

Конспект по алгебре
I семестр
СПбГУ, факультет математики и компьютерных наук
(лекции Степанова Алексея Владимировича)

Тамарин Вячеслав

23 декабря 2019 г.

Оглавление

1	Линейная алгебра. Векторные пространства	5
1.1	Лекция 1	5
1.2	Лекция 2	7
1.3	Лекция 3	7
1.3.1	Произведение матриц	8
1.4	Лекция 4	9
1.5	Лекция 5	11
1.6	Лекция 6	11
1.7	Лекция 7	11
1.8	Лекция 8	11
1.9	Лекция 9	13
1.10	Лекция 10	16
1.11	Лекция 11	16
1.12	Лекция 12	18
1.13	Лекция 13	21
1.14	Лекция 14	21
2	Начала теории групп	23
2.1	Лекция 15	23
2.2	Лекция 16	24
2.3	Лекция 17	25
2.4	Лекция 18	27
2.5	Лекция 19	29
2.5.1	Поговорим о коммутаторах	29
2.5.2	Возвращаемся к матрицам	29
2.6	Лекция 20	31
2.6.1	Симметрическая группа	31
2.7	Лекция 21	32
2.7.1	Продолжаем возиться с перестановками. Четность.	32
2.8	Лекция 22	34
2.9	Лекция 23	36
2.9.1	Теорема о гомоморфизме для колец	36
2.9.2	Комплексные числа	37
2.10	Лекция 24	38
2.10.1	Окончание комплексных чисел	38
2.11	Лекция 25	40
2.11.1	Кольца главных идеалов	41
2.11.2	Китайская теорема об остатках	42
2.12	Лекция 26	42
2.12.1	Простые и максимальные идеалы	44

2.13	Лекция 27	45
2.13.1	Фактор кольцо по максимальному идеалу	45
2.13.2	Единственность разложения	45
2.13.3	Нётеровы кольца	46
2.14	Лекция 28	47
2.14.1	Продолжение нёторвых колец	47
2.14.2	Факториальное кольцо	48
2.15	Лекция 29	49
2.15.1	Локализация кольца	49

Глава 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)

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

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

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

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

Exs.

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

Designation.

- \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

$$\begin{aligned} \cdot : R \times R &\rightarrow R \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

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)

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

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

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

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

Exs.

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

Def 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 $\forall x, y \in V, \forall a, b \in F$:

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

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

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

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

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

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

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

Exs.

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

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

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

Def 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 "+")

Def 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

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

скалярное произведение

Def 13. Транспонирование матрицы.

D - матрица $I \times J$ над X

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

Note. 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"

Designation.

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 $Z = X \cdot Y, \quad (AB)_{ik} = a_{i*} \cdot b_{*k} = \sum_{j \in J} a_{ij} \cdot b_{jk}.$

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

1.4 Лекция 4

Def 14. $(G, *)$, $(H, \#)$ – группа
 $\varphi : G \rightarrow H$ – гомоморфизм, если:

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

Def 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: $\varphi(1) = 1$

Def 16. U, V – векторные пространства над F
 $\varphi : U \rightarrow V$ – линейное отображение, если:

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

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

Note. Изоморфизм – биективный гомоморфизм.

Def 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.

Note. $U \subseteq V$

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

Lemma. $U \subseteq V$

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

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

Def 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

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

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 $v_i \forall i \in I$

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

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

□

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

Designation. 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 $f : I \rightarrow V$
 $i \mapsto f_i$

Def 20. $v \in {}^I V$
 v – **линейно независим**, если $\forall a \in F^I, a \neq 0 \Rightarrow va \neq 0$

Theorem 1. $v \subseteq V$

Следующие утверждения эквивалентны:

1. v – линейно независимая система образующих
2. v – максимальная линейно-независимая система
3. v – j 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)

$x \in V \setminus v$

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

$va = x \cdot 1 = 0$ – линейная зависимость набора $v \cup x$

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

(1) \Rightarrow (2)

$x \in V \setminus v$

$v \subseteq V \cup x$ – линейно зависим

$va + xa_x = 0$

$a \neq 0$

Если $a_x = 0 \Rightarrow va = 0 \Rightarrow a = 0$?!

Значит $a_x \neq 0$

$va = c \cdot (-a_x)$

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

□

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

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

$M \in \mathcal{C}$ – максимальная, если $M \subseteq M' \subseteq \mathcal{A} \Rightarrow M = M'$

Theorem 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. \mathcal{A} — множество всех линейно независимых подмножеств, лежащих между X и Y . $X \in \mathcal{A}$
 $\mathcal{C} \leq \mathcal{A}$

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

Пусть $\cup C \in \mathcal{C}$ — 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

Statement.

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

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

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

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

□

Corollary.

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

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

25.09.2019

1.8 Лекция 8

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

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

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

Lemma.

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

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

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

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.

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

□

Statement. 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:

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

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

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

□

Corollary. 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.

□

Statement. Если матрица двусторонне обратима, то она квадратная.

Corollary. u, v - базисы V

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

Доказательство.

$$x = ux_u = vx_v$$

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

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

□

Corollary. (Матричные линейные отображения)

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

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

При этом $(L_u^v)_{*k} = L(u_k)_v$

Note.

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

$$L : U \rightarrow V$$

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

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

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

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

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

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

Доказательство.

$$x = ux_u$$

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

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

Положим $L_u^v := L(u)_v$.

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

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

□

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

26.09.2019

1.9 Лекция 9

Exs.

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

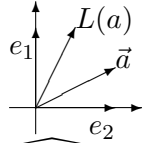
$$v = (1, t, \frac{t^2}{2}, \dots, \frac{t^n}{n!}, \dots).$$

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

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

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

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



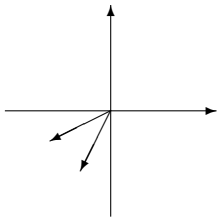
$$\widehat{a, L(a)} = \varphi$$

$e = (e_1, e_2)$ - базис

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

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

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



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

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

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

Statement. $L : U \rightarrow V$

u, u' — базис U

v, v' — базис V

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

Доказательство.

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

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

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

$$\begin{aligned} L(x)_v &= C_{v \rightarrow v'} L_{u'}^{v'} C_{u' \rightarrow u} x_k. \\ L_u^v &= C_{v \rightarrow v'} L_{u'}^{v'} C_{u' \rightarrow u}. \end{aligned}$$

□

Note.

$$\begin{aligned} \text{Если } U = V \quad u = v, u' = v'. \\ L_{u'} = C_{u' \rightarrow u} L_u C_{u \rightarrow u'}. \end{aligned}$$

Statement. Линейное отображение однозначно определяется образом базисных векторов.

$u = (u_1, \dots, u_n)$ — базис U

Для любого векторного пространства V :

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

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

Доказательство.

$$\begin{aligned} L(ua) &:= va \\ \forall L^* : L(ua) &= L(u)a = va \end{aligned}$$

□

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.

Statement. $V, \quad v, v' — \text{базис } V$

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

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

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

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

по другому

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

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

Def 21. $f : X \rightarrow Y$

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

$L : U \rightarrow V$ — линейное отображение

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

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

Lemma.

$$Im L \leq V$$

$$Ker L \leq U$$

Пусть $L(x) = y$

$$\forall y \in V : L^{-1} = x + Ker L$$

$$L^{-1}(y) = \{z \in U \mid L(z) = y\}$$

$$x + Ker L = \{x + z \mid z \in Ker L\}$$

1.10 Лекция 10

Theorem 3. $L : U \rightarrow V$

$$\dim U = \dim \text{Ker } L + \dim \text{Im } L.$$

Доказательство. $u = (u_1, \dots, u_k)$ – базис $\text{Ker } L$

$v = (v_1, \dots, v_m)$ 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. $\forall x \in \text{Im } L \quad \exists y \in U : L(y) = x. \quad y = ua + vb, \quad a \in F^k, b \in F^m$

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

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

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

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

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

Theorem 4. (формула Грассмана о размерности суммы и пересечения)

$U, V \leq W$

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

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

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

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

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

08.10.2019

1.11 Лекция 11

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

Простейший базис:

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

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

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

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

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

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

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

Def 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 , $u = \dim V$

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

$$\theta_v = L_v$$

Statement. θ_v - биективно.

Practice. Построить обратное θ_v

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

Statement. θ_v - изоморфизм

F - алгебра

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

-

Theorem 5. $U \leq V$

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

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

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

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 : $\text{Ker } \tilde{L} = 0_{V \setminus U}$ □

Theorem 6 (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. \square

Def 23. Ранг:

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

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

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

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

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

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

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

или наибольшее количество независимых столбцов (строк).

Lemma. $A \in M_{m \times n}$

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

Доказательство. (6)

$$\text{из (1)} \Rightarrow c.rkA = n$$

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

\square

10.10.2019

1.12 Лекция 12

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

$$rkL = c.L_U^V$$

Для любых базисов u, v пространств U, V .

Доказательство.

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

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

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

$$rkA = c.rkA - \text{ранг оператора умножения на } A. \text{ Из диаграммы } \text{Im } L \cong \text{Im } L_U^V \Rightarrow rkL = c.rkL_U^V$$

\square

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

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

$rkA = rkBAC$ - 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 $c.rk A = c.rk BAC = rk L$. Со столбцами все хорошо. Теперь со строками: $r.rk A^T = c.rk A$
 $r.rk(BAC)^T = r.rk(A^T B^T C^T)$ $r.rk(BAC)^T = c.rk BAC$

Тогда $r.rk A^T = r.rk C^T A^T B^T$. (Заметим, что $(B^T)^{-1} = ((B^{-1})^T)$ Следовательно, B^T, C^T - произвольные обратимые матрицы. \square

Practice. $(AB)^T = B^T A^T$

Theorem 7 (PDQ - разложение, равенство базисов). $L : U \rightarrow V$ - линейное отображений, U, V - конечн

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

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

Размер $E = rk L$.

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. $c.rk A = r.rk A$

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

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

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

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

Def 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.

Theorem 8 (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.

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

$$ua = ()$$

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 $GL_n(F) = BWB$

$a \in GL_n(F)$

□

Theorem 9 (разложение Гаусса).

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

$w \in W : wB^-B$ - клетка Гаусса.

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

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

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

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

Доказательство.

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

□

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

Доказательство. Будет в теории групп

□

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

Theorem 10 (Приведенной разложение Брюа). $B = \bigcup_{w \in W} U_w w D U$ При этом w , а также элементны из U_w, D, U определены по элементам из B из единственным образом.

Доказательство. □

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

Доказательство. $BwB = U_w w B$ □

□

Statement.

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

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 .

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

Lemma. 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. □

Lemma. $a \in U^-B \Leftrightarrow$ 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. □

Lemma. $\forall a \in GL_n(F) \exists w \in W$: 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

Theorem 11 (Кронекера-Капелли). Система линейных уравнений $Ax = b$ Имеет хотя бы одно решение тогда и только тогда, когда $rkA = rk(Ab)$, где (Ab) - расширенная матрица.

Доказательство.

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

\square

Глава 2

Начала теории групп

2.1 Лекция 15

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

$$H \leq G.$$

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

Statement. G, H - группы.

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

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

Def 27. $\varphi: X \rightarrow Y, (X, *), (Y, \cdots) -$

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.

Lemma. $G, H \leq F$

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

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

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

Def 28.

$\varphi G \rightarrow H$ - гомоморфизм.

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

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

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

Доказательство.

$a, b \in Ker \varphi.$

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

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

□

Lemma.

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

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

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

□

Def 29. $H \leq G$

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

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

Lemma. $H \leq G$

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

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

□

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

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

Lemma.

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

Доказательство.

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

Обратная $y \mapsto g_1g_2^{-1}y$

□

Theorem 12 (Лагранж). G - конечна группа. Тогда $|G| = |H| \cdot |G : H|$, где $|G : H|$ - количество левых смежных классов G по H . $|G : H|$ - индекс H в G .

Доказательство. Из прошлой леммы и следствия □

Corollary. 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 $k-l \neq 0$, $g^n = g^{m(k-l)+r} = g^r$, $r < k-l \leq p-1$. 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. $\varphi : \mathbb{Z}_p \rightarrow G, \varphi(k) = g^k$ □

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

Statement. 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 $g^n = 1$.

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

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

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

□

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

Statement (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.

Def 32. $S \subseteq G$

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

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

Def 33. $s^g := g^{-1}sg$

Note. $(s^g)^h = s^{gh}$
 $h(g_s) = {}^hgs$

Property.

1. $(s_1s_2)^g = s_1^gs_2^g$
2. $(s^g)^{-1} = (s^{-1})^g$
 $s \mapsto s^g$ - автоморфизм G .

Def 34. $H \leq G$

$H^G = \langle h^g \mid h \in H, g \in G \rangle$ – нормальное замыкание H 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 .

$H^g = \langle h^g \mid h \in H \rangle$ – подгруппа, сопряженная с H при помощи g .

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

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

Statement. $\varphi : G \rightarrow A$ - 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 .

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

Statement. $[a, b]^{-1} = [a, b]$

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

Designation.

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

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

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

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

корректность определения.

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

$$g'_2 \in g_2H \Rightarrow g'_2h_2.$$

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

□

Def 38. $\pi_H : G \rightarrow G/H, g \mapsto gH$
 π_H — эпиморфизм, $\text{Ker } \pi_H = H$

Theorem 13 (универсальное свойство факторгруппы). $N \trianglelefteq G, \varphi : G \rightarrow H$ — гомоморфизм. Если $\text{Ker } \varphi \geq N$, то существует единственный гомоморфизм $\hat{\varphi} : G/N \rightarrow H$, такой что $\varphi = \hat{\varphi} \circ \pi_N$. Если $\hat{\varphi}$ — эпиморфизм, то φ — эпиморфизм. Если $\text{Ker } \varphi = N$, то φ — мономорфизм.

Theorem 14. $\varphi : G \rightarrow F$

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

Доказательство. Заменяем N на $\text{Im } \varphi$.

$$\varphi' \rightarrow \text{Im } \varphi \quad \text{Ker } \varphi' = \text{Ker } \varphi.$$

По прошлой теореме существует единственное:

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

φ — сюръективно. Следовательно, φ' — сюръективно.

□

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

Ex. $\mathbb{Z} \rightarrow \mathbb{Z}_n, \quad \varphi(x) \equiv x \pmod{n}$.
 $\text{Ker } \varphi = n\mathbb{Z}$
 $\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$

2.4 Лекция 18

Ex.

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

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.

Lemma. $U_n^{(k)} \setminus U_n^{(k-1)} \cong \underbrace{F \times \dots \times F}_{n-k}, \quad F = (F, +)$. 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, $\varphi^{-1}(e) = U_n^{k+1}$.

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

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

Def 39. $[a, b] = aba^{-1}b^{-1}$ - коммутатор.
 $H, K \leq G, \quad [H, K] := \langle [h, k] \mid h \in H, k \in K \rangle$ - коммутант.

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

Statement. $\varphi : G \rightarrow A$ - 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 $[G, G] \subseteq \text{Ker } \varphi$. \square

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

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

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:

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

Заметим, что

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

Тогда

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

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

Lemma.

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

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 $g = y_1 \cdot \dots \cdot y_m$, $y_i \in U \cup Y^{-1}$.

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

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

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

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

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

□

Note. 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 $[x, y]$.

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

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

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

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

$h \in H, k \in K, x \in H$ (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

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

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

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

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

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

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

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

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

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

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

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

□

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

$$U_w = \langle t_{ij}(\alpha) \mid j > 1, \alpha \in F, t_{ij}(\alpha)^w \in U_n \rangle.$$

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

Доказательство.

□

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

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

□

2.6 Лекция 20

2.6.1 Симметрическая группа

Def 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:

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

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

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

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

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

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

Lemma.

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

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). □

Def 43. Отношение на группе G :

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

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

Класс эквивалентности „ \sim_c ” – класс сопряженных элементов.

Theorem 15. Класс сопряженных элементов в S_n состоит из всех перестановок фиксированного циклического типа.

Доказательство. Следует из леммы 2.6.1 □

Ex. 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.

Practice. Найти S_4/K_4 . Там 6 элементов.

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

Порядок перестановки равен НОКу порядков независимых циклов.

2.7 Лекция 21

2.7.1 Продолжаем возиться с перестановками. Четность.

Def 44 (Инверсия). $\sigma \in S_n$.

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

Ex. Четыре инверсии:

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

Def 45 (Четность перестановки).

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

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

Def 46. Транспозиция – цикл длины 2.

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

Lemma. 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

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

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

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

Theorem 16. $\varepsilon : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ - гомоморфизм группы.

Доказательство.

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

Проверим требуемые свойства:

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

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

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

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

□

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:

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

Statement. A - абелева группа.

$$a, b \in A, \quad \text{ord}(a) = m, \text{ord}(b) = n, \quad h = \text{lcm}(m, n)$$

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

Тогда $\text{ord}(ab) \mid k$.

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

Доказательство.

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

Тогда

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

□

Corollary.

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

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

Corollary.

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

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

□

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

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

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

Theorem 17. 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

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

□

2.8 Лекция 22

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

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

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

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

Note. Можно использовать одну из доказанных лемм, тогда решение будет проще.

□

Theorem 18. $p \in \mathbb{P}$
 $(\mathbb{Z}/p^k\mathbb{Z})^*$ - 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 $G = \mathbb{Z}/p^k\mathbb{Z}$

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

Рассмотрим множество чисел вида $1 + px$. Они не делятся на p . Чтобы эти числа были меньше $|G^*|$, ограничим x .

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

Statement. 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 теоремы 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

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

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

Remark.

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

Remark. 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

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

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

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

Тогда

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

□

Глава 3

Коммутативные кольца

3.1 Лекция 23

3.1.1 Теорема о гомоморфизме для колец

Note. Воспоминания R, R' – кольца с 1 (не обязательно коммутативные).

$\varphi : R \rightarrow R'$ – гомоморфизм, если

$$\begin{aligned}\varphi(r + s) &= \varphi(r) + \varphi(s) \\ \varphi(r \cdot s) &= \varphi(r) \cdot \varphi(s) \\ \varphi(1) &= 1\end{aligned}$$

$\text{Im } \varphi = \{\varphi(r) \mid r \in R\}$ – подкольцо в R' .

$\text{Ker } \varphi = \{r \mid \varphi(r) = 0\}$ – аддитивная подгруппа в R .

Def 48. I – аддитивная подгруппа в R . I называется двусторонним (правым, левым) идеалом в R тогда и только тогда, когда

$$\forall a \in R, t \in I : ar, ra \in I \quad (\text{соответственно для правого и левого } ra \in I, ar \in I).$$

Lemma. $\text{Ker } \varphi$ – двусторонний идеал.

Def 49. I – двусторонний идеал, R – кольцо. Аддитивная факторгруппа R/I является кольцом относительно операции $(r + I)(s + I) = rs + I$

Доказательство. Если $x, y \in I : (r + x)(s + y) = rs + \underbrace{xs + sy + xy}_{\in I} \in rs + I$ □

Ex. $2\mathbb{Z} \trianglelefteq \mathbb{Z}$

$$4\mathbb{Z} \stackrel{\text{как множества}}{=} (0 + 2\mathbb{Z}) \cdot (0 + 2\mathbb{Z}) \stackrel{\text{def}}{=} 0 + 2\mathbb{Z}.$$

Designation. $\pi : R \rightarrow R/I \quad \pi(r) = r + I$

Theorem 19. Универсальное свойство I – идеал в R . $\varphi : R \rightarrow R', \quad I \subseteq \text{Ker } \varphi \Rightarrow \exists! \psi : R/I \rightarrow R' :$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \downarrow \pi & \nearrow \psi & \\ R/I & & \end{array}$$

– коммутативна. $\text{Ker } \varphi = I \Rightarrow \psi$ – инъективна. φ – сюръективна $\Rightarrow \psi$ – сюръективна.

Note. Далее считаем кольца коммутативными.

Def 50. $X \subseteq R$ – кольцо. Идеал, порожденный X – наименьший идеал, содержащий X . Он равен

$$\left\{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in X, n \in \mathbb{N} \right\}.$$

Обозначается: $\sum_{x \in X} xR = \langle X \rangle_R$

$xR = (x)$ – главный идеал, порожденный x .

Ех. В \mathbb{Z} любой идеал главный.

$$I \subseteq \mathbb{Z},$$

$$0 < r < I, \quad r \leq |s| \forall s \in I.$$

Рассмотрим $x \in I$.

$$x = rs + y, \quad 0 \leq y < r.$$

$$y = x - rs \in I.$$

Так как r – наименьший, то $y = 0$.

Ех.

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2.$$

Идеал, порожденный $1 + \sqrt{-3}$ и 2 ($(1 + \sqrt{-3})R + 2R$), не является главным идеалом.

3.1.2 Комплексные числа

$$\mathbb{C} = \mathbb{R}[x] / (x^2 + 1)$$

$$i := x + (x^2 + 1)\mathbb{R}[x].$$

$$i^2 + 1 = x^2 + 1 + (x^2 + 1)\mathbb{R}[x] = 0_{\mathbb{C}} \implies i^2 = -1.$$

$\mathbb{R} \hookrightarrow \mathbb{R}[x] \rightarrow \mathbb{C}$ – инъективное отображение. отождествляем $r \in R \longleftrightarrow r + (x^2 + 1)\mathbb{R}[x]$ и считаем, что $\mathbb{R} = \mathbb{C}$.

$$p \in \mathbb{R}[x]$$

$$p = (x^2 + 1) \cdot f + (a + bx) \in a + bx + (x^2 + 1)\mathbb{R}[x].$$

$$p + (x^2 + 1)\mathbb{R}[x] = a + bi.$$

Таким образом

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

$$(a + bi)(c + di) = ac - bd + i(ad + bc).$$

$$\overline{a + bi} = a - bi$$

$$\forall w, z \in \mathbb{C} :$$

$$\begin{aligned} \overline{z \cdot w} &= \bar{z} \cdot \bar{w} \\ \overline{z + w} &= \bar{z} + \bar{w} \\ \overline{\bar{z}} &= z \end{aligned}$$

$\bar{} : \mathbb{C} \rightarrow \mathbb{C}$ – автоморфизм.

$$a = \operatorname{Re} z, \quad b = \operatorname{Im} z$$

\mathbb{C} – векторное пространство над \mathbb{R} с базисом $\{1, i\}$

3.2 Лекция 24

3.2.1 Окончание комплексных чисел

$$\mathbb{C} := \mathbb{R}[x] / (x^2 + 1).$$

$$i := x + x(2+1)\mathbb{R}[x]$$

Любое комплексное число представляется в виде $a + bi$, $a, b \in \mathbb{R}$, сопряжение: $\overline{a + bi} = a - bi$. Умножение на сопряженное: $(a + bi)(a - bi) = a^2 + b^2$. Сложение с сопряженным: $(a + bi) + (a - bi) = 2a$. Получили, что $z \cdot \bar{z}, z + \bar{z} \in \mathbb{R}$.

Statement. Существует ровно два автоморфизма на комплексных числах, оставляющие вещественные на месте.

Доказательство. $f \in \mathbb{R}[x]$.

$$f(\varphi(i)) = \varphi(f(i)), \quad \alpha \in \mathbb{C}$$

так как $\varphi(\alpha^2) = \varphi(\alpha)^2$

$\varphi(a\alpha^n) = a\varphi(\alpha)^n, a \in \mathbb{R}$. Если $f(x) = x^2 + 1$, $f(i) = 0$. $f(\varphi(i)) = \varphi(f(i))$, то есть корень переходит в корень. Значит, нетривиальный только один. А второй — тривиальный. \square

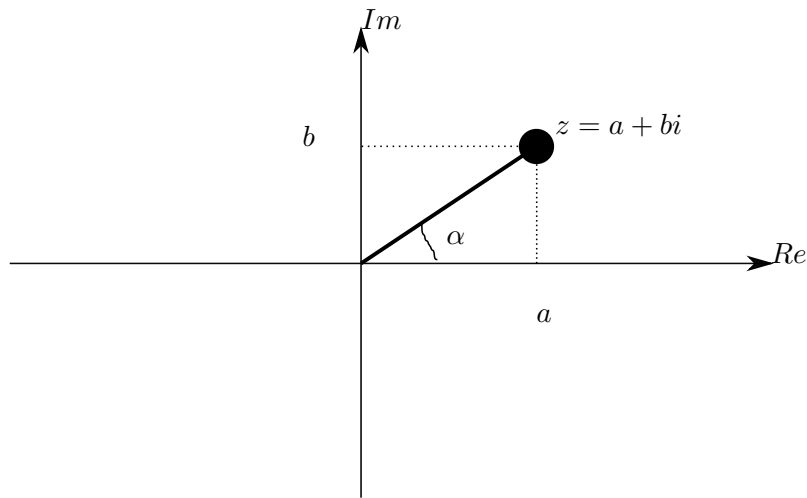


Рис. 3.1: Комплексное число на плоскости

$$|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \bar{z}}.$$

$$\text{Arg} z := \alpha \in \mathbb{R} / 2\pi\mathbb{Z}.$$

Можно выразить через аргумент:

$$a = |z| \cdot \cos \alpha$$

$$b = |z| \cdot \sin \alpha$$

$$z = |z| \cdot (\cos \alpha + i \sin \alpha) - \text{тригонометрическая формула}$$

$$\text{Arg} z = \begin{cases} \arctg \frac{b}{a} + 2\pi\mathbb{Z}, & a > 0 \\ \pi + \arctg \frac{b}{a} + 2\pi\mathbb{Z}, & a < 0 \\ \frac{\pi}{2} \cdot \text{sign}(b), & a = 0 \end{cases}.$$

Statement.

$$(\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta) = \cos(\alpha + \beta) + i \sin(\alpha + \beta).$$

Statement. $\varepsilon : \mathbb{R}/2\pi\mathbb{Z} \rightarrow \mathbb{C}^*$, $\varepsilon(\alpha) = \cos \alpha + i \sin \alpha$ – это гомоморфизм.

$$\text{Im } \varepsilon = S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

Так же:

$$\begin{aligned} \varepsilon(\alpha + \beta) &= \varepsilon(\alpha)\varepsilon(\beta) \\ \varepsilon(-\alpha) &= \varepsilon(\alpha)^{-1} \\ \varepsilon(\beta - \alpha) &= \frac{\varepsilon(\alpha)}{\varepsilon(\beta)} \\ \varepsilon(n\alpha) &= \varepsilon(\alpha)^n, \quad n \in \mathbb{Z} \\ (\cos \alpha + i \sin \alpha)^n &= \cos n\alpha + i \sin n\alpha - \text{формула Муавра} \end{aligned}$$

Несколько слов о комплекснопеременных функциях

Def 51. Дифференциал:

$$f(x + \delta x) = f(x) + df(\delta x) + o(\delta x).$$

В случае дифференцирования функции от двух переменных, x – столбец, а df – матрица 2×2 .

Note. Для комплексных коэффициентов: умножение на $\lambda + \mu i \rightarrow \begin{pmatrix} \lambda & -\mu \\ \mu & \lambda \end{pmatrix}$

Statement. Напишем степенные ряды для тригонометрических функций:

$$\begin{aligned} e^t &= \sum_{n=0}^{\infty} \frac{t^n}{n!} \\ \cos t &= \sum_{n=1}^{\infty} \frac{t^{2k}}{(2k)!} \cdot (-1)^k = \sum_{k=0}^{\infty} \frac{\alpha^{2k}}{(2k)!} \\ \sin t &= \sum_{n=1}^{\infty} \frac{t^{2k+1}}{(2k+1)!} \cdot (-1)^k = i \sum_{k=0}^{\infty} \frac{\alpha^{2k+1}}{(2k+1)!} \\ e^{i\alpha} &= \sum_{n=2k} \frac{(i\alpha)^{2k}}{(2k)!} + \sum_{n=2k+1} \frac{(i\alpha)^{2k+1}}{(2k+1)!} \\ e^{i\alpha} &:= \cos \alpha + i \sin \alpha. \\ \varepsilon(\alpha) &= e^{i\alpha} \end{aligned}$$

Note (Показательная форма комплексного числа).

$$z = |z| \cdot e^{i \cdot \text{Arg} z}$$

$$e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1.$$

2π – период для экспоненты.

$$e^{\alpha+2\pi i} = e^{\alpha}.$$

$$a, b \in \mathbb{R} : e^{a+bi} = e^a e^{bi} = e^{a(\cos b + i \sin b)}.$$

На языке теории групп:

$$r \in \mathbb{R}_{>0}^*, \alpha \in \mathbb{R}/2\pi\mathbb{Z} : (r, \alpha) \mapsto r \cdot e^{i\alpha}.$$

То есть $\mathbb{R}_{>0}^* \times \mathbb{R}/2\pi\mathbb{Z} \rightarrow \mathbb{C}^*$ – изоморфизм.

$$\mathbb{C}^* \cong \underbrace{\mathbb{R}_{>0}^* \times \mathbb{R}/2\pi\mathbb{Z}}_{\ln} \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{C}/2\pi\mathbb{Z}.$$

$$\text{Ln} : \mathbb{C}^* \rightarrow \mathbb{C}/2\pi\mathbb{Z}.$$

$$\text{Ln} : (r, e^{i\alpha+2\pi\mathbb{Z}}) = \ln r + i(\alpha + 2\pi\mathbb{Z}) = \ln r + i\alpha + 2\pi\mathbb{Z}.$$

Statement (вычисление корня n -й степени). *Вычисление корня в аддитивной группе $\mathbb{C}/2\pi\mathbb{Z}$ – решение уравнения:*

$$\begin{aligned} xn &\equiv 0 \pmod{2\pi i\mathbb{Z}} \\ xn &= 2\pi in, k \in \mathbb{Z} \\ x &\equiv \frac{2\pi ik}{n} \pmod{2\pi i\mathbb{Z}}, k \in \mathbb{Z}/n\mathbb{Z} \end{aligned}.$$

$z^n = 1, \quad z = Lnz$, далее

$$\begin{aligned} nx &= 0 \mid 2\pi i\mathbb{Z}. \\ z &= e^x = e^{\frac{2\pi ik}{n}}. \end{aligned}$$

3.3 Лекция 25

$$\begin{aligned} z^n &\iff z = e^{\frac{2\pi ik}{n}}, k \in \mathbb{Z}/n\mathbb{Z}. \\ \Theta_n(Z) &= z^k - \text{гомоморфизм } \mathbb{C} \rightarrow \mathbb{C}^*. \\ \mu_n &= \text{Ker } \Theta_n = \{e^{\frac{2\pi ik}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z}\}. \end{aligned}$$

Эти числа делят окружность на n равных частей.

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\rightarrow \mu_n \\ k + n\mathbb{Z} &\mapsto e^{\frac{2\pi ik}{n}} - \text{изоморфизм}. \end{aligned}$$

Def 52. Образующие элементы μ_n называются превообразными корнями из 1.

Corollary. $e^{\frac{2\pi ik}{n}}$ – превообразный корень тогда и только тогда, когда $\gcd(k, n) = 1$.

Statement. $z^n = w = re^{i\varphi}$. Одно из решений этого уравнения: $\left(\sqrt[n]{r} \cdot e^{\frac{i\varphi}{n}}\right)^n$.

А все решения можно записать:

$$\sqrt[n]{w} = \{\sqrt[n]{r} \cdot e^{i\frac{\varphi + 2\pi k}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z}\}, \quad z^n = w.$$

Theorem 20 (Основная теорема алгебры). $p \in \mathbb{C}[x], \deg p \geq 1$
Тогда $\exists \alpha \in \mathbb{C} : p(\alpha) = 0$.

Theorem 21 (Лиувиль). Любая ограниченная дифференцируемая функция $\mathbb{C} \rightarrow \mathbb{C}$ – константа.

3.3.1 Кольца главных идеалов

Евклидовы кольца

Def 53. Область целостности – коммутативное кольцо с единицей без делителей нуля.

Designation. R – коммутативное кольцо с 1 без делителей нуля.

Def 54. $f : R \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ Обладает свойствами:

1. $f(0) < f(r), \quad \forall r \in R$
2. $\forall a, b \in R, b \neq 0 \exists c, r \in R : a = bc + r \wedge f(r) < f(b)$

Тогда R – евклидова кольцо с евклидовой нормой f .

Theorem 22. Любой идеал евклидова кольца главный.

Доказательство. Пусть $I \triangleleft R$.

$$a \in I \setminus \{0\} : f(a) \leq f(b) \quad \forall b \in I \setminus \{0\}.$$

$$b = ac + r, \quad f(r) < f(a).$$

$$r = \underbrace{b}_{\in I} - \underbrace{ac}_{\in I} \in I.$$

Если $r \neq 0$, то $f(a) \leq f(r) < f(a)$. Противоречие. □

Note. На практике ищется с помощью алгоритма Евклида.

Statement. $b = ac + r_1$

$$a = r_1c_1 + r_2$$

$$r_1 = r_2c_2 + r_3$$

\vdots

$$f(r_{i+1}) < f(r_i)$$

\vdots

$$f(r_n) \leq f(d) \quad \forall d \in I \quad aR + bR = r_nR$$

Statement. R – область главных идеалов. $a_i \in R$

$$\sum_{i=1}^m a_i R = dR.$$

Тогда $d := \gcd(a_i)$.

	Кольцо	Норма
Exs.	\mathbb{Z}	$ \cdot $
	$F[x]$, F – поле	\deg
	Гауссовы целые числа: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$	$ \cdot $

Ex (не евклидово число). $\mathbb{Z}[\sqrt{19}]$ – не евклидово кольцо главных идеалов.

3.3.2 Китайская теорема об остатках

Theorem 23. КТО для целых чисел $x \equiv x_1 \pmod{n_1}$

$$x \equiv x_2 \pmod{n_2}$$

\vdots

$$x \equiv x_m \pmod{n_m}$$

Существует единственное x по модулю произведения $n_1 \dots n_m$, удовлетворяющее данным сравнениям.

Theorem 24. КТО R – коммутативное кольцо с 1. I_1, \dots, I_m – идеалы в R .

$I_i + I_k = R \quad \forall j \neq k$. Тогда

$$R/I_1 \oplus \dots \oplus R/I_m \cong R/I_1 \dots I_m.$$

Remark. A, B – кольца. Декартово произведение

$$A \oplus B = A \times B.$$

с покомпонентными операциями.

$$(a_1, b_1) + \cdot (a_2, b_2) = (a_1 + \cdot a_2, b_1 + \cdot b_2).$$

Statement. Идеалы I, J взаимно простые, если $I + J = R$.

Доказательство. $I \cap J$ – идеал. $I + J = \{a + b \mid a \in I, b \in J\}$ – идеал. $I \cdot J = \left\{ \sum_{i=1}^m a_i b_i \mid m \in \mathbb{N}, a_i \in I, b_i \in J \right\}$ □

Lemma. $I \cdot J \subseteq I \cap J$ верно всегда.

Lemma. $I + J = R \implies I \cdot J = I \cap J$

Доказательство. $I \cap J = (I \cap J) \cdot R = (I \cap J)(I + J) = \underbrace{(I \cap J) \cdot I}_{\in I \cdot J} + \underbrace{(I \cap J) \cdot J}_{\in I \cdot J} \subseteq I \cdot J$ □

3.4 Лекция 26

I, J – идеалы в R

$I + J = R \Leftrightarrow I, J$ взаимно простые.

Lemma. $I + J = R$. Тогда

$$R/IJ \cong R/I \oplus R/J.$$

Доказательство.

$$\varphi : R \rightarrow R/I \oplus R/J.$$

$$r \mapsto (r + I, r + J).$$

$$\text{Ker } \varphi \ni r \Leftrightarrow \begin{cases} r + I = I \\ r + J = J \end{cases} \Leftrightarrow r \in I \cap J$$

$$\text{Ker } \varphi = I \cdot J.$$

$$\exists a \in I, b \in J : a + b = 1.$$

$$r = br_1 + ar_2 \equiv r_1 \pmod{I}.$$

$$r = br_1 + ar_2 \equiv r_2 \pmod{J}.$$

То есть $\varphi(r) = (r_1 + I, r_2 + J)$, следовательно, φ – сюръективно.

По теореме о гомоморфизме колец

$$R/IJ \cong R/I \oplus R/J.$$

□

Lemma. J, I_1, \dots, I_n – идеалы в R .

$$J + I_n = R \forall k \implies J + I_1 \cdot \dots \cdot I_n = R.$$

Доказательство. Индукция. База для $k = 1$. Очевидно. Переход:

По предположению индукции $J + \underbrace{I_1 + \dots + I_{n-1}}_I = R$. Нужно доказать, что $J + I \cdot I_n = R$.

$$\begin{aligned} R &= J + I \cdot R = J + I(J + I_n) = \\ &= J + IJ + II_n = J + II_n \end{aligned} \quad .$$

□

Theorem 25 (Китайская теорема об остатках). I_1, \dots, I_n – попарно взаимно простые идеалы, то есть $\forall j \neq k : I_j + I_k = R$. Тогда

$$\frac{R}{I_1 \cdot \dots \cdot I_n} \cong \frac{R}{I_1} \oplus \dots \oplus \frac{R}{I_n}.$$

Note. Здесь дробью обозначается фактор кольцо.

Доказательство. Индукция по n . Так как I_k взаимно просто с $I_1 \cdot \dots \cdot I_{n-1}$

$$\frac{R}{I_1 \cdot \dots \cdot I_n} \cong \frac{R}{I_1 \cdot \dots \cdot I_{n-1}} \oplus \frac{R}{I_n}.$$

Дальше по предположению индукции получаем то, что хотим. □

Statement. $x \equiv x_k \pmod{I_k}, \quad k = 1, \dots, n$ равносильно тому, что

$$x \equiv \sum_{k=1}^n x_k c_k \pmod{I_1 \cdot \dots \cdot I_n}, \quad c_k \in \prod_{j \neq k} I_j \cap (1 + I_k).$$

Note. В целых числах:

$$x \equiv x_k \pmod{m_k}, \quad k = 1, \dots, n.$$

Чтобы найти c_k , нужно решить диофантово уравнение:

$$y \cdot m_k + z \cdot \underbrace{\prod_{j \neq k} m_j}_{=c_k} = 1.$$

Statement (применение КТО). В $F[t]$:

$$p(x_k) = y_k \quad \forall k = 1, \dots, n, x_i \neq x_k \quad \forall i \neq k$$

равносильно

$$p \equiv y_k \pmod{(t - x_k)}.$$

$$p(t) \equiv \sum_{k=1}^n y_k \prod_{i \neq k} \frac{t - x_i}{x_k - x_i} \pmod{(t - x_1) \dots (t - x_n)}.$$

3.4.1 Простые и максимальные идеалы

Все кольца будут коммутативные с единицей.

Def 55. Простой идеал $P \neq R$ кольца R называется простым, если $ab \in P \Rightarrow a \in P \vee b \in P$

Note. Другими словами $R \setminus P$ замкнуто относительно умножения

Ex. В \mathbb{Z} идеал $n\mathbb{Z}$ – простой тогда и только тогда, когда n – простое.

Ex. В $F[t]$ идеал $f \cdot F[t]$ простой тогда и только тогда, когда f – неприводимый многочлен.

Ex. Однако в $\mathbb{Z}[\sqrt{-3}] = R$ идеал $2R$ – не простой, хотя 2 не приводимо.

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 \in 2R.$$

Докажем, что элементы $2, 1 \pm \sqrt{-3}$ неприводимы. Обозначим их за $\alpha = \beta\gamma$. Квадраты равны 4.

$$|\alpha|^2 = 4 = |\beta|^2 \cdot |\gamma|^2.$$

$$|a + b\sqrt{-3}|^2 = a^2 + 3b^2, \quad a, b \in \mathbb{Z}.$$

Либо $|\beta|^2 = 1$, либо $|\gamma|^2 = 1$, то есть β или γ обратимы.

Ех. $F[x, y] = R$

$$I = xR + yR.$$

– простой.

Def 56. Максимальны идеал – максимальный собственный идеал. Что равносильно тому, что это максимальный из идеалов, не содержащих единицу.

Note. Другими словами, M – максимальный идеал, если $M \neq R$ и $M \subseteq I \subset R \Rightarrow I = M$

Theorem 26. Любой собственный идеал содержится в каком-то максимальном.

Доказательство. $J \trianglelefteq R$.

\mathcal{X} – множество всех идеалов, содержащих J и не содержащих единицу.

\mathcal{Y} – линейно упорядоченное подмножество \mathcal{X} , то $\bigcup_{I \in \mathcal{Y}} I \in \mathcal{X}$

$$a, b \in \bigcup_{I \in \mathcal{Y}} I \Rightarrow \exists I_1, I_2 \in \mathcal{Y} : a \in I_1, b \in I_2 \wedge (I_1 \subseteq I_2 \vee I_2 \subseteq I_1),$$

так как \mathcal{Y} – линейно упорядочено.

$$a, b \in I_k \ (k = 1, 2) : a + b \in I_k \subseteq \bigcup_{I \in \mathcal{Y}} I.$$

$$a \in \bigcup I \Rightarrow ra \in \bigcup I, r \in R.$$

Следовательно, $\bigcup_{I \in \mathcal{Y}} I$ – идеал.

$$\bigcup_{I \in \mathcal{Y}} I \subseteq J \wedge \bigcup_{I \in \mathcal{Y}} I \not\supseteq 1.$$

По лемме Цорна \mathcal{X} содержит максимальный элемент. Пусть это M . Если $M \subset N \subset R$, $N \in \mathcal{X} \Rightarrow N = M$ □

3.5 Лекция 27

3.5.1 Фактор кольцо по максимальному идеалу

Statement. P – простой идеал в R тогда и только тогда, когда R/P – область целостности.

\mathfrak{M} – максимальный тогда и только тогда, когда R/\mathfrak{M} – поле.

Доказательство. $ab \in P \Leftrightarrow a \in P \vee b \in P$.

Пусть $\bar{\cdot} : R \rightarrow R/P$.

Тогда предыдущее утверждение равносильно

$$\bar{a}\bar{b} \Leftrightarrow \bar{a} = 0 \vee \bar{b} = 0.$$

Обозначим $L(I, \mathfrak{R})$ – множество идеалов в R , содержащих I .

$$\bar{\cdot} : R \rightarrow R/P.$$

Докажем, что

$$\bar{\cdot} : L(R/\mathfrak{M}), I \mapsto \bar{I}.$$

– Образ этого идеала в R/\mathfrak{M} При эпиморфизме идеал отображается в идеал. $\bar{a} \in \bar{I}$, где $a \in I$. $\bar{r} \in R/\mathfrak{M}$, $\bar{r}a \in \bar{I}$

Обратное: $L(0, R/\mathfrak{M}) \rightarrow L(\mathfrak{M}, R)$. Взятие полного прообраза $\bar{I} \mapsto I + \mathfrak{M} \triangleleft R$.

$L(M, R) = \{\mathfrak{M}, R\} \Leftrightarrow L(\{0\}, R/M) = \{\{0\}, R/M\} \Leftrightarrow R/M$ – поле.

$\bar{\alpha} \in R/M \wedge \alpha \neq 0 \Leftrightarrow \bar{\alpha}R/M = R/M \Leftrightarrow \bar{\alpha}$ – обратим.

□

Corollary. Любой максимальный идеал является простым.

Theorem 27. В R любой ненулевой простой идеал является максимальным.

Доказательство. Обозначим простой идеал pR и предположим, что он содержится в каком-то идеале $mR \neq R$. Тогда $p = mr \Rightarrow m \in pR \vee r \in pR$. В первом случае $mR = pR$, а втором $r = pa$, то есть $p = mar \Rightarrow 1 = ta \Rightarrow mR = R$. Противоречие. □

3.5.2 Единственность разложения

R – кольцо с 1.

Def 57. $p \in R$ – простой, если pR – простой.

Def 58. $a, b \in R$ ассоциированные тогда и только тогда, когда $aR = bR$

Lemma. R – область целостности. a, b – ассоциированные тогда и только тогда, когда $a = b\varepsilon$ для некоторого $\varepsilon \in R^*$

Доказательство. $aR = bR \Rightarrow a = b \cdot \varepsilon, b = a\delta \Rightarrow a = a\delta\varepsilon \Leftrightarrow a(1 - \delta\varepsilon) = 0 \Rightarrow \varepsilon$ обратим □

Def 59. $a \in R$ приводим, если $a = bc \wedge aR \neq bR \wedge aR \neq cR$. Иначе a называется неприводимым.

Lemma. Простой элемент неприводим. В ОГИ неприводимый является простым.

Доказательство. pR – простой идеал, следовательно,

$$ab = p \Rightarrow \begin{bmatrix} a \in pR \\ b \in pR \end{bmatrix} \Rightarrow \begin{bmatrix} aR \subset pR \\ bR \subset pR \end{bmatrix}.$$

Но $pR \subset aR \cap bR$. Тогда

$$\begin{bmatrix} aR = pR \\ bR = pR \end{bmatrix}.$$

Получаем, что p – неприводим.

Теперь в обратную сторону.

R – область главных идеалов, p – неприводим. $ab \in pR$.

$aR + bR = cR \Rightarrow p = cd \Rightarrow c, d \in R^*$

Если $d \in R^* \Rightarrow cR = pR \Rightarrow aR \subset pR$, если $c \in R^* \Rightarrow aR + pR = R$, домножим на b : $\underbrace{abR + pbR}_{\subset pR} =$

$bR \Rightarrow bR \subset pR$ □

Def 60. Для колец $\dim R$ – размерность Крулля кольца или максимальная длина цепочки строго вложенных простых идеалов.

Ex. $\dim F[x_1, \dots, x_n] = n$

3.5.3 Нётеровы кольца

Def 61. R – нётерово тогда и только тогда, когда любое линейно упорядоченное множество идеалов содержит наибольший элемент.

ACC – ascending chain condition (условие обрыва возрастающих цепей)

Def 62. Артиново кольцо – аналогично, но заменить наибольший, на наименьший.

DCC – descending chain condition (условие обрыва убывающих цепей)

Lemma. R – нётерово тогда и только тогда, когда любой идеал в R конечно порожден.

Доказательство. Пусть R – нётерово, $I \triangleleft R$. Возьмем $a_1 \in I$.

$$a_1 R = I_1 \neq I \implies \exists a_2 \in I \setminus I_1, I_2 := a_1 R + a_2 R \dots$$

Получаем цепочку, которая не может быть бесконечной, значит она где-то оборвется и мы получим, что любой идеал порожден этим набором.

В обратную сторону.

\mathcal{A} – линейно упорядоченное множество идеалов.

$$\bigcup_{I \in \mathcal{A}} I = a_1 R + \dots + a_n R.$$

(так как оно конечно порожден) $\exists I_1, \dots, I_n \in \mathcal{A}$, такие что $a_k \in I_k$. Так как \mathcal{A} – линейно упорядочено, существует наибольший из I_k , пусть I_j .

$$a_1, \dots, a_n \in I_j \implies a_1 R + \dots + a_n R = I_j.$$

I_j – наибольший из \mathcal{A}

□

Theorem 28. R – нётерово. Тогда любой элемент раскладывается в произведение неприводимых.

3.6 Лекция 28

Отступление

p – неприводим тогда и только тогда, когда pR – максимальный среди собственных главных идеалов.

R – область целостности.

$$pR \subseteq aR \implies p = ar \implies \begin{cases} a \in R^* \\ r \in R^* \end{cases}$$

Тогда либо $aR = R$ или $aR = pR$.

Если R не область целостности, из $p = ar$ следует, что

$$\begin{cases} aR = pR \\ rR = pR \end{cases}$$

Тогда $r = px \wedge p = apx$, дальше $p(ax - 1)$.

Теперь придумаем контрпример:

$$R = \mathbb{Z}[a, p, x] / (p(ax-1)).$$

Хотим доказать, что p неприводим и $\bar{p}R \subsetneq \bar{a}R \subsetneq R$. Профакторизуем: \bar{p} – образ p в R ,

$$R / (\bar{p}) \cong \mathbb{Z}[a, p, x] / (p, p(ax-1)).$$

Это изоморфно

$$\mathbb{Z}[a, p, x] / (p) \cong \mathbb{Z}[a, x].$$

Statement. $I, J \triangleleft R, \pi_I : R \rightarrow R/I$

$$R/(I+J) \cong (R/I)/\pi_I(J) \cong (R/J)/\pi_J(I).$$

Тогда $\bar{p}R$ – простой идеал, следовательно, p – неприводим. В фактор кольце $R/(\bar{p}) : \bar{p}R \rightarrow 0, \bar{a}R \rightarrow$ не 0 и не все кольцо

Ex. $\mathbb{Z}[i]/(7) \cong (\mathbb{Z}[x]/(x^2+1))/(7) \cong (\mathbb{Z}[x]/(7))/(x^2+1) \cong (\mathbb{Z}/7\mathbb{Z})[x]/(x^2+1).$
 x^2+1 неприводим в $\mathbb{Z}/7\mathbb{Z}$ Значит, $\mathbb{Z}[i]/(7) \cong \mathbb{F}_{49}.$

Statement. Рассмотрим кольцо R, A – R -алгебра. Тогда

$$\forall a_1, \dots, a_n \in A : \exists! \varphi_{a_1, \dots, a_n} : R[x_1, \dots, x_n] \rightarrow A : \varphi_{a_1, \dots, a_n}(x_i) = a_i.$$

Это гомоморфизм подстановки ("eval").

3.6.1 Продолжение нёторовых колец

Theorem 29 (Теорема Гильберта о базисе). R – нётерово (коммутативное кольцо с единицей). Тогда $R[x]$ – нётерово.

Note. $b \mid a \Leftrightarrow aR \subseteq bR$

Theorem 30. R – неторова область целостности. Любой необратимый элемент раскладывается в произведение неприводимых.

Доказательство. $a \in R \setminus R^*$

1. Докажем, что существует такое p , что $p \mid a$ для неприводимого p . Если a неприводим, все отлично, иначе он представляется в виде $a = r_1 a_1$. При этом $a_1 R \neq aR$ и тогда $aR \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots \subsetneq a_n R$. Эта цепочка точно оборвется, так как R – неторово. Причем $p = a_n$ – неприводим, иначе он не может быть последним. Значит $p \mid a$.

2. $p = p_1$ – неприводим. $a = p_1 c_1$

Если $c_1 \in R^*$, то $p_1 c_1$ – неприводим. Иначе $p_1 c_1 = p_1 p_2 c_2 = \dots = p_1 p_2 \dots p_m c_m$.

$c_m \mid c_{m-1} \dots \mid c_1$ и $c_1 R \subsetneq c_2 R \subsetneq \dots \subsetneq c_m R$

$$c_i = p_{i+1} c_{i+1}.$$

Так как p_i необратим, то $c_i R \neq c_{i+1} R$. Цепочка обрывается, так как R неторово.

□

3.6.2 Факториальное кольцо

Def 63. Кольцо называется факториальным, если любой необратимый элемент единственным образом раскладывается в произведение неприводимых с точностью до ассоциированности.

Lemma. Факториальное кольцо – область целостности.

Доказательство. Если $p_1 \dots p_m = 0$, то $p_1^2 \cdot p_2 \dots p_m = 0$ – другое разложение.

Единственность означает: $p_1 \dots p_m = q_1 \dots q_n$, где p_i, q_j – необратимые $\Rightarrow m = n \wedge \exists \sigma \in S_m : p_i$ ассоциировано с $\sigma(i)$. □

Theorem 31. В R любой элемент раскладывается в произведение неприводимых и любой неприводимый элемент является простым. Тогда R – факториально.

Note. Верно и обратное

Доказательство. Пусть $p_1 \cdot p_2 \dots \cdot p_m = q_1 \dots q_n$.

Индукция по $\max(n, m)$.

База $m = n = 1$.

Переход: $\max(n, m) > 1$

Пусть $n > 1$.

$$q_1 \cdot \dots \cdot q_n \in p_1 R \xrightarrow{p_1 R - \text{простое}} p_1 \mid q_i \text{ для некоторого } i.$$

тогда $q_i \in p_i R \implies q_i = p_i r_i$. Так как q_i неприводим, r_i – обратим, следовательно, q_i ассоциирует с p_1 .

$$q_1 \dots q_{i-1} r_1 q_{i+1} \dots q_n = p_1 \dots p_m.$$

По предположению индукции p_i ассоциировано с сомножителями левой части (и $m - 1 = n - 1$). □

Corollary. Область главных идеалов является факториальным кольцом.

Theorem 32. R – факториальное кольцо. Тогда $R[x]$ – тоже факториально.

3.7 Лекция 29

3.7.1 Локализация кольца

$s \in R \xrightarrow{\varphi} A$, $\varphi(s)^e$ – обратный.

Если $r \cdot s = 0$, то $\varphi(r) = 0$.

Def 64. $S \subseteq R$, S – мультипликативное подмножество, если:

- $1 \in S$
- $\forall s_1, \dots, s_2 \in S : s_1 s_2 \in S$

Def 65. Локализация кольца R в мультипликативном подмноестве S – кольцо $S^{-1}R$ вместе с гоморфизмом $\lambda_S : R \rightarrow S^{-1}R$, такое что:

- $\lambda_S(s)$ – обратимо в $S^{-1}R \quad \forall s \in S$
- $\forall \varphi : R \rightarrow A : \varphi(s)$ обратимо в $A \quad \forall s \in S \exists!$ гомоморфизм $\psi : S^{-1}R \rightarrow A$ такое что: $\varphi = \psi \circ \lambda_S$

$$R \xrightarrow{\lambda_S} S^{-1}R$$

Построение:

$R \times S$, введем отношение эквивалентности: $(r_1, s_1)(r_2, s_2) \Leftrightarrow \exists s \in S : sr_1 s_2 = sr_2 s_1$

Докажем, что это отношение эквивалентности.

- Рефлексивность: очевидно
- Симметричность: очевидно

- Транзитивность: $(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3) \implies \exists s, s' \in S : sr_1s_2 = sr_2s_1 \wedge s'r_2s_3 = s'r_3s_2$ Домножим на s , потом на s_3 первое равенство, второе на s_1 .

$$s_3s'sr_1r_2 = s'sr_2s_1s_3 = s_1ss'r_2s_3 = ss'r_3s_2s_1.$$

$$(s'ss_2)r_1s_3 = (s'ss_2)r_3r_1.$$

Тогда $(r_1, s_1) \sim (r_3, s_3)$.

$S^{-1}R := R \times S / \sim$ Класс пары (r, s) обозначим $\frac{r}{s}$.

$$\lambda_S : R \rightarrow S^{-1}R : \quad \lambda_S(r) = \frac{r}{1}.$$

Сложение и умножение:

- $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$

Несложно доказать, что это определение не зависит от выбора представителей классов.

- $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2}$

Известно: $\frac{r'_1}{s'_1} = \frac{r_1}{s_1} \Leftrightarrow r'_1s_1s = r_1s'_1s \quad (\exists s \in S)$. Также

$$\frac{r'_1}{s'_1} + \frac{r_2}{s_2} = \frac{r'_1s_2 + r_1s'_1}{s'_1s_2} \Leftrightarrow \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2}.$$

Тогда $(r_1s_2 + r_2 + s_1)s'_1s_2 = (r'_1s_2 + r_2s'_1)s_1s_2s$. Сокращаем, получаем, что не зависит от выбора элемента класса.

$$\lambda_S(x_1) + \lambda_S(r_1) = \frac{r_1}{1} + \frac{s_2}{1} = \frac{r_1 + s_2}{1} = \lambda_S(r_1 + r_2)$$

$$\lambda_S(s) = \frac{s}{1} \text{ обратим: } \frac{s}{1} \frac{1}{s} = \frac{s}{s} = 1$$

Таким образом, $S^{-1}R$ – кольцо.

$$\varphi : R \rightarrow A, \quad \exists \varphi(s)^{-1} \quad \forall s \in S$$

$$\psi : S^{-1}R \rightarrow A$$

$$\varphi\left(\frac{r}{s}\right) := \varphi(r)\varphi(s)^{-1} \text{ Если } \frac{r'}{s'} = \frac{r}{s}, \text{ то есть } \exists s'' \in S : s''r's = s''rs'.$$

$$\varphi(s')\varphi(s)\varphi(r) = \varphi(s'')\varphi(s')\varphi(r).$$

$$\varphi(s)\varphi(r')^{-1} = \varphi(r)\varphi(s)^{-1}.$$

$$\psi\left(\frac{r'}{s'}\right) = \psi\left(\frac{r}{s}\right).$$

Построенное $R \times S / \sim$ вместе с λ_S удовлетворяет второму из определения локализации.

Note. ψ задается единственным образом.

Lemma. λ_S – инъекция тогда и только тогда, когда в S нет делителей нуля.

Доказательство. $\frac{r_1}{1} \frac{r_2}{1} \Leftrightarrow \exists s \in S : s(r_1 - r_2) = 0 \Leftrightarrow r_1 = r_2 \Leftrightarrow$ в S нет делителей нуля □

Ex. R – область целостности. $S = R \setminus \{0\}$

Тогда $S^{-1}R$ – поле частных.

Statement. Любая область целостности вкладывается в поле.

Ex. S – множество всех неделителей нуля.

$S^{-1}R$ – полное кольцо частных.

Ex. P – простой идеал. $S = R \setminus P$ – мультипликативное подмножество. $R_P := (R \setminus P)^{-1}R$ – локализация в простом идеале.

Ex. $P = 2\mathbb{Z}, R = \mathbb{Z}$

$$\mathbb{Z}_{(2)} := R_P = \left\{ \frac{m}{n} \mid n \in \mathbb{Z}, 2 \nmid m \right\}$$

Def 66. Главная локализация – $R_S = \langle s \rangle^{-1} R$
 $\langle s \rangle := \{1, s, s^2, \dots\}, s \in R$

Еж. Кольцо многочленов над кольцом $R[x]$.
 S – множество унитарных многочленов. $S^{-1}R[x]$

$$F[x_1, \dots, x_n] = F[x_1, \dots, x_{n-1}][x_n].$$

3.8 Лекция 30

3.8.1 НОК и НОД

Def 67. R – ОГИ, $a, b \in R$.

$$aR + bR = dR.$$

$d = \gcd(a, b)$ – наибольший общий делитель.

Theorem 33. $\forall a, b \in R \exists x, y \in R : ax + by = \gcd(a, b)$

Def 68. R – ОГИ, $a, b \in R$.

$$aR \cap bR = cR.$$

$x = \text{lcm}(a, b)$ – наименьшее общее кратное.

$$\text{Practice. } \text{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)}$$

Statement. F – поле частных R . $a, b, b_i \in R$. Разложим $\frac{a}{b} = \frac{a}{b_1 b_2}$, где $\gcd(b_1, b_2)$. Тогда

$$\exists x_1, x_2 \in R : a = b_1 x_1 a + b_2 x_2 a.$$

Из чего следует, что $\frac{a}{b} = \frac{ax_1}{b_2} + \frac{ax_2}{b_1}$.

Statement.

$$b = p_1^{k_1} \cdot \dots \cdot p_m^{k_m} \quad p_i - \text{неприводимы.}$$

$p_i^{k_i}$ взаимно просто с $\prod_{j \neq i} p_j^{k_j}$.

Statement. R – ОГИ, F – поле частных.

$$\forall a \in R \exists a_i \in R : \frac{a}{b} = \sum_{i=1}^m \frac{a_i}{p_i^{k_i}}, \quad b = \prod p_i^{k_i}.$$

Def 69. R – евклидово кольцо с евклидовой нормой f .

$\frac{c}{p^k}$ называется простейшей дробью, если p – простой в R , $k \in \mathbb{N}, c \in R, f(c) < f(p)$.

Theorem 34. Любой элемент поля частных F евклидова кольца R раскладывается в сумму элемента из R и простейших дробей.

Доказательство. p – неприводим, $k \in \mathbb{N}, a \in R$. Разложим $\frac{a}{p^k}$ в сумму простейших дробей и элемента кольца R .

Индукция по k .

База $k = 1$:

$$a = pb + x \implies \frac{a}{p} = b + \frac{c}{p}.$$

Переход $k - 1 \rightarrow k$:

$$\frac{a}{p^k} = \frac{b}{p^{k-1}} + \frac{c}{p^k}.$$

По предположению индукции $\frac{b}{p^{k-1}}$ раскладывается, а $\frac{c}{p^k}$ – простейшая. □

3.8.2 Кольца многочленов

R – коммутативное кольцо с единицей.

Def 70. Многочлен от t над R – кортеж $(\alpha_0, \dots, \alpha_n)$, записанный в виде $\alpha_0 + \alpha_1 t + \dots + \alpha_n t^n$

Def 71. Сумма, произведение и степень $(+, \cdot, \deg)$ многочленов определены стандартным образом.

Def 72.

$$\alpha_0 + \dots + \alpha_n t^n.$$

α_n – старший коэффициент, α_0 – свободный член.

$R[t]$ – множество всех многочленов от переменной t в поле R .

Note. $R[t]$ – коммутативное кольцо с единицей. $R \hookrightarrow R[t] \rightarrow R, \quad \alpha_0 + \dots + \alpha_n t^n \mapsto \alpha_0$

R - алгебра.

Def 73. A -алгебра над R , если A – кольцо и R – модуль и $r(a_1 a_2) = (ra_1)a_2$.

По другому: $\varphi : R \rightarrow A$

$$\varphi(r) = r \cdot 1_A$$

Обратно: Если задана $\varphi : R \rightarrow A$ (гомоморфизм колец с единицей)

$$ra := \varphi(r) \cdot a$$

задает на A структуру R -модуля.

Note. В определении A не обязательно является коммутативным.

Def 74. A, B алгебры над R .

$$\Theta : A \rightarrow B$$

– гомоморфизм R -алгебр, если

1. $\Theta(a_1 a_2) = \Theta(a_1) \Theta(a_2)$
2. $\Theta(a_1 + a_2) = \Theta(a_1) + \Theta(a_2)$
3. $\Theta(1) = 1$ (если все с 1)
4. $\Theta(ra) = r \Theta(a)$

Def 75. A – R -алгебра, $a \in A, p \in R[t]$, $p(t) = \alpha_0 \cdot 1 + \dots + \alpha_n \cdot t^n$.

$$\varepsilon_a(p) = p(a) := \alpha_0 + \dots + \alpha_n a^n.$$

$\varepsilon_a : R[t] \rightarrow A$ – гомоморфизм подстановки.

Statement (Универсальное свойство кольца многочленов). $\forall a \in A \exists!$ гомоморфизм R -алгебры $\varepsilon : R[t] \rightarrow A : t \mapsto a$.

Доказательство. $\forall r \in R : \varepsilon(r) = \varepsilon(r \cdot 1) = r \cdot \varepsilon(1) = r \cdot 1$

$$\varepsilon(\alpha_0 + \dots + \alpha_n t^n) = \varepsilon(\alpha_0) + \dots + \alpha_n \varepsilon(t^n) = \alpha_0 \cdot 1 + \dots + \alpha_n \cdot a^n.$$

□

3.8.3 Пара слов о многочленах от нескольких переменных

$$R[t_1, \dots, t_n] := R[t_1, \dots, t_{n-1}][t_n].$$

$$R[t_1, \dots, t_n] = \left\{ \sum_{i_1, \dots, i_n=0}^m \alpha_{i_1, \dots, i_n} t_1^{i_1} \cdot \dots \cdot t_n^{i_n} \mid m \in \mathbb{N}_0, \alpha_{i_1, \dots, i_n} \in \mathbb{R} \right\}.$$

Statement. $\forall a_1, \dots, a_n \in A \exists \exists!$ гомоморфизм R -алгебры :

$$R[t_1, \dots, t_n] \rightarrow A : \forall i \ t_i \mapsto a_i.$$

3.8.4 Вернемся к многочленам от одной переменной

F – поле. $F[t]$ – евклидово с евклидовой нормой \deg .

Theorem 35 (Безу). Остаток от деления $p \in F[t]$ на $t - \alpha$ равен $p(\alpha)$.

Corollary. p делится на $t - \alpha$ тогда и только тогда, когда $p[\alpha] = 0$.

Corollary. Многочлен степени n имеет не более n корней.

Theorem 36. F – поле, $G \leq F^*$. $|G| < \infty$. Тогда G – циклическая.

Доказательство. $\exp G = k \implies \forall g \in G : g^k = 1$, то есть все элементы G корни многочлена $t^k - 1 \implies |G| \leq k$. А он имеет не больше k корней. k делит $|G| \implies \exp G = |G|$. Следовательно, G – циклическая. □

3.9 Лекция 31

Theorem 37 (Карнайкера). Если $8 \nmid 8$,

$$\exp(\mathbb{Z}/n\mathbb{Z})^* = \text{lcm}_i (p_i^{k_i} - p_i^{k_i-1},$$

если $8 \mid n$,

$$\text{lcm}_{i, p_i \neq 2} (2^{k-2}, p_i^{k_i} - p_i^{k_i-1}.$$

Def 76. $n : \forall a \in (\mathbb{Z}/n\mathbb{Z})^*$ Псевдопростое число Ферма — такое число a , что $a^{n+1} \equiv 1 \pmod n$.

Practice. Для любых $p, q \in \mathbb{P}$

1. $p \cdot q$ не псевдопростое
2. p^k тоже не псевдопростое
3. Найти самое маленькое псевдопростое число
4. Может ли $p^k q^l$ быть псевдопростым?

3.9.1 Кратность корня и формальная производная

Def 77. α — корень $p \in F[t]$, F — поле.

$$p = (t - \alpha)p_1 = \dots = (t - \alpha)^k g, \quad g(\alpha) \neq 0.$$

k — кратность корня α в p .

Note. Если кратность корня равна нулю, это не корень.

Theorem 38. $F = \mathbb{R}, p(\alpha) = 0$. Кратность α в p' на один меньше кратности α в p .

Доказательство. Взяли $(t - \alpha)^k g)' = k((t - \alpha)^{k-1} g + (t - \alpha)^k g' = (t - \alpha)^{k-1} (kg + (t - \alpha)g')$. Второй сомножитель в точке α не равен нулю, следовательно, кратность α уменьшилась на один. \square

Def 78. A — F -алгебра. $\delta : A \rightarrow A$ называется дифференцированием, если она F -линейна и

$$\partial(u \cdot v) = \partial u \cdot v = \partial v \cdot u \quad u, v \in A.$$

Def 79. F — коммутативное кольцо с единицей. Определим формальную производную на $F[t]$:

$$\begin{aligned} (\alpha)' &= 0 \quad \forall \alpha \in F \\ (t^n)' &= nt^{n-1} \\ \left(\sum_{k=1}^n \alpha_k t^k\right)' &= \sum_{k=1}^n \alpha_k \cdot kt^{k-1} \end{aligned}.$$

Property.

1. $(\alpha v)' = \alpha v'$

$$2. (uv)' = u'v + v'u$$

$$3. (f(g(t)))' = f'(g(t)) \cdot g'(t)$$

Пусть $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, R – кольцо. $P(R)$ – некоторое утверждение про кольцо R . Предположим, что P наследуется подкольцами и факторкольцами, то есть

$$\forall \tilde{R} \subseteq R, I \triangleleft R: P(R) \implies \begin{bmatrix} P(\tilde{R}) \\ P(R/I) \end{bmatrix}.$$

P формулируется:

$$\forall \alpha_1, \dots, \alpha_n \in \mathbb{R} \quad (3.1)$$

Тогда $P(\mathbb{R}) \implies P(R) \quad \forall$ кольца R .

Lemma.

$$\forall n: \mathbb{Z}[t_1, \dots, t_n] \hookrightarrow \mathbb{R}.$$

Theorem 39. ?? равносильно тому, что $P(R)$ следует из любого конечнопорожденного подкольца $\tilde{R}: P(\tilde{R})$

Доказательство. $P(\mathbb{R}) \implies (P(\mathbb{Z}[t_1, \dots, t_n])) \implies P(\text{ для любого конечнопорожденного кольца } \tilde{R} \text{ порождено элементами } \alpha_1, \dots, \alpha_k)$ □

Theorem 40. Если $k \neq 0$ в F , то при дифференцировании кратность падает на один.

Note. В общем случае: α – корень g кратности $k \geq 1 \implies \alpha$ – корень g кратности $k - 1$.

Ex. в $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$:

$$t^p - 1 = (t - 1)^p.$$

1 – корень кратности p .

$$(t^p - 1)' = 0 - \text{ кратность } \infty.$$