langle H \cup K \rangle$

$h \in H, k \in K, x \in H$ (для $x \in K$ аналогично).

$$[h, k]^x = {}^{x^{-1}}[h, k] = [h^{-1}h, k]^{-1} \cdot [x^{-1}, k]^{-1} \in [H, K].$$

2.5.2 Возвращаемся к матрицам

$$U_n^{(k)}(F) = U_n^{(k)} = \{a \in M_n(F) \mid a_{i,i} = 1, a_{i,j} \forall i \neq j, j-i < k\} = \langle t_{i,j}(\alpha) \mid \alpha \in F, j-i \geq k \rangle.$$

Лемма. $U_n^{(k)} \trianglelefteq U_n = U_n^{(1)}$

Доказательство. Докажем, что $a = [t_{i,j}(\alpha), t_{h,l}(\beta)] \in U_n^{(k)} \quad \forall j-i \geq k. \quad l > h$

Первый случай $i \neq h, i \neq l \Rightarrow a = e \in U_n^{(k)}$.

Второй случай $j = h \Rightarrow i \neq j : \quad a = t_{i,l}(\alpha\beta), l-i \geq k+1$. Тогда $a \in U_n^{(k+1)} \leq U_n^{(k)}$.

Третий случай $j \neq h, i = l : \quad a = [t_{h,j}(\beta), t_{i,j}(\alpha)]^{-1} = t_{h,j}(\beta\alpha)^{-1} = t_{h,j}(-\beta\alpha). \quad j-h \geq k+1 \Rightarrow t_{h,j}(-\beta\alpha) \in U_n^{(k+1)}.$ \square

Лемма. Пусть \preceq - отношение линейного порядка на $P = \{(i, j) \mid 1 \leq i < j \leq n\}$.

$$U_n(F) = \left\{ \prod_{(i,j) \in P} t_{ij}(\alpha_{ij}) \mid \alpha_{ij} \in F \right\}.$$

Замечание. $H \trianglelefteq G, \quad x, y \in G : \quad xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow x \equiv y \pmod{H}$

Доказательство. Рассмотрим элемент $h \in U_n(F)$. Докажем по индукции (по k), что

$$h \equiv \prod_{\substack{(i,j) \in P \\ 0 \leq j-i < k}} t_{ij}(\alpha_{ij}) \pmod{U_n^{(k)}}.$$

При $k = 1$ утверждение очевидно, доказывать нечего.

Переход: $k-1 \rightarrow k$

По предположению индукции

$$h \equiv \prod_{0 < j-i < k-1} t_{ij}(\alpha_{ij}) \pmod{U_n^{(k-1)}} = \prod_{0 < j-i < k-1} t_{ij}(\alpha_{ij}) \cdot \prod_{j-i=k-1} t_{ij}(\alpha_{ij}) U_n^{(k)}$$

Так как коммутатор $[u, t_{i,i+k-1}(\alpha)] \in U_n^{(k)} \quad \forall u \in U_n$. То есть $[u, t_{i,i+k-1}(\alpha)] \equiv 1 \pmod{U_n^{(k)}}$. Это равносильно

$$ut_{i,i+k-1}(\alpha) \equiv t_{i,i+k-1} \cdot u \pmod{U_n^{(k)}}.$$

Получаем

$$h \equiv \prod_{0 < j-i < k} t_{ij}(\alpha_{ij}) \pmod{U_n^{(k)}}.$$

\square

Введем обозначения: w - матрица перестановки.

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in U.$$

$$\begin{pmatrix} \bullet & & 0 \\ & \ddots & \\ 0 & & \bullet \end{pmatrix} \in D.$$

$$B_n = D_n U_n = U_n D_n \quad (\forall d \in D_n : U_n^d = U_n).$$

$B_n w B_n = U_n D_n w B_n$, где $U_w = \langle t_{ij}(\alpha) \mid \alpha \in F, j > i, t_{ij}(\alpha)^w \in U_n^- \rangle$ - ниже треугольные.
 $U_w = \langle t_{ij}(\alpha) \mid j > 1, \alpha \in F, t_{ij}(\alpha)^w \in U_n \rangle$.

Следствие. Матрица U_n представляется в виде произведения трансвекций в любом порядке. $U_n = U_w \cdot \bar{U}_w$

Доказательство. □

Следствие (приведенное разложение Брюа). $B_n w B_n \subseteq w B_n^- B_n$

Доказательство. $B_n w B_n = U_n w B_n = w U_w w^{-1} \bar{U}_w w B_n = w \underbrace{U_w^w}_{\subseteq U_n^-} \underbrace{\bar{U}_w^w B_n}_{\subseteq U_n} \subseteq w U_n^- B_n = w B_n^- B_n$ □

2.6 Лекция 20

2.6.1 Симметрическая группа

Определение 40 (Перестановка). $\sigma \in S_n \iff \sigma : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}$ Табличная запись перестановки:

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}, i_j \neq i_k (j \neq k).$$

Циклическая запись перестановки:

$$\tau = (j_1, \dots, j_n) \iff \tau(j_1) = j_2, \tau(j_2) = j_3, \dots, \tau(j_{n-1}) = j_n, \tau(j_n) = j_1, \quad \tau(i) = i, \forall i \neq j_k.$$

Определение 41. $(j_1 \dots j_n)$ и $(k_1 \dots k_m)$ независимы, если $j_h \neq j_l \quad \forall h, l$.

Лемма. Любая перестановка равна произведению независимых (композиции) циклов.

Определение 42. Циклический (цикленный) тип перестановки – набор из длин независимых циклов, в произведение которых раскладывается перестановка.

Замечание. В определении слово "набор" подразумевает мультимножество, то есть порядок не важен, но элементы повторяются.

Пример. $(12)(345) \in S_6$ записывают $2 + 3$.

Лемма.

$$\sigma(i_1, i_2, \dots, i_k) \sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_k)).$$

Следовательно, сопряжение не меняет циклический тип.

Доказательство. $\sigma(i_1 \dots i_k) \sigma^{-1}(\sigma(t_j)) = \sigma \circ (i_1 \dots i_k) \sigma(i_{l+1 \bmod m})$, где $\bmod m$ - почти модуль (вместо 0 будет m). \square

Определение 43. Отношение на группе G :

$$x \sim_c y \Leftrightarrow \exists z : x = y^z.$$

$$x = y^z \wedge y = ab \Rightarrow x = (a^b)^z = a^{bz}.$$

Класс эквивалентности " \sim_c " – класс сопряженных элементов.

Теорема 2.6.1. Класс сопряженных элементов в S_n состоит из всех перестановок фиксированного циклического типа.

Доказательство. Следует из леммы 2.6.1 \square

Пример. Рассмотрим группу S_4 и перестановки циклического типа $2 + 2$:

$$\begin{aligned} &(12)(34) \\ &(13)(24) \\ &(14)(32) \end{aligned}$$

$$\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$$

Еще есть нейтральный класс e и $2, 3, 4$. Двумерная группа Клейна

$$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

- единственная нормальная подгруппа в S_n для любого n , индекс которой более 2.

Упражнение. Найти S_4/K_4 . Там 6 элементов.

Утверждение. $\text{ord}(ab) \mid \text{НОК}(\text{ord}(a), \text{ord}(b))$.

Порядок перестановки равен НОКу порядков независимых циклов.

2.7 Лекция 21

2.7.1 Продолжаем возиться с перестановками. Четность.

Определение 44 (Инверсия). $\sigma \in S_n$.

Инверсия в σ – пара $(i, j) : i < j \wedge \sigma(i) > \sigma(j)$.

Пример. Четыре инверсии:

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

Определение 45 (Четность перестановки).

$$\varepsilon : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}.$$

$\sigma \mapsto$ количество инверсий по модулю 2.

Определение 46. Транспозиция – цикл длины 2.

$$\tau(i) = \tau(j), \quad \tau(j) = \tau(i), \quad \tau(k) = k.$$

Лемма. Любая перестановка σ раскладывается в произведении транспозиций соседних индексов.

$$S_n = \langle (12), (23) \dots (n-1 \ n) \rangle.$$

Доказательство. Индукция по количеству инверсий I в $\sigma \in S_n$.

База: $I = 0$ Это $\sigma = id$.

Переход: $I > 0$. Заметим, что

$$\exists i : \sigma(i) > \sigma(i+1).$$

Тогда рассмотрим $\tau = \sigma \circ (i, i+1)$.

$$\tau(i) = \sigma(i+1) < \tau(i+1) = \sigma(i).$$

Так как $\tau(k) = \sigma(k) \quad \forall k \notin \{i, i+1\}$, количество инверсий стало на одну меньше, чем количество инверсий в σ . Теперь по предположению индукции полученная перестановка раскладывается, а тогда и σ раскладывается. \square

Лемма. $\tau = \sigma(i \ i+1) \Rightarrow |I(\tau) - I(\sigma)| = 1$

Лемма. Если $\sigma = \tau_1 \cdot \tau_2 \dots \cdot \tau_k, \quad \forall i : \tau_i$ - транспозиция соседних индексов, то

$$\varepsilon(\sigma) = k \pmod{2}.$$

Теорема 2.7.1. $\varepsilon : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ - гомоморфизм группы.

Доказательство.

$$\begin{aligned} \sigma &= \tau_1 \cdot \dots \cdot \tau_k \\ \rho &= \tau_{k+1} \cdot \dots \cdot \tau_n \\ \sigma \cdot \rho &= \tau_1 \cdot \dots \cdot \tau_n \end{aligned} \quad \forall i : \tau_i = (j \ j+1).$$

Проверим требуемые свойства:

$$\varepsilon = k \pmod{2}, \quad \varepsilon(\rho) = n - k \pmod{2}$$

$$\varepsilon(\sigma\rho) = m \pmod{2} = \varepsilon(\sigma) + \varepsilon(\rho) \pmod{2}$$

$$\varepsilon(\rho^{-1}\sigma\rho) = -\varepsilon(\rho) + \varepsilon(\sigma) + \varepsilon(\rho)$$

$$\varepsilon((i_1, \dots, i_k)) = \varepsilon((1, \dots, k)) = k - 1 \pmod{2} \quad \square$$

Рассмотрим кольцо $(\mathbb{Z}_n, +_n, \cdot_n)$. \mathbb{Z}_n^* - множество обратимых элементов.

$x \in \mathbb{Z}_n$ - обратимо тогда и только тогда, когда $\gcd(x, n) = 1$.

$\varphi|\mathbb{Z}_n^*|$ - количество чисел от 1 до $n-1$ взаимно простых с n . Из теоремы Лагранжа очевидно следует, что:

$$x^{\varphi(n)} \pmod{n} = 1.$$

Утверждение. A – абелева группа. $a, b \in A$, $\text{ord}(a) = m$, $\text{ord}(b) = n$, $h = \text{lcm}(m, n)$

$$(ab)^k = a^k b^k = (a^m)^x (b^n)^y = 1.$$

Тогда $\text{ord}(ab) \mid k$.

Лемма. $\langle a \rangle \cap \langle b \rangle = \{1\} \Rightarrow \text{ord}(ab) = \text{lcm}(\text{ord}(a), \text{ord}(b))$

Доказательство.

$$(ab)^l = 1 \Rightarrow \underbrace{a^l}_{\in \langle b \rangle} = \underbrace{b^{-l}}_{\in \langle b \rangle} = 1.$$

Тогда

$$\left. \begin{array}{l} \text{ord}(a) \mid l \\ \text{ord}(b) \mid l \end{array} \right\} \Rightarrow \text{lcm}(\text{ord}(a), \text{ord}(b)) \mid l.$$

□

Следствие.

$$a \in A, b \in B, \quad A, B \leq A \times B.$$

Тогда $\text{ord}(ab) = \text{lcm}(\text{ord}(a), \text{ord}(b))$

Следствие.

$$\text{lcd}(\text{ord}(a), \text{ord}(b)) = 1.$$

Тогда $\text{ord}(ab) = \text{lcm}(\text{ord}(a), \text{ord}(b))$

Доказательство. $|\langle a \rangle \cap \langle b \rangle| = h$

$$h \mid |\langle a \rangle| \wedge h \mid |\langle b \rangle| \Rightarrow h \mid \gcd(\text{ord}(a), \text{ord}(b)) = 1 \Rightarrow h = 1.$$

Следовательно, $\langle a \rangle \cap \langle b \rangle = \{1\}$.

□

Следствие. Порядок перестановки равен наибольшему общему делителю порядков независимых циклов, в произведение которых она раскладывается.

Определение 47 (Экспонента (показатель)). $\exp(A)$ – наименьшее натуральное число, такое что $a^n = 1 \quad \forall a \in A$.

Лемма. $\exp(A) = \text{lcm}_{a \in A}(\text{ord}(a))$

Теорема 2.7.2. A – абелева группа. $\exp(A) < \infty$.

Тогда $\exists a \in A : \text{ord}(a) = \exp(A)$

Доказательство. Разложим экспоненту на простые множители:

$$\exp A = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}, \quad \forall i \in [1, m] : p_i \in \mathbb{P}, k_i \in \mathbb{N}.$$

Так как $\exp(A) = \text{lcm}_{x \in A}(\text{ord} x)$, существует $\forall i \in [1, m] x_i : p_i^{k_i} \mid \text{ord}(x_i)$.

$$\text{ord} x_i = p_i^{k_i} \cdot n_i = \text{ord}(x_i^{n_i}) = p_i k_i.$$

Так как порядки всех $x_i^{n_i}$ взаимно просты, то

$$\text{ord}\left(\prod_{i=1}^m x_i^{n_i}\right) = \prod_{i=1}^m \text{ord}(x_i^{n_i}) = \prod_{i=1}^m p_i k_i = \exp(A).$$

□

2.8 Лекция 22

Утверждение. $\varphi : G \rightarrow h$ -гомоморфизм. $g \in G$. Тогда $\text{ord}(\varphi(g)) \mid \text{ord} g$.

Доказательство. Рассмотрим сужение $\tilde{\varphi} : \langle g \rangle \rightarrow \varphi(\langle g \rangle) = \langle \varphi(g) \rangle$.

$$\langle \varphi(g) \rangle \cong \langle g \rangle / \text{Ker} \tilde{\varphi}.$$

$$\text{ord} \varphi(g) = |\langle \varphi(g) \rangle| = \frac{|\langle g \rangle|}{|\text{Ker} \tilde{\varphi}|}.$$

Замечание. Можно использовать одну из доказанных лемм, тогда решение будет проще. \square

Теорема 2.8.1. $p \in \mathbb{P} (\mathbb{Z}/p^k\mathbb{Z})^*$ - циклическая, если $p \neq 2$ или $k \leq 2$. Иначе $(\mathbb{Z}/p^k\mathbb{Z})^* \cong C_2 \times C_{2^{k-2}}$

Доказательство. Обозначим $G = \mathbb{Z}/n\mathbb{Z}$

$$|(\mathbb{Z}/p^k\mathbb{Z})^*| = p^k - p^{k-1} = p^{k-1}(p-1).$$

Рассмотрим множество чисел вида $1 + px$. Они не делятся на p . Чтобы были меньше $(|\mathbb{Z}_n|)^*$, ограничим x .

$$H = \{1 + px \mid x \in \{0, \dots, p^{k-1} - 1\}\}.$$

Утверждение. H - подгруппа.

$$(1 + px)(1 + py) = 1 + pz \in H.$$

Если

$$(1 + px)(1 + py) \equiv 1 \pmod{p^k}.$$

$$a + apx + py + p^2xy \equiv 1 \pmod{p^k}.$$

Следовательно, $a = 1 + pz$. *Обратный элемент:*

$$(1 + px)^{-1} = (1 + pz + py) \in H.$$

$$|H| = p^{k-1}, |G/H| = p-1 \text{ - циклическая (докажем позже).}$$

$$\exists b \in G : \text{ord}(bH) = p-1, \quad \pi(b) = bH, \pi : G \rightarrow G/H.$$

То есть $p-1 \mid \text{ord} b$. Получаем $\exists l \in \mathbb{N} : \text{ord} b^l = p-1$. (или можно сказать, $p-1 \mid \exp(G)$).

По следствию из теорема Лагранжа $|H| \cdot p \cdot p^{k-1} \wedge 1+p \in H \Rightarrow (1+p)^{p^{k-1}} \equiv 1 \pmod{p^k}$. Тогда $\text{ord}(1+p) \mid p^{k-1}$.

Осталось доказать, что

$$(1+p)^{p^{k-2}} \not\equiv 1 \pmod{p^k}.$$

Будем доказывать по индукции. Для $k = 2$ - очевидно. При $k > 2$:

$$(1+p)^{p^{k-3}} = 1 + p^n x, \quad p \nmid p.$$

По предположению индукции $1 \leq n < k - 1$.

$$(1+p)^{p^{k-2}} = \left((1+p)^{p^{k-3}} \right)^p = (1+p^n x)^p = 1 + p \cdot p^n + \sum_{i=2}^p C_p^i p^{ni} x^i \equiv 1 + p^{n+1} x + p^{n+2} y \pmod{p^{n+2}},$$

так как

$$(1+p)^{p^{k-2}} = 1 + p^{n+1} \underbrace{(x + py)}_{\text{не делится на } p}.$$

$$n+1 < k \Rightarrow p^k \nmid (1+p)^{p^{k-2}} - 1$$

Ремарка.

$$C_p^i = \frac{p(p-1)!}{(p-1)! i!} \vdots p.$$

Ремарка. Если $p = 2$, то при $i = 2, n = 1$

$$C_p^i = 1 \Rightarrow C_p^i p^2 \not\vdots p^3.$$

Поэтому для $p = 2$ эти рассуждения не работают.

Теперь разберем случай $p = 2$.

$$|G| = 2^{k-1}, k \geq 3.$$

1. Любой элемент имеет порядок не более 2^{k-1} , то есть $(1+2x)^{2^{k-2}} \equiv 1 \pmod{2^k}$.

Индукция по k . База $k = 3$.

$$(1+2x)^2 = 1 + 4x + 4x^2 = 1 + 4x(x+1) \equiv 1 \pmod{2^3},$$

так как либо x , либо $x+1$ четное.

Переход. По индукционному предположению

$$(1+2x)^{2^{k-3}} = 1 + 2^{k-1} y.$$

Дальше

$$(1+2x)^{2^{k-2}} = (1+2^{k-1} y)^2 = 1 + 2^k y + 2^{2k-2} y^2 \equiv 1 \pmod{2^k}.$$

Доказано.

$\text{ord}_G 5 = 2^{k-2}$, то есть

$$5^{2^{k-3}} \not\equiv 1 \pmod{2^k}.$$

Индукция по k . База $k = 3$.

$$5 \not\equiv 1 \pmod{8}.$$

Переход: по индукционному предположению

$$5^{2^{k-4}} \not\equiv 1 \pmod{2^{k-1}}.$$

$$5^{2^{k-1}} = 1 + 2^n z, \quad 1 < n < k-1, \quad 2 \nmid z.$$

Ремарка. $n > 1$, так как $5 \equiv 1 \pmod{2^2}$

Тогда

$$\begin{aligned} 5^{2^{k-3}} &= (1 + 2^n \cdot z)^2 = 1 + 2 \cdot 2^n \cdot z + 2^{2n} \cdot z^2 = \\ &= 1 + 2^{n+1}(z + z^2 \cdot 2^{n-1}) \not\equiv 1 \pmod{2^{n+2}} \quad . \end{aligned}$$

□