Билеты по алгебре
I семестр

Тамарин Вячеслав

15 января 2020 г.

Оглавление

Вопрос 1 Векторное пространство

Def 1. Пусть $(V,+)$ — абелева группа, F — поле, и задана операция (умножение) $V \times F \to V$. Предположим, что $\forall u, v \in V$ и $\alpha, \beta \in F$ выполнены следующие свойства:

1. $v(\alpha\beta) - (v\alpha)\beta$
2. $v(\alpha + \beta) = v\alpha + v\beta$
3. $(v + u)\alpha = v\alpha + v\beta$
4. $v \cdot 1 = v$

Тогда V называется **векторным пространством** над полем F.

Property.

1. $v \cdot 0 = 0 \cdot \alpha = 0$
2. $v \cdot (-1) = -v$
3. $v \cdot (-\alpha) = (-v)\alpha = -(v\alpha)$
4. $v \cdot \sum \alpha_i = \sum v\alpha_i$
5. $\sum v_i \cdot \alpha = \sum v_i\alpha$

Exs.

1. Множество векторов в $\mathbb{R}^3$
2. $$F^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \middle| a_i \in F \right\}.$$
$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \alpha = \begin{pmatrix} a_1\alpha \\ \vdots \\ a_n\alpha \end{pmatrix}, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}.$$
3. X — множество, $F^X = \{f \mid f : X \to F\}$
   $f, g : X \to F$
   $(f + g)(x) = f(x) + g(x)$
   $(f\alpha)(x) = f(x)\alpha$
4. $F[t]$ — многочлены от одной переменной t

Вопрос 2 Подпространство, линейная оболочка

Def 2. Подмножество $U \subseteq V$ называется **подпространством**, если оно само является векторным пространством относительно тех же операций, которые заданы в V.

Statement 1 (критерий подпространства)**.** *Подмножество* $U \subseteq V$ *является подпространством тогда и только тогда, когда* $\forall u, v \in U,\ \alpha \in F : u + v, u\alpha \in U$.

Def 3. Пусть $u_1, \ldots, u_n \in V$, $\alpha_1, \ldots, \alpha_n \in F$. Сумма

$$\sum_{k=1}^{n} u_k \alpha_k$$

называется **линейной комбинацией** векторов $u_1, \ldots, u_n$ с коэффициентами $\alpha_1, \ldots, \alpha_n$.

Линейная комбинация называется **тривиальной**, если все ее коэффициенты равны нулю.

Note. Пусть $S \subseteq V$, и задан набор чисел $\alpha_s \in F,\ s \in S$. Операция бесконечной суммы будет определена только в случае, когда почти все α_s равны нулю.

Def 4. **Линейной оболочкой** набора S называется подпространство, порожденное S, то есть наименьшее подпространство, содержащее S.

Designation. Линейная оболочка набора S обозначается $\langle S \rangle$.

Statement 2. $\langle S \rangle = \left\{ \sum\limits_{k=1}^{n} u_k \alpha_k \middle| u_k \in S,\ \alpha_k \in F \right\}$

Def 5. Если $\langle S \rangle = V$, то S называется **системой образующих** пространства V.

Def 6. Кортеж векторов $(u_1, \ldots u_n)$ называется **линейно независимым**, если любая нетривиальная линейная комбинация этих векторов не равна нулю.

Множество $S \subseteq V$ называется **линейно независимым**, если любой кортеж , составленный из конечного числа различных векторов из S, является линейно независимым.

Def 7. **Базис** — линейно независимая система образующих.

Вопрос 3 Матрицы

i Конечные матрицы

Def 8. Двумерный массив $m \times n$ элементов поля F называется **матрицей** размера $m \times n$ над F.

Designation. Множество таких матриц обозначается $M_{m\times n}(F)$. Если $m = n$, пишут $M_n(f)$. Элемент матрицы A в позиции (i, j) записывается a_{ij}.

Property.

- *Для двух матриц одинакового размера определена операция поэлементной суммы:* $(A + B)_{ij} = a_{ij} + b_{ij}$.

- *Также определено умножение матрицы на число:* $(A\alpha)_{ij} = a_{ij}\alpha$.
- *Произведением матрицы* $A \in M_{m\times n}(F)$ *на матрицу* $B \in M_{n\times k}$ *называется матрица* $C = AB \in M_{m\times k}(F)$ *элементы которой вычисляются по формуле*

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}.$$

Theorem 1. *Множество* $M_{m\times n}(F)$ *с операциями сложения и умножения на число является векторным пространством над полем* F.

Доказательство. Произведение матриц ассоциативно, дистрибутивно и перестановочно с умножением на число:

$$\begin{cases} (AB)C = A(BC) \\ A(B+C) = AB + BC \\ (B+C)A = BA + CA \\ (AB)\alpha = A(B\alpha) = (A\alpha)B \end{cases}.$$

Все кроме первого свойства очевидны. Проверим ассоциативность:

$$\begin{aligned} ((AB)C)_{il} &= \sum_{k\in K} (AB)_{ik} c_{kl} = \sum_{k\in K} \left(\sum_{j\in J} a_{ij} b_{jk} \right) c_{kl} = \\ &= \sum_{k\in K} \left(\sum_{j\in J} a_{ij} b_{jk} c_{kl} \right) = \\ &= \sum_{j\in J} \left(\sum_{k\in K} a_{ij} b_{jk} c_{kl} \right) = \\ &= \sum_{j\in J} a_{ij} \left(\sum_{k\in K} b_{jk} c_{kl} \right) = \sum_{j\in J} a_{ij} (BC)_{jl} = (A(BC))_{il} \end{aligned}.$$

Def 9. Квадратная матрица E с 1 на главной диагонали и остальными нулями называется единичной.

Property. *Умножение данной матрицы на единичную справа и слева не ее не изменяет.*

Матрица E_n является нейтральным элементом в $M_n(F)$. ☐

Обобщение конечных матриц

Пусть даны множества X_{ij}, Y_{jh}, коммутативные моноиды $(Z_{ih}, +)$, где $i = 1, \dots m,\ j = 1, \dots n,\ h = 1, \dots k$, и функции «умножения» $X_{ij} \times Y_{jh} \to Z_{ih},\ (x, y) \mapsto xy$. Обозначим через X, Y, Z наборы множеств X_{ij}, Y_{jh}, Z_{ih}, соответственно, через $M(X)$ — множество матриц A с элементами $a_{ij} \in X_{ij}$, и аналогично $M(Y), M(Z)$. Тогда можно определить произведение матриц $A \in M(X)$ и $B \in M(Y)$ как матрицу $C = AB \in M(Z)$, где $c_{ih} = \sum\limits_{j=1}^{n} a_{ij} b_{jh}$.

Если все X_{ij}, Y_{jh} будут коммутативными моноидами, а функция умножения дистрибутивной, умножение матриц тоже будет дистрибутивным и ассоциативным.

ii Произвольные матрицы

Пусть I, J — произвольные множества (возможно бесконечные), элементами которых мы будем индексировать строки и столбцы матриц. Пусть $\forall i \in I \wedge j \in J$ задано множество X_{ij}, и обозначим набор всех таких множеств через X. Тогда матрицей размера $I \times J$ над X называется функция $A : I \times J \to \bigcup X_{ij}$ $(i, j) \mapsto a_{ij}$, такая что $a_{ij} \in X_{ij}$.

Designation. Множество матриц размера $I \times J$ над X обозначается $M_{I \times J}(X)$. Если $I = \{1\}$, то матрица размера $I \times J$ будут назваться столбцами длины J, а если $J = \{1\}$, то столбцами высоты I. Множества строк обозначим данной длины ${}^{J}X$, множество столбцов — X^J.

Будем считать, что все X_{ij} — абелевы группы в аддитивной записи. Тогда сумма двух матриц одного размера определяется поэлементно: $(A + B)_{ij} = a_{ij} + b_{ij}$. Если все X_{ij} — векторные пространства над полем F, также можно определить умножение на число: $(A\alpha)_{ij} = a_{ij}\alpha$.

Умножение матриц

Пусть все операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$ дистрибутивны (для $a \cdot 0 = 0$), и в каждом столбце матрицы Y почти все элементы равны 0.

Designation. Обозначим $M^{c.f.}_{J \times H}(Y) \subset M_{J \times H}(Y)$, состоящее из всех матриц B, у которых для любого фиксированного $h \in H$ почти все элементы b_{jh} равны 0.

Def 10. Пусть $\forall i \in I, j \in J, h \in H$ заданы операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$, причем $\forall x, x' \in X_{ij}$ и $\forall y, y' \in Y_{jh}$ выполнены равенства

$$(x + x')y = xy + x'y \wedge x(y + y') = xy + xy'.$$

Произведение матриц $A \in M_{i \times J}(X)$ и $B \in <^{c.f.}_{J \times H} (Y)$ как матрицу $AB \in M_{I \times H}(Z)$ с элементами

$$(AB)_{ih} = \sum_{j \in J} a_{ij} b_{jh}.$$

При этом суммы определены, так как почти все слагаемые равны нулю.

Note. Аналогично определяется умножение матриц $A \in M^{r.f.}_{I \times J}(X)$ и $B \in M_{J \times H}(Y)$.

Lemma 1. *Обычные свойства умножения матриц 1 выполнены, если определены все входящие в формулы операции.*

Если $\forall i, j, h \in I$ заданы дистрибутивные операции умножения $X_{ij} \times X_{jh} \to X_{ih}$, то множество $M^{c.f.}_{I \times I}(X)$ является кольцом с единицей.

Designation. Если X_{ij} одно и то же поле F для всех i, j, будем писать $M_{i \times J}(F)$ вместо $M_{I \times J}(X)$. Если $I = J$, то будем писать $M_I(F)$ вместо $M_{I \times I}(F)$. Если $I = \{1, \dots m\}, J = \{1, \dots n\}$, то можем писать $M_{m \times n}(F)$.

Другие характеристики матриц

Def 11. Множество обратимых элементов кольца $M_n(F)$ называется полной линейной группой степени n над F и обозначается $\mathrm{GL}_n(F)$.

Designation. Для множества $M^{c.f.}_{I \times \{1\}}(F)$ введем специальное обозначение F^I_{fin} и будем называть его множеством финитных столбцов высоты I над F. Другим словами, F^I_{fin} — множество финитных (у которых почти все значения равны 0) функций из I в F. Аналогично, ${}^{J}F_{fin} = M^{r.f.}_{\{1\} \times J}(F)$.

Def 12. Пусть $A \in M_{I\times J}(F)$. Матрица $A^T \in M_{J\times I}(F)$ с элементами $(A^T)_{ij} = a_{ji}$ называется транспонированной к A.

Statement 3. $(AB)^T = B^T A^T$

Note. Для обозначения столбца часто используется строка $(a_1, \dots a_n)^T$.

Вопрос 4 Эквивалентные определения базиса

Theorem 2 (Эквивалентные определения базиса)**.** *Следующие условия на подмножество v векторного пространства V эквивалентны:*

(1) *v — линейно независимая система образующих*
(2) *v — максимальная линейно независимая система*
(3) *v — минимальная система образующих*
(4) *любой элемент $x \in V$ представляется в виде линейной комбинации набора v, причем единственным образом*

Доказательство.

$\boxed{1 \Longrightarrow 2}$ Пусть v — не максимальная линейно независимая система. Мы знаем, что v — система образующих. Тогда любой элемент $a \in V$ представляется в виде линейной комбинации v, а значит любой набор, содержащий v, принадлежит линейной оболочке $\langle v\rangle$, следовательно, набор линейно зависимый.

$\boxed{2 \Longrightarrow 1}$ Так как v максимальная линейно независимая система, любой элемент $a \in V$ выражается через элементы v. Следовательно, v — система образующих.

$\boxed{1 \Longrightarrow 3}$ Пусть из v можно убрать некоторые элементы так, что полученный набор u будет минимальной системой образующих. Тогда любой элемент набора $v \setminus u$ представим в виде линейной комбинации u. Следовательно, v линейно зависим.

$\boxed{3 \Longrightarrow 1}$ Если v линейно зависим, то во всех линейных комбинациях набора v можно заменить один элемент на линейную комбинацию других. А тогда v не минимален.

$\boxed{1 \Longrightarrow 4}$ Так как v — система образующих $\langle v\rangle = V$. Теперь докажем, что представление единственно. Пусть $x = va = \sum_{y\in v} ya_y, \quad a \in F^v_{fin}$. Предположим, что $\exists b \in F^v_{fin} : x = vb$. Тогда $0 = va - vb \Longrightarrow 0 = v(a-b)$. Так как v линейно независим, можем сократить: $0 = a-b$, значит представление единственно.

$\boxed{4 \Longrightarrow 1}$ Так как любой элемент представим в виде линейной комбинации набора v, $\langle v\rangle = V$. Так как представление единственно, v линейно независим.

□

Вопрос 5 Существование базиса

Theorem 3 (О существовании базиса)**.** *Пусть $X, Y \subseteq V$, причем набор X линейно независим, а Y — система образующих. Тогда существует базис Z, содержащий X и содержащийся в Y.*

Доказательство. Пусть $\mathscr{A}$ — набор всех линейно независимых подмножеств Y, содержащих X. Этот набор не пуст, так как содержит X. Пусть $\mathscr{L}$ — линейно упорядоченный поднабор в $\mathscr{A}$. Обозначим через S объединение всех множеств из $\mathscr{L}$. Так как $\forall C \in \mathscr{L}$ лежит между X и Y, S обладает этим свойством. Рассмотрим конечное подмножество $\{v_1, \dots v_n\} \subseteq S$. По определению объединения множеств $\forall i = 1, \dots n \ \exists B_i \in \mathscr{L}$, содержащее v_i. Так как $\mathscr{L}$ — лум, среди множеств $B_1, \dots B_n$ найдется наибольшее B_k. Тогда $v_1, \dots v_n \in B_k$. Так как B_k линейно независимо, то и $\{v_1, \dots v_n\}$ линейно независимо. Следовательно, S линейно независимо, значит $S \in \mathscr{A}$. По лемме Цорна получаем, что $\mathscr{A}$ содержит максимальных элемент. Пусть это Z — максимальное из линейно независимых подмножеств Y, содержащих X.

Пусть $y \in Y \setminus Z$. Так как Z линейно независимо, $Z \cup \{y\}$ линейно зависимо, то есть $\exists a \in F^Z_{fin}$, $a_y \in F$: $ya_y + Za = 0$, где $a_y \neq 0$. Следовательно, $y \in \langle Z \rangle$. Тогда $Y \subseteq \langle Z \rangle$. С другой стороны, $V = \langle Y \rangle$ — наименьшее подпространство, содержащее Y. Значит $V \subseteq \langle V \rangle$, то есть Z — система образующих, следовательно, и базис. □

Вопрос 6 Лемма о замене

Theorem 4 (лемма о замене)**.** *Пусть $u = \{u_1, \dots u_n\}$ — линейно независимый набор из n векторов, v — система образующих пространства V. Тогда:*

1. *$\exists v_1, \dots v_n \in v : v \setminus \{v_1, \dots v_n\} \cup u = w$ — система образующих.*
2. *Причем, если u — базис, то w — базис.*

Доказательство. Индукция по n.

База: $n = 0$. Утверждение для нуля верно.

Переход: $n - 1 \to n$. По предположению индукции $\exists v_1, \dots v_{n_i} \in v$ такие, что $w' = v \setminus \{v_1, \dots v_{n-1}\} \cup \{u_1, \dots u_{n-1}\}$ является системой образующих. Причем, если v был линейно независимым, то w' — базис.

u_n выражается через линейную комбинацию набора w':

$$u_n = \sum_{i=1}^{n-1} u_i \alpha_i + \sum_{j=1}^{m} w_j \beta_j, \qquad \alpha_i, \beta_j \in F, w_j \in v \setminus \{v_1, \dots v_{n-1}\}.$$

Заметим, что кто-то из $\beta_j \neq 0$ (иначе u линейно зависим). Не умаляя общности, считаем, что $\beta_m \neq 0$. Пусть $v_n = w_m$. Тогда v_n выражается через линейную комбинацию набора $w = w' \setminus \{v_n\} \cup \{u_n\}$. Следовательно, $w' \subseteq \langle w \rangle$, значит w — система образующих.

Пусть набор v (а тогда и w') линейно независим. Рассмотрим $w'' = w' \setminus \{v_n\}$ и линейную комбинацию $w''a + u_n\alpha$ набора w, где $a \in F^{w''}_{fin}$.

$$0 = w''a + u_n\alpha = w''a + \sum_{i=1}^{n-1} u_i \alpha_i \alpha + \sum_{j=1}^{m} w_i \beta_j \alpha = w''b + v_n \beta_m \alpha, \qquad b \in F^{w''}_{fin}.$$

Если $\alpha \neq 0$, то $w''b + v_n\beta_m\alpha$ является нетривиальной линейной комбинацией набора $w'' \cup \{v_n\} = w''$, равной нулю. Значит, $\alpha = 0$, тогда $w''a = 0$. Так как $w'' \subseteq w'$, w'' линейно независим, следовательно, $a = 0$.

Получаем, что w линейно независим.

□

Вопрос 7 Количество элементов в базисе

Theorem 5 (количество элементов в базисе)**.** *Любые два базиса пространства V равномощны.*

Доказательство. Пусть $v, u = \{u_1, \dots u_n\}$ — базисы пространства V. Не умаляя общности, считаем, что мощность множества $v > n$. Перенумеруем элементы базиса u так, что $u_1, \dots u_k \notin v$ и $u_{k+1}, \dots v_n \in v$.

Тогда по лемме о замене 4 существует подмножество $\{v_1, \dots v_k\} \subseteq v : w = v \setminus \{v_1, \dots v_k\} \cup \{u_1, \dots u_k\}$ — базис. $u \subseteq w$ и $|v| = |w|$. Так как базис — максимальная линейно независимая система, то один базис не может строго содержаться в другом. Следовательно, $w = u$, откуда $|v| = n$. ☐

Def 13. **Размерность пространства** — мощность любого базиса этого пространства.

Пространство называется **конечномерным**, если в нем существует конечный базис.

Вопрос 8 Линейные отображения и их матрицы. Матрица композиции линейных отображений

i Линейные отображения

Def 14. Пусть V и U — векторные пространства, L — функция $V \to U$. L называется **линейным отображением**, если $\forall x, y \in V,\ \alpha \in F$:

$$L(x + y) = L(x) + L(y)$$
$$L(x\alpha) = L(x)\alpha$$

Биективное линейное отображение называется **изоморфизмом**. Линейное отображение из пространства в само себя называется **линейным оператором**. Отображение из пространства в основное поле часто называется **функционалом**.

Property. *Пусть вектор $v = (v_1, \dots v_n)$ и отображение $L : V \to U$.*

$$L(v) = (L(v_1), \dots L(v_n)) \in^n U.$$

Тогда

$$L(va) = L(v)a, \text{ где } a \in F^n.$$

<u>Note</u>. В случае бесконечного v можем переписать аналогично, обозначив $L(v) \in^n U : L(v)_x = L(x) \quad \forall x \in v$:

$$L(va) = L(v)a, \text{ где } a \in F^v.$$

Designation. Пусть v — базис V. Тогда $\forall x \in V\ \exists! a \in F^v_{fin} : x = va$. Тогда $a = x_v$ — столбец координат x в базисе v.

Lemma 2. *Пусть V — векторное пространство над полем F, а v — базис V. Отображение $\varphi_v : V \to F^v$, заданное равенством $\varphi_v(x) = x_v$, является изоморфизмом векторных пространств.*

Доказательство. Рассмотрим $x, y \in V$.

$$\begin{cases} vx_v = x \\ vy_v = y \end{cases} \implies v(x_v + y_v) = x + y = v(x + y)_v \implies \varphi_v(x + y) = \varphi_v(x) + \varphi_v(y).$$

$$v(x\alpha)_v = x\alpha = v(x_v\alpha) \implies \varphi_v(x\alpha) = \varphi_v(x)\alpha.$$

Построим обратное отображение: $\theta_v : F^v \to V,\ \theta_v(a) = va$. Следовательно, φ_v — биективное линейное отображение. ☐

Corollary 1 (классификация векторных пространств)**.** *Любое векторное пространство изоморфно пространству F^I для некоторого множества I, мощность которого равна размерности пространства.*

Два пространства изоморфны между собой тогда и только тогда, когда их размерности равны.

ii Матрицы линейных отображений

Statement 4. *Пусть* $L : U \to V$ *— линейное отображение,* $u = (u_1, \dots u_n)$ *— базис* U*,* $v = (v_1, \dots v_m)$ *— базис* V*.*

$$\exists! A \in M_{m\times n}(F) : \forall x \in U \ L(x)_v = Ax_u.$$

Столбцы матрицы A *вычисляются по формуле* $a_{*k} = L(u_k)_v$*.*

Доказательство. По определению столбца координат $x = ux_u$.

$$\varphi_v \circ L(x) = \varphi_v \circ L(ux_v).$$

Тогда $L_{(}x)_v = \varphi_v\big(L(x)\big) = \varphi_v\big(L(u)\big)x_u$. Пусть $A = \varphi_v\big(L(u)\big) = \big(L(u_1)_v, \dots L(u_n)_v\big)$.

Докажем единственность. Предположим, что $Ax = Bx$ для любого столбца x. Тогда $A = B$. ☐

Def 15. Матрица A из прошлого утверждения 4 называется матрицей отображения L в базисах u, v и обозначается через L_u^v.

Если $U = V$, $u = v$, говорят о матрице оператора L в базисе u и обозначают ее через L_u.

$$L(x)_v = L_u^v x_v \text{ или } L(x)_u = L_u x_u \text{ в случае } U = V \wedge u = v.$$

Theorem 6. *Матрица композиции линейных операторов является произведением матриц этих операторов.*

Если U, V, W *— конечномерные линейный пространства с базисами* u, v, w*, соответственно,* $L : U \to V$*,* $M : V \to W$ *— линейные отображения, то* $(M \circ L)_u^w = M_v^w L_u^v$*.*

Если $U = V = W$ *и* $u = v = w$*, то* $(M \circ L)_u = M_u L_u$*.*

Вопрос 9 Матрица перехода от одного базиса с другому. Замена координат и изменение матрицы оператора при замене базиса

i Матрица перехода

Theorem 7. *Пусть* v *— базис* n*-мерного пространства* V *над полем* F*. Набор* $u = (u_1, \dots u_n)$ *является базисом тогда и только тогда, когда существует* $A \in \mathrm{GL}_n(F)$ *такая, что* $u = vA$*.*

Def 16. Если u, v — базисы, то A называется матрицей перехода от v к u и обозначается через $C_{v\to u}$

При этом:

(1) *Столбец матрицы* $C_{v\to u}$ *с номером* k *равен столбцу координат вектора* u_k *в базисе* v*.* $(C_{v\to u})_k = (u_k)_v$

(2) $C_{v\to u}^{-1} = C_{u\to v}$

(3) *Если матрица двусторонне обратима, то она квадратная.*

Доказательство.

$\boxed{\Longrightarrow}$ Положим $\forall k \in [1, n] : a_{*k} = (u_k)_v$. Тогда $va_{*k} = u_k \Longrightarrow u = vA$

$\boxed{\Longrightarrow}$ Если $u = vA$, $\langle u\rangle = \langle vA\rangle = V$. При этом u минимален, так как иначе и v не минимален, значит u — базис.

1. По построению.

2. $\begin{cases} u = vC_{v\to u} \\ v = uC_{u\to v} \end{cases} \Longrightarrow uE = uC_{u\to v}C_{v\to u} \Longrightarrow E = C_{u\to v}C_{v\to u}$
3. Пусть $B \in M_{n\times m}(F)$ двусторонне обратима. $BB_1 = E_{n\times n} \wedge B_2B = E_{m\times m}$. Тогда $B_2 = B_2E_n = B_2(BB_1) = (B_2B)B_1 = E_mB_1 = B_1$. Значит $B_1 = B_2$. $B_1B = C_{u\to v}C_{v\to u} = B_1B \Longrightarrow B$ — квадратная.

□

Note. Если пространство V бесконечномерно, почти все элементы каждого столбца должны быть равны нулю.

Note. Если $V = F^n$, e — стандартный базис, то $C_{e\to u}$ — матрица, составленная из столбцов базиса u.

ii Преобразование координат при замене базиса

Theorem 8. *Пусть u, v — базисы пространства V.*

$$\forall x \in V : x_v = C_{v\to u}x_u.$$

Доказательство. Запишем определение столбца координат $x = ux_u = vx_v$. Про базисы мы знаем, что $v = uC_{u\to v}$. Тогда

$$ux_u = uC_{u\to v}x_v \Longrightarrow x_u = C_{u\to v}x_v.$$

□

iii Преобразование матрицы оператора при замене базиса

Note. Матрица перехода $C_{u\to v}$ совпадает с матрицей тождественного отображения 1_V в базисах u и v.

Lemma 3. *Пусть $u = (u_1, \dots u_n)$ — базис пространства U, $v = (v_1, \dots v_n) \in^n V$ — набор векторов пространства V. Тогда существует единственное линейное отобборажение*

$$L : U \to V : L(u) = v.$$

При этом

L инъективно тогда и только тогда, когда u линейно независим
L сюръективно тогда и только тогда, когда u — система образующих
L — изоморфизм тогда и только тогда, когда u — базис

Доказательство. $\forall x \in U : x = ux_u$. Тогда $\forall L : L(x) = L(u)x_u$. Зададим L так: $L(x) = vx_u$. Оно линейно и единственно. □

Note. Пусть u, v — базисы пространства V. Тогда матрица отображения L из леммы в базисе u совпадает с матрицей перехода $C_{u\to v}$.

Statement 5. *Пусть u, u' — базисы пространства U, v, v' — базисы пространства U, v, v' — базисы пространства V, $L : V \to U$ — линейное отображение. Тогда*

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

Доказательство.

$$\begin{aligned} &L(x)_v = L_u^vx_u \\ &C_{v'\to v}L(x)_v = L(x)_{v'} = L_{u'}^{v'}x_{u'} = L_{u'}^{v'}C_{u'\to u}x_u \\ &L(x)_v = C_{v\to v'}L_{u'}^{v'}C_{u'\to u}x_u \\ &L_u^v = C_{v\to v'}L_{u'}^{v'}C_{u'\to u} \end{aligned}$$

□

Note. Если $U = V$ и $u = v,\ u' = v'$,

$$L_{u'} = C_{u' \to u} L_u C_{u \to u'}.$$

Вопрос 10 Внешняя и внутренняя пряма сумма пространств, естественный изоморфизм между ними

Designation. U, V — подпространства векторного пространства W над полем F.

Def 17. Сумма $U + V$ — совокупность $\{x + y \mid x \in U, y \in V\}$.

Note. $U + V \subseteq W \wedge U \cap V \subseteq W$.

Def 18. Пространство W называется внутренней прямой суммой подпространств U и V, если

$$\forall z \in W\ \exists! x \in U, y \in V : z = x + y.$$

То есть $W = U + V \wedge V \cap U = \{0\}$.

Def 19. U, V — векторные пространства. Их внешней прямой суммой называется их декартово произведение с покомпонентыми операциями.

Designation. Обе прямые суммы обозначаются $U \oplus V$.

Note. Пространства U, V естественно вкладываются в из внешнюю прямую сумму: $\forall x \in U : x \mapsto (x, 0) \wedge \forall y \in V : y \mapsto (0, y)$. Если отождествить U и V с их образами, то внешняя сумма превращается в прямую сумму подпространств.

Statement 6. *$U, C \leqslant W$, $U \oplus V$ — их внешняя прямая сумма. Зададим $\varphi : U \oplus V \to W$ так $\varphi(x, y) = x + y$. φ — изоморфизм тогда и только тогда, когда W является внутренней суммой подпространств U и V.*

Если $W = U \oplus V$, то объединение базисов U и V — базис W. Поэтому $\dim(U \oplus V) = \dim(U) + \dim(V)$.

Statement 7. $\forall U \leqslant W\ \exists V \leqslant W : W = U \oplus V$.

Доказательство. Выберем базис u подпространства U и дополним его до базиса пространства W: $u \cup v$. Тогда подойдет $V = \langle v \rangle$. ☐

Theorem 9. *Для пространств $U_1, \dots U_n \leqslant V$ следующие условия эквивалентны:*

(1) $U_1 \oplus \dots U_n \to V,\ (x_1, \dots x_n) \mapsto x_1 + \dots x_n$ — *изоморфизм*
(2) $\forall x \in V\ \exists! \big(x_1 \in U_1, \dots x_n \in U_n\big) : x = x_1 + \dots x_n$
(3) $V = U_1 + \dots U_n$ *и* $U_i \cap \Big(\sum_{j \neq i} U_j\Big) = \{0\} \qquad i \in [1, n]$
(4) *Объединение базисов подпространств* $U_1, \dots U_n$ — *базис* V.

Вопрос 11 Ядро и образ линейного отображения. Слои линейного отображения

Def 20. Пусть $L : U \to V$ — линейное отображение. Тогда

Ядро отображения L — $\operatorname{Ker} L = L^{-1}(0) \coloneqq \{x \in U \mid L(x) = 0\}$
Образ отображения L — $\operatorname{Im} L = \{L(x) \mid x \in U\}$

Statement 8. *Пусть $L : U \to V$ — линейное отображение.*

$$\operatorname{Ker} L \leqslant U \wedge \operatorname{Im} L \leqslant U.$$

Def 21. $L : U \to V$ — линейное отображение. **Слой** отображения над точкой $y \in V$ — множество $\{x \in X \mid L(x) = y\} = L^{-1}(y)$

Statement 9. *Все слои отображения L являются сдвигами ядра. $L(x) = y, \ x \in U$:*

$$L^{-1}(y) = x + \operatorname{Ker} L.$$

Вопрос 12 Теорема о размерности ядра и образа. Теорема о размерности прямой суммы

Theorem 10 (о размерности ядра и образа)**.** $L : U \to V$ *— линейное отображение. Тогда*

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

Доказательство. $u = (u_1, \dots u_k)$ — базис $\operatorname{Ker} L$, $v = (v_1, \dots v_m)$. Дополним базис ядра до базиса U: $u \cup v$ — базис U. Докажем, что $L(v) = (L(v_1), L(v_2), \dots L(v_m))$ — базис образа.

$$\forall x \in \operatorname{Im} L \ \exists y \in U : L(y) = x.$$

Разложим $y = ua + vb, \qquad a \in F^k, \ b \in F^m$
Тогда

$$x = L(y) = L(u) \cdot a + L(v) \cdot b.$$

Так как $u \in \operatorname{Ker} \ : L(u) = (L(u_1), \dots L(u_k)) = (0, \dots 0)$. Следовательно, $L(v)$ — система образующих. Проверим, что $L(v)$ линейно независим. Пусть

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

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

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

Theorem 11 (формула Грассмана о размерности суммы и пересечения)**.** *Пусть $U, V \leqslant W$.*

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

Доказательство. Зададим линейное отображение $L : U \oplus V \to W : L(u, v) = u + v$. Тогда $\operatorname{Im} L = U + V$.

$$(u, v) \in \operatorname{Ker} L \iff u + v = 0 \iff u = -v \in U \cap V.$$

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

По теореме о размерности ядра и образа

$$\dim U + \dim V = \dim(U \oplus V) = \dim \operatorname{Ker} L + \dim \operatorname{Im} L = \dim U \cap V + \dim U + V.$$

☐

Вопрос 13 Факторпространство и его универсальное свойство

Designation. V — векторное пространство, $U \leqslant V$.

Def 22. $x + U$ — аффинное подпространство или смежный класс V по U.
$y \sim_U x \Longleftrightarrow y - x \in U$ — эквивалентность.

Def 23. Множество смежных классов V по U с операциями

$$\begin{aligned}(x + U) + (y + U) &= (x + y) + U \\ (x + u)\alpha &= x\alpha + U\end{aligned}$$

называется **факторпространством** V по U и обозначается V/U.

Проверка корректности определения. Докажем, что определение операций не зависит от выбора представителей классов.

- Сложение

$$x' + U = x + U \Longrightarrow x' + 0 \in x + U \Longrightarrow x' \in x + U.$$

$$y' + U = y + U \Longrightarrow y' + 0 \in y + U \Longrightarrow y' \in y + U.$$

Тогда $\exists z \in U : x' = x + z$ и $\exists t \in U : y' = y + t$.

$$\begin{aligned}(x' + U) + (y' + U) &\coloneqq (x' + y') + U = \\ &= (x + y) + \underbrace{(z + t)}_{\in U} + U \subseteq \\ &\subseteq (x + y) + U\end{aligned}$$

Аналогично доказываем включение в обратную сторону.

- Умножение

$$\begin{aligned}(x' + U)\alpha &\coloneqq x'\alpha + U = \\ &= (x + z)\alpha + U = x\alpha + \underbrace{z\alpha}_{\in U} + U \subseteq \\ &\subseteq x\alpha + U\end{aligned}$$

Аналогично доказываем включение в обратную сторону.

□

Designation. $\pi_U : V \to V/U$ — естественная проекция: $\pi_U(x) = x + U$.

Note. π_U линейно и сюрьективно $\operatorname{Ker} \pi_U = U$.

По теореме о размерности ядра и образа $\dim V/U = \dim V - \dim U$.:

Statement 10. *Пусть* $U \subseteq V$. *Для любого линейного отображения* $L : V \to W$, $U \subseteq \operatorname{Ker} L$, *существует единственное отображение* $\tilde{L} : V/U \to W : L = L \circ \pi_U$. *При этом сюрьективность* $\tilde{L}$ *равносильна сюрьективности* L, *а инъективность* $\tilde{L}$ *— тому, что* $\operatorname{Ker} L = U$. *То есть такая диаграмма коммутативна:*

$$\begin{tikzcd} V \arrow[r, "L"] \arrow[d, "\pi_U"'] & W \\ V/U \arrow[ur, "\tilde{L}"'] & \end{tikzcd}$$

Доказательство. Пусть $\tilde{L}(x+U) = L(x)$. Эта формула задает линейное отображение и равносильна $L = \tilde{\pi}_U$. Следовательно, $\tilde{L}$ существует и единственно.

π_U инъективно, следовательно, L сюрьективно $\iff \tilde{L}$ сюрьективно.

Отображение $\tilde{L}$ инъективно $\iff \operatorname{Ker}\tilde{L} = \{0_{V/U} + U\}$.

$$x + U \in \operatorname{Ker}\tilde{L} \iff \tilde{L}(x+U) = 0 \iff L(x) = 0 \iff x \in \operatorname{Ker} L.$$

□

Theorem 12 (о гомоморфизме)**.** $L : V \to W$ *— линейное отображение.*

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

Доказательство. Возьмем $U = \operatorname{Ker} L$ и заменим W на $\operatorname{Im} L$. Далее применим утверждение 10. □

Вопрос 14 Ранг набора элементов векторного пространства, ранг оператора, строчной и столбцовый ранг матрицы

Def 24.

Рангом набора векторов называется размерность линейной оболочки этого набора.

Рангом линейного оператора называется размерность образа этого оператора.

Столбцовым (строчным) рангом матрицы называется ранг набора ее столбцов (строк).

Note. Из любой системы образующих можно выбрать базис, следовательно, ранг набора векторов — наибольшее количество линейно независимых векторов из этого набора. Так как образы базисных векторов порождают образ оператора, то ранг оператора равен рангу набора базисных векторов, а он равен столбцовому рангу матрицы оператора (вне зависимости от выбора базиса).

Theorem 13. *Пусть* $A \in M_{m\times n}(F)$.

(1) *Набор столбцов матрицы A линейно независим тогда и только тогда, когда ее столбцовый ранг равен n.*

(2) *Набор столбцов матрицы A порождает F^m тогда и только тогда, когда ее столбцовый ранг равен m.*

(3) *Набор столбцов матрицы A является базисом в F^m тогда и только тогда, когда ее столбцовый ранг $m = n$. В этом случае A обратима.*

(4) *Если все строки матрицы A линейно независимы, и все столбцы линейно независимы, то $m = n$, а A обратима.*

Доказательство. Пункты (1) и (2) очевидны. Из них следует, что столбцовый ранг равен $m = n$ тогда и только тогда, когда набор столбцов — базис в F^m. В этом случае A — матрица перехода от стандартного базиса к базису из столбцов матрицы A, а значит A обратима.

Количество линейно независимых столбцов и строк не может быть больше размерности, следовательно, $n \leqslant m \wedge n \geqslant m \Longrightarrow n = m$. □

Lemma 4. *Умножение матрицы на обратимую (слева или справа) не меняет ее столбцовый и строчной ранги.*

Доказательство. Умножение матрицы оператора слева на обратимую матрицу соответствует замене базиса в его области значений, а справа — в области определения. Так как столбцовый ранг оператора не зависит от выбора базиса, то столбцовый ранг не меняется при умножении.

Строчный ранг равен столбцовому рангу транспонированной к ней, а транспонированная к обратимой — обратима. □

Вопрос 15 PDQ-разложение. Равенство строчного и столбцового рангов матрицы

Theorem 14 (PDQ-разложение)**.** *Пусть U, V — конечномерные пространства. Для любого линейного отображения $L : U \to V$ существуют базисы пространств U и V, в которых матрица отображения L имеет вид* $\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$.

Любая матрица $A \in M_{m\times n}(F)$ представляется в виде $A = PDQ$, где $P \in \mathrm{GL}_M(F)$, $Q \in \mathrm{GL}_n(F)$, а D записывается в блочном виде $D = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$. При этом размер единичной матрицы равен строчному и столбцовому рангу A.

Доказательство.

Первое утверждение Выберем базис $(f_1, \dots f_k)$ ядра оператора L и дополним его до базиса $u = (g_1, \dots g_l, f_1, \dots f_k)$ пространства U. Тогда векторы $L(g_1), \dots L(g_l)$ линейно независимы и их можно дополнить до базиса v пространства V. Получаем нужную матрицу отображения L в базисах u, v.

Второе утверждение Пусть $L : F^n \to F^m$ — оператор умножения на матрицу A. Выберем базис u пространства F^n и v — пространства F^m так, чтобы $L_v^u = D$. Тогда

$$A = A_e^e = C_{e\to u} L_v^u C_{v\to e} = PQD,$$

где e — стандартный базис пространства столбцов.

Так как ранги при умножении обратимую матрицу не меняются, столбцовый и строчной ранги равны рангу единичной матрицы.

□

Lemma 5. *Квадратная матрица обратима тогда и только тогда, когда е ранг равен ее размеру.*

Theorem 15 (Кронокера-Капелли)**.** *Система $Ax = b$ совместима тогда и только тогда, когда ранг матрицы A равен рангу расширенной матрицы (Ab).*

Вопрос 16 Разложение Брюа

Def 25. Матрица A называется верхней (нижней) треугольной, если $a_{ij} = 0 \quad \forall i > j \ (i < j)$.

Треугольная матрица с 1 на диагонали называется унитреугольной.

Designation.

$B = B_n(F)$ — множество верхних треугольных матриц.
$B^- = B_n^-(F)$ — множество нижних треугольных матриц.
$U = U_n(F)$ — множество верхних унитреугольных матриц.
$U^- = U_n^-(F)$ — множество нижних унитреугольных матриц.
$W = W_n$ — множество матриц перестановок, то есть матрицы, отличающиеся от единичной перестановкой столбцов.

Lemma 6. *Множества W, B, B^-, U, U^- являются подгруппами в $\mathrm{GL}_n(F)$.*

Theorem 16 (разложение Брюа)**.** $\mathrm{GL}_n(F) = BWB$

Доказательство. Докажем, что $\forall a \in \mathrm{GL}_n(F)\ \exists b, c \in D,\ w \in W : a = bwc.$

По индукции по n докажем, что, домножая a слева и справа на верхнетреугольные матрицы, можно получить матрицу перестановку.

Пусть i — наибольший индекс, для которого $a_{i1} \neq 0$. Запишем a в виде

$$a = \begin{pmatrix} x & * \\ a_{i1} & z \\ 0 & * \end{pmatrix}, \quad \text{где } x = \begin{pmatrix} a_{11} \\ \vdots \\ a_{i-11} \end{pmatrix}, \quad \text{а } z - (a_{i2}, \dots a_in).$$

Домножая a слева на верхнетреугольныую матрицу, получим матрицу, у которой первый столбец совпадает с i-м столбцом единичной матрицы. После этого, домножая справа на подходящую верхнереугольныю матрицу можем сделать i-ю строку равной первой строке единичной матрицы:

$$\begin{pmatrix} E & -\frac{x}{a_{i1}} & 0 \\ 0 & \frac{1}{a_{i1}} & 0 \\ 0 & 0 & E \end{pmatrix} \begin{pmatrix} x & * \\ a_{i1} & z \\ 0 & * \end{pmatrix} \begin{pmatrix} 1 & -\frac{z}{a_{i1}} \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & f \\ 1 & 0 \\ 0 & g \end{pmatrix} \qquad \text{для некоторых матриц } f, g.$$

Заметим, что так как строки полученной матрицы линейно независимы, то и строки матрицы $\begin{pmatrix} f \\ g \end{pmatrix}$ тоже линейно независимы. Поэтому последняя матрица обратима и к ней можно применить индукционное предположение. Следовательно, существуют матрицы $u, v \in B_{n-1}(F) : u \begin{pmatrix} f \\ g \end{pmatrix} v \in W_{n-1}$. Пусть

$$u = \begin{pmatrix} u^{(1)} & u^{(2)} \\ 0 & u^{(3)} \end{pmatrix}, \quad \text{где } u^{(1)} \in B_{i-1}(F),\ u^{(3)} \in B_{n-i}(F).$$

Тогда

$$\begin{pmatrix} u^{(1)} & u^{(2)} \\ 0 & u^{(3)} \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} \cdot v$$

является матрицей-перестановкой, следовательно,

$$\begin{pmatrix} u^{(1)} & 0 & u^{(2)} \\ 0 & 1 & 0 \\ 0 & 0 & u^{(3)} \end{pmatrix} \begin{pmatrix} 0 & f \\ 1 & 0 \\ 0 & g \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix}$$

— тоже матрица-перестановка.

Так как обратная к верхнетреугольной — верхнетругольная, получаем нужное утверждение.

□

Def 26. Множество BwB при фиксированном w называется клеткой Брюа.

Statement 11. *Две различные клетки Брюа не пересекаются.*

Вопрос 17 Разложение Гаусса

Def 27. **Главная подматрица** матрица A порядка k — подматрица, стоящая на пересечении первых k строк и первых k столбцов.

Lemma 7. *Умножение матрицы на нижнюю унитреугольную слева и на верхнюю унитреугольную справа не меняет обратимости главных подматриц.*

Доказательство. $a^{(k)}$ — главная подматрица $k \times k$ в a. Умножим на нижнюю унитреугольную матрицу слева:

$$\begin{pmatrix} b & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} a^{(k)} & * \\ * & * \end{pmatrix} = \begin{pmatrix} ba^{(k)} & * \\ * & * \end{pmatrix}.$$

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

Lemma 8. *Все главные подматрицы обратимы тогда и только тогда, когда матрица раскладывается в произведение обратимых унитреугольных верхнетреугольной и нижнетреугольной.*

Доказательство. Доказываем следствие влево. Индукция по n.

База: $n = 1$ — очевидно

Переход:

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

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

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 9. $\forall a \in \mathrm{GL}_n(F)\ \exists w \in W$: *все подматрицы в* wa *обратимы.*

Доказательство. Индукция по k. Докажем, что существует перестановка $a \in \mathrm{GL}_n(F)$ такая, что главные подматрицы размера не более $k \times k$ обратимы.

База: $k = 1$

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

Меняем i-ю строку с первой.

Переход: $k \to k + 1$ Все столбцы обратимой матрицы линейно независимы, следовательно, ранг матрицы, составленной из первых k столбцов, равен k Тогда существует k линейно независимых строк этой матрицы. Переставим эти строки на первые k мест.

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

У полученной матрицы $a^{(k)}$ главная подматрица порядка k обратима. По индукционному предположению все меньшие главные подматрицы в $a^{(k)}$ обратимы.

□

Theorem 17 (Разложение Гаусса)**.** $\mathrm{GL}_n(F) = WB^-B$

Доказательство. Рассмотрим $a \in \mathrm{GL}_n(F)$. Построим перестановку w, чтобы все главные подматрицы были обратимы. Дальше домножим справа и слева на унитреугольные матрицы так, чтобы получить верхнетругольную матрицу: $wa \in B^-B$. Домножая на B, B^-, получим, что хотели. ☐

Вопрос 18 Определение группы, подгруппы, прямое произведение групп

Def 28. Множество X с операцией $*$, удовлетворяющее

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),

называется группой.

Def 29. Непустое подмножество $H \subset G$ называется подгруппой G, если H — группа относительно операции, заданной в G.

Designation. Обозначается: $H \leqslant G$

Lemma 10. *$H \subset B$. H — подгруппа тогда и только тогда, когда $\forall h, g \in H : gh, g^{-1} \in H$.*

Property. *Любая группа имеет две тривиальные подгруппы: сама группа и множество, состоящее из одного нейтрального элемента.*

Def 30. Пусть G_1, G_2 — группы с операциями $*_1$ и $*_2$ соответственно. Прямое произведение $G = G_1 \times G_2$ — декартово произведение G_1 и G_2 с операцией $*$:

$$(g_1, g_2) * (g_1', g_2') = (g_1 *_1 g_1', g_2 *_2 g_2'), \quad g_1, g_1' \in G_1, \ g_2, g_2' \in G_2.$$

Аналогично определяется произведение любого семейства групп.

Вопрос 19 Подгруппа, порожденная множеством. Классификация циклических подгрупп

Def 31. Пусть X — подмножество группы G. Подгруппой, порожденной множеством X, называется наименьшая группа по включению, содержащая X.

Designation. Подгруппа, порожденная X, обозначается $\langle X \rangle$.

Def 32. Группа, порожденная одним элементом, называется циклической.

Lemma 11. $\langle X \rangle = \{x_1 \dots x_k \mid k \in \mathbb{Z}_+, \ x_i \in X \cap X^{-1}\}$.

Statement 12. *Любая циклическая группа изоморфна $\mathbb{Z}$ или $\mathbb{Z}_n$.*

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

1. $g^m \neq 1 \quad \forall m \in \mathbb{Z} \Longrightarrow \nexists a, b \in \mathbb{Z} : g^a = g^b$. Тогда отображение
$$\varphi : \mathbb{Z} \to G, \quad \varphi(m) = g^m \text{ — изоморфизм.}$$
$$\varphi(m+k) = g^{m+k} = g^m g^k = \varphi(m)\varphi(k).$$
2. Пусть n — наименьшее натуральное число, такое, что $g^n = 1$. Заметим, что любое целое l можно с остатком разделить на $n : l = ns + r,\ 0 \leqslant r < n$. Тогда
$$g^l = g^{ns} g^r = g^r.$$
Следовательно, $\langle g \rangle = \{1, g, g^2, \dots g^{n-1}\}$. Тогда отображение
$$\varphi : G \to \mathbb{Z}_n, \quad k \to g^k \text{ — изоморфизм.}$$

☐

Вопрос 20 Смежные классы по подгруппе. Теорема Лагранжа

Def 33. Пусть $H \leqslant G$. Множества gH и Hg называются левым и правым смежными классами по подгруппе H соответственно.

Designation.

$G \diagup H = \{gH \mid g \in G\}$ — множество левых смежных классов.
$H \diagdown G = \{Hg \mid g \in G\}$ — множество правых смежных классов.

Def 34. Отношение сравнимости по модулю H:
$$a \equiv b \mod H \Longleftrightarrow a \in bH.$$

Lemma 12. *Сравнимость по модулю H — отношение эквивалентности. Два смежных класса либо не пересекаются, либо совпадают.*

Доказательство.

Рефлексивность: $a = ae \in aH$
Симметричность: $a \in B \Longrightarrow \exists h \in H : a = bh \Longrightarrow b = ah^{-1} \in aH$
Транзитивность: $a \in bH, b \in cH \Longrightarrow a = bh, b = ch' \Longrightarrow a = chh' \in cH$

Второе утверждение вытекает из того, что классы сравнимости — левые смежные классы по подгруппе. ☐

Corollary 2.
$$G = \bigsqcup_{g \in X} gH, \text{ где } X \text{ — множество представителей левых смежных классов по } H$$

Lemma 13.
$$|g_1 H| = |g_2 H|, \quad \forall g_1, g_2 \in G,\ H \leqslant G.$$

Доказательство. Такое отображение будет изоморфизмом:
$$\begin{pmatrix} g_1 H \to g_2 H \\ x \mapsto g_2 g_1^{-1} x \end{pmatrix}.$$

Обратное: $y \mapsto g_1 g_2^{-1} y$ ☐

Theorem 18 (Лагранж)**.** *G — конечная 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 $\square$

Lemma 14. *Множества $G\diagup H$ и $H\diagdown G$ равномощны.*

Доказательство. Зададим биекцию $\varphi : G\diagup H \to H\diagdown G, \quad aH \mapsto (aH)^{-1} = Ha^{-1}$. $\square$

Вопрос 21 Порядок элемента группы.

Def 35. Порядок $g \in G$ — наименьшее натуральное число, такое что $g^n = 1$.
Второе определение: $\operatorname{ord}(g) = |\langle g \rangle|$.

Theorem 19. *Пусть G — группа, $g \in G$. Тогда $|G| \,\vdots\, \operatorname{ord}(g)$*

Доказательство. Применим теорему Лагранжа для подгруппы порожденной g : $|G| \,\vdots\, |\langle g \rangle|, \ \operatorname{ord}(g) = |\langle g \rangle|$ $\square$

Theorem 20. *Пусть $\varphi : G \to H$ — гомоморфизм. $g \in G, \ \operatorname{ord}(g) = n$. Тогда $\operatorname{ord}(g) \,\vdots\, \operatorname{ord}(f(g))$.*

Доказательство.

$$1_H = f(1_G) = f(g^n) = f(g)^n \Longrightarrow n \,\vdots\, \operatorname{ord}(f(g)).$$

$\square$

Statement 13. *Пусть G — абелева группа, $a, b \in G$. Тогда $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) \,\vdots\, \operatorname{ord}(ab)$.*

Доказательство. Обозначим $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = n, \ \operatorname{ord}(ab) = m$

$$(ab)^n = a^n b^n = 1 \Longrightarrow n \,\vdots\, m.$$

$\square$

Theorem 21. *Пусть G — абелева группа, $a, b \in G, \ \gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$. Тогда $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.*

Доказательство. Рассмотрим $\langle a \rangle \cap \langle b \rangle = H$. Это подгруппа $\langle a \rangle$ и $\langle b \rangle$. По теореме Лагранжа $\operatorname{ord}(a) \,\vdots\, |H|$ и $\operatorname{ord}(b) \,\vdots\, |H|$. Так как порядки a и b взаимно просты, $\langle a \rangle \cap \langle b \rangle = \{e\}$. Тогда

$$a^s = b^t \Longleftrightarrow a^s = b^t = e.$$

Это равносильно тому, что

$$s \,\vdots\, \operatorname{ord}(a), \ t \,\vdots\, \operatorname{ord}(b).$$

Если $(ab)^n = e$, то $a^n = b^{-n}$, значит $n \,\vdots\, \operatorname{ord}(a) \wedge n \,\vdots\, \operatorname{ord}(b)$. Порядки взаимно просты, следовательно $n \,\vdots\, \operatorname{ord}(a)\operatorname{ord}(b)$. С другой стороны, по прошлому утверждению $\operatorname{ord}(a)\operatorname{ord}(b) \,\vdots\, \operatorname{ord}(ab)$. Следовательно,

$$\operatorname{ord}(a)\operatorname{ord}(b) = \operatorname{ord}(ab).$$

$\square$

Вопрос 22 Экспонента группы, критерий цикличности группы

Def 36. Экспонентой или показателем группы G называется натуральное число $d : g^d = e \quad \forall g \in G$. Если такого g не существует, то говорят, что экспонента группы равна бесконечности.

Theorem 22 (свойства экспоненты группы)**.**

(1) *Экспонента группы равна НОКу всех порядков ее элементов.*
(2) *Если группа конечна, то ее экспонента делит ее порядок.*
(3) *Экспонента прямого произведения групп $G_1 \times \ldots G_l$ равна НОКу экспонент этих групп.*
(4) *Если G — абелева группа конечной экспоненты, то существует элемент, порядок которого равен ее экспоненте.*
(5) *Конечная абелева группа является циклической тогда и только тогда, когда ее экспонента равна ее порядку.*

Доказательство. Докажем пункт (4). Пусть $d = p_1^{k_1} \cdot \ldots p_l^{k_l}$ — экспонента группы G, где $p_1, \ldots p_l \in \mathbb{P}$. Тогда $\exists g_1, \ldots g_l \in G$, порядки которых делятся на $p_1^{k_1}, \ldots p_l^{k_l}$ соответственно.

Если $\operatorname{ord}(g) = mn$, то $\operatorname{ord}(g^m) = n$. Возведем $g_1, \ldots g_l$ в нужные степени и считаем, что $\operatorname{ord}(g_i) = p_i^{k_i} \quad \forall i \in [1, l]$.

Воспользуемся теоремой 21, и по индукции докажем, что $\operatorname{ord}(g_1 \cdot \ldots g_l) = \operatorname{ord}(g_1) \cdot \ldots \operatorname{ord}(g_l) = d$. □

Вопрос 23 Нормальные подгруппы. Гомоморфизмы групп. Свойства ядра и образа.

i Нормальные подгруппы

Def 37. Пусть $H \leqslant G$. H называется нормальной подгруппой, если $gH = Hg \quad g \in G$.

Designation. Обозначается: $H \trianglelefteq G$.

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

ii Гомоморфизмы групп

Def 38. Пусть $(G, *)$, $(H, \#)$ — группы. Функция $f : G \to H$ называется гомоморфизмом, если $f(a \cdot b) = f(a) \# f(b) \quad \forall a, b \in G$.

Образ гомоморфизма $\operatorname{Im} f = \{f(g) \mid g \in G\}$.

Ядро гомоморфизма $\operatorname{Ker} f = \{g \in G \mid f(g) = e_H\}$.

Def 39.

Мономорфизм — инъективный гомоморфизм.
Эпиморфизм — сюрьективный гомоморфизм.
Изоморфизм — биективный гомоморфизм.

Lemma 15. *Если $f : G \to H$ — гомоморфизм групп, $f(e_G) = e_H$ и $\forall x \in G : f(x^{-1}) - f(x)^{-1}$*

Lemma 16. *Пусть $f : G \to H$ — гомоморфизм групп, $g \in G$, $h = g(g)$. Тогда $f^{-1}(h) - g\operatorname{Ker} f$.*

Гомоморфизм инъективен тогда и только тогда, когда его ядро состоит из одного элемента.

Lemma 17. *Образ гомоморфизма групп является подгруппой, а ядро — нормальной подгруппой.*

Вопрос 24 Существование эпиморфизма групп с данным ядром, факторгруппа.

Statement 14. *Для любой нормальной подгруппы H группы G существует группа F и эпиморфизм $\pi : G \to F$, ядро которого равно H.*

Доказательство. Пусть $F = G/H$ и зададим отображение $\pi : G \to F$ по формуле $\pi(x) = xH$. Зададим операцию в F по формуле $(xH) \cdot (yH) = xyH$. Так как $H \trianglelefteq G$, эта операция не зависит от выбора представителей x и y смежных классов xH и yH:

$$xhyh' = xy(y^{-1}hy)h' \in xyH.$$

Ассоциативность операции следует из ассоциативности операций в G. Нейтральный элемент — смежный класс $eH = H$, обратный для xH — смежный класс $x^{-1}H$. Следовательно, H — группа. По построению F сразу получаем, что π — гомоморфизм. При этом π сюрьективно.

$$\pi(x) = e_{G/H} = H \iff x \in H.$$

Следовательно, $\operatorname{Ker} \pi = H$. ☐

Def 40. Группа, построенная в доказательстве, называется **факторгруппой** G по H, а отображение π — **канонической проекцией** или **гомоморфизмом редукции по модулю** H.

Вопрос 25 Универсальное свойство факторгруппы и теорема о гомоморфизме

Theorem 23 (универсальное свойство факторгруппы)**.** *Пусть $f : G \to H$ — гомоморфизм, а $N \trianglelefteq G$. Если $\operatorname{Ker} f \geqslant N$, то существует единственный гомоморфизм $g : G/N \to H$, такой что $f = g \circ \pi$.*

Если f — эпиморфизм, то g — эпиморфизм. Если $\operatorname{Ker} F = N$, то g — мономорфизм.

Доказательство. Пусть $x \in G$. $f = g \circ \pi \implies$

$$g(xN) = f(x) \tag{1}$$

Если y — другой представитель смежного класса xN, то $y = xn$ для некоторого $n \in N$, и $g(yN) = f(y) = f(x)f(n) = g(x)$, так как $n \in N \leqslant \operatorname{Ker} f$. Следовательно, формула 1 корректно определяет отображение g. Оно является гомоморфизмом из определения умножения смежный классов. Очевидно, что g единственно, так как удовлетворяет $f = g \circ \pi$.

Если композиция сюрьективна, то g обязан быть сюрьективным, так как применяется последним.

Если $\operatorname{Ker} f = N$,

$$xN \in \operatorname{Ker} g \iff x \in \operatorname{Ker} f = N \iff xN = 1_{G/N}.$$

☐

Theorem 24 (о гомоморфизме групп)**.** *Пусть $f : G \to H$ — гомоморфизм групп. Тогда*

$$\operatorname{Im} f \cong G/\operatorname{Ker} f.$$

Доказательство. Отображение $\overline{f} : G \to \operatorname{Im} f$, заданное формулой $\overline{f}(x) = f(x)$ является эпиморфизмом, причем его ядро равно $\operatorname{Ker} f$. По универсальному свойству факторгруппы существует изоморфизм $\operatorname{Im} f \to G/\operatorname{Ker} f$. ☐

Вопрос 26 Сопряженные элементы, коммутаторы, коммутант.

i Сопряженные элементы

Def 41. Пусть $x, y \in G$. Элемент $x^y := y^{-1}xy$ называется правым сопряженным к x при помощи y. А ${}^y x = x^{y^{-1}} = yxy^{-1}$ — левым сопряженным к x при помощи y.

Lemma 18. *Пусть $x, y, z \in G$. Тогда*

1. $(xy)^z = x^z \cdot y^x$ *и* ${}^z(xy) = {}^z x \cdot {}^z y$, *то есть сопряжение при помощи z — гомоморфизм.*
2. ${}^{yz}x = {}^z({}^y x)$, *то есть отображение из группы G в группу автоморфизмов группы G, переводящее элемент в левое сопряжение при помощи этого элемента, является гомоморфизмом.*

Note. Отношение «x сопряжено с y» — отношение эквивалентности. Классы этой эквивалентности называются классами сопряженных элементов.

Lemma 19. *Пусть $H = \langle X \rangle$ — подгруппа в группе $G = \langle Y \rangle$. Тогда $H \trianglelefteq$ тогда и только тогда, когда* $\forall x \in X,\ y \in Y : x^y \in H$

Доказательство.

$\boxed{\Longrightarrow}$ Очевидно.

$\boxed{\Longleftarrow}$ Пусть $h \in H$, а $g = y_1 \cdot \ldots y_m \in G, \quad y_i \in Y$.

Индукция по m.

База: $m = 0$. $g = 1$.

Переход: $m - 1 \to m$. По предположению индукции $h^{y_1\cdot\ldots y_{m-1}} \in H$, следовательно, $h^{y_1\cdot\ldots Y_{m-1}} = x_1 \cdot \ldots x_n$ для некоторого $n \in N$ и $x_1, \ldots x_n \in X$. Тогда $h^g = (x_1 \cdot \ldots x_n)^{y_m} = x_1^{y_m} \cdot \ldots x_n^{y_m}$, а каждый сомножитель лежит в H по условию.

$\square$

Def 42. Наименьшая нормальная подгруппа группы G, содержащая подгруппу H называется порождающим замыканием H и G.

Designation. Обозначается: H^G.

Note. H^G порождается всеми элементами вида $h^g,\ h \in H,\ g \in G$.

ii Коммутатор

Def 43. Коммутатором называется элемент $[x, y] = xyx^{-1}y^{-1}$.

Property. *Выполнены следующие коммутаторные формулы:*

1. $[x, y]^{-1} = [y, x]$
2. $[x, yz] = [x, y] \cdot {}^y[x, z]$
3. $[x, y]^z = [x^z, y^z]$

iii Коммутант

Def 44. Пусть X, Y — подгруппы G. **Взаимным коммутантом** этих подгрупп называется подгруппа, порожденная всеми коммутаторами $[x, y], \quad x \in X,\ y \in Y$.

Designation. Обозначается: $[X, Y]$.

Lemma 20. *Пусть X и Y — подгруппы в G. Тогда $[X, Y] \trianglelefteq \langle X \cup Y \rangle$.*

Доказательство. По формуле 2 из свойств коммутаторов ii

$$[x, y]^z = {}^{z^{-1}}[x, y] = [x, z^{-1}]^{-1} \cdot [x, z^{-1}y] \in [X, Y].$$

Аналогично, для $x, z \in X,\ y \in Y$:

$$[x, y]^z = \left([y, z]^{-1}\right)^z = \left({}^{z^{-1}}[y, x]\right)^{-1} = \left([y, x^{-1}]^{-1} \cdot [y, z^{-1}x]\right)^{-1} = [z^{-1}z, y] \cdot [z^{-1}, y]^{-1} \in [X, Y].$$

По лемме 19 получаем нормальную подгруппу. ☐

Lemma 21. *Пусть S_X и S_y — множества образующих подгрупп X и Y соответственно. Тогда $[X, Y] = \langle [s, t] \mid s \in S_X,\ t \in S_Y \rangle^{\langle X \cup Y \rangle} = Z$.*

Доказательство. По лемме 20 $Z \subset [X, Y]$. Докажем, что любой образующий элемент $[X, Y]$ содержится в Z.

Пусть $s \in S_X,\ y = t_1 \dots t_n, \quad t_i \in S_Y$. По индукции докажем, что $[s, y] \in Z$.

База: $n = 1$. По определению Z.
Переход: $n - 1 \to n$.

$$[s, y] = [s, t_1] \cdot {}^{t_1}[s, t_2 \dots t_n].$$

По индукционному предположению $[s, t_2 \dots t_n] \in Z$, следовательно, $[s, y] \in Z \quad \forall s \in S_X,\ y \in Y$. Аналогично для $s \in S_Y,\ x = t_1, \dots t_n, \quad t_i \in S_X$.

☐

Statement 15. *$\varphi : G \to A$ — гомоморфизм. A — абелева $\Longrightarrow [G, G] \subseteq \operatorname{Ker} \varphi$.*

Доказательство.

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

Тогда

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

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

Вопрос 27 Соотношения между трансвекциями. Взаимные коммутанты верхнетреугольных групп. Порождение верхнетреугольной группы.

Designation. Пусть F — поле,

$$U_n^{(k)} = U_n^{(k)}(F) = \{a \in M_n(f) \mid a_{ii} = 1,\ a_{ij} = 0\ \forall i \neq j,\ j - i < k\}.$$

$$U_n = U_n F \coloneqq U_n^{(1)}(F) \land U_n^{(k)} = \{1\}\ k \geqslant n.$$

Lemma 22. *Группа $U_n^{(k)}$ порождена трансвекциями $t_{ij}(\alpha)$ по всем $\alpha \in F \land j - i \geqslant k$.*

Statement 16. *Пусть i, j, k, h — попарно различные индексы. Тогда*

$$\begin{aligned} t_{ij}(\alpha)t_{ij}(\beta) &= t_{ij}(\alpha+\beta) \\ [t_{ij}(\alpha), t_{jk}(\beta)] &= t_{ik}(\alpha\beta) \\ [t_{ij}(\alpha), t_{ki}(\beta)] &= t_{kj}(-\alpha\beta) \\ [t_{ij}(\alpha), t_{hk}(\beta)] &= e. \end{aligned}$$

Lemma 23. *Группа $U_n^{(k)}$ нормальна в U_n. Более того, $[U_n^{(k)}, U_n^{(m)}] = U_n^{(k+m)}$.*

Доказательство. Используем лемму 19 и формулы из прошлого утверждения, чтобы доказать нормальность.

Из формул прошлого утверждения также следует

$$[U_n^{(k)}, U_n^{(m)}] \subset U_n^{(k+m)}.$$

Так как $U_n^{(k+m)}$ нормальна, из леммы 21 следует, что $[U_n^{(k)}, U_n^{(m)}]$ содержится в этой подгруппе. С другой стороны, каждая образующая группы $U_n^{(k+m)}$ — коммутатор образующих $U_n^{(k)}$ и $U_n^{(m)}$. А тогда выполнено требуемое равенство. □

Lemma 24. *Любой элемент группы U_n единственным образом выражается в виде произведения $\prod_{j>i} t_{ij}(\alpha_{ij})$ в любом наперед заданном порядке на множестве пар $(i, j),\ j > i$.*

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

$$u \in \prod_{1 \leqslant j-i<k} t_{ij}(\alpha_{ij}) \cdot U_n^{(k)},$$

где произведение берется в заданном порядке.

База ($k = 1$): утверждение очевидно, доказывать нечего.

Переход ($k - 1 \to k$). По предположению индукции

$$u \in \prod_{1 \leqslant j-i<k-1} t_{ij}(\alpha_{ij}) \cdot U_n^{(k-1)}.$$

Любой элемент $a \in U_n^{(k-1)}$ лежит в смежном классе

$$\prod_{t_{i\ i+k-1}} (\alpha_{i\ i+k-1}) U_n^{(k)}, \quad a_{i\ i+k-1} \text{ — элемент матрицы } a \text{ на позиции } (i, i+k-1).$$

По лемме 23 трансвекции $t_{i\ i+k-1}(\alpha_{i\ i+k-1})$ коммутируют с элементами U_n по модулю $U_n^{(k)}$. (Так как коммутатор $[u, t_{i\ i+k-1}(\alpha_{i\ i+k-1})] \in U_n^{(k)} \quad \forall u \in U_n$. То есть $[u, t_{i\ i+k-1}(\alpha)] \equiv 1 \mod U_n^{(k)}$.) Поэтому эти трансвекции можно поставить в нужное место произведения $\prod_{1 \leqslant j-i<k-1} t_{ij}(a_{ij})$, чтобы получить требуемое включение. Получаем

$$a \equiv \prod_{1 \leqslant j-i<k} t_{ij}(\alpha_{ij}) \mod U_n^{(k)}.$$

□

Вопрос 28 Приведенное разложение Брюа. Соотношение между клетками Брюа и Гаусса.

Theorem 25 (приведенное разложение Брюа)**.** *Пусть $w \in W$. Тогда $B_n w B_n = U_w w B_n$, следовательно, $\mathrm{GL}_n(F) = U_w w B_n$. При этом разложение данного элемента единственно, то есть*

$$\forall g \in \mathrm{GL}_n(F)\ \exists! w \in W, u \in U_w, b \in B_n : g = uwb.$$

Доказательство. Обозначим через $T_n = T_n(F)$ множество обратимых диагональных матриц. Любая обратимая треугольная матрица однозначно представляется в виде произведения унитреугольной на диагональную:

$$B_n = U_n T_n.$$

Кроме того, $T_n^w = T_n$. Поэтому

$$B_n W B_n = U_n w B_n.$$

Обозначим $\overline{U}_w = \langle t_{ij} \mid t_{ij}(\alpha)^w \in U_n \rangle$. Тогда по лемме 24 $U_n = U_w \overline{U}_n$. Следовательно,

$$B_n w B_n = U_n w B_n = U_w \overline{U_n} w B_n = U_w \overline{U}_n^w B_n \subseteq U_w w B_n.$$

Обратное включение очевидно.

Докажем единственность.

Пусть $uwb = u'w'b'$, где $w, w' \in W$, $u \in U_{w'}$, $b, b' \in B_n$. Тогда $(w')^{-1}(u')^{-1}uw = b'b^{-1} = c \in B_n$.

Пусть w соответствует перестановке σ, то есть $w_{i,\sigma(i)} = 1$ для некоторой перестановки $\sigma \in S_n$, и $w_{ij} = 0$ при $j \neq \sigma(i)$.

Пусть w' соответствует $\sigma' \in S_n$. Тогда у матрицы $(w')^{-1}$ единицы стоят в позициях $(\sigma'(i), i)$.

Следовательно, $c_{\sigma'(i)\sigma(i)} = \big((u')^{-1}u\big)_{ii} = 1$. Если $\sigma \neq \sigma'$, то $\exists i : \sigma'(i) > \sigma(i)$. Но тогда c не верхнетреугольная матрица.

Тогда $w = w'$, $\sigma = \sigma'$.

По определению U_w имеем $(u')^{-1}u \in U_w$ и $c = w^{-1}(u')^{-1}uw \in U_n^-$. Так как $U_n^- \cap B_n = \{e\}$, то $u' = u$, $b' = b$. □

Corollary 3. *Любая клетка Брюа содержится в соответствующей клетке Гаусса.*

Доказательство. $B_n w B_n = U_w w B_n = w U_w^w B_n \subseteq w B_n^- B_n$ □

Вопрос 29 Симметрическая группа. Циклическая запись перестановки. Классы сопряженных элементов в S_n.

i Симметрическая группа

Def 45. Пусть X — множество. Множество биекций $X \to X$ с операцией композиции называется симметрической группой множества X и обозначается через S_X.

Def 46 (Перестановка). $\sigma \in S_n \iff \sigma : \{1, \dots n\} \overset{\sim}{\to} \{1, \dots n\}$

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 47. Перестановки $(j_1 \dots j_n)$, $(k_1 \dots . k_m)$ называются **независимыми**, если $j_h \neq j_l \quad \forall h, l$.

Lemma 25. *Любая перестановка равна произведению независимых (композиции) циклов.*

Def 48. **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 повторятся.

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

Lemma 26.

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

Следовательно, сопряжение не меняет циклический тип.

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

Def 49. Отношение на группе G :

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

$x = y^z \wedge y = ab \Longrightarrow x = (a^b)^z - a^{bz}$.
Класс эквивалентности «$\sim_c$» — класс сопряженных элементов.

Theorem 26. *Класс сопряженных элементов в S_n состоит из всех перестановок фиксированного циклического типа.*

Доказательство. Следует из леммы 26 ☐

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

$$(12)(34)$$
$$(13)(24)$$
$$(14)(32)$$

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

Statement 17. $\operatorname{ord}(ab) \mid \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$. *Порядок перестановки равен НОКу порядков независимых циклов.*

Вопрос 30 Транспозиции и инверсии. Четность перестановки.

Def 50 (Инверсия)**.** Пусть $\sigma \in S_n$. **Инверсия** в перестановке σ — пара $(i, j) : i < j \wedge \sigma(i) > \sigma(j)$.

Def 51 (Четность перестановки)**.**

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

$$\sigma \mapsto \text{ количество инверсий по модулю 2.}$$

Def 52. **Транспозиция** — циклическая перестановка длины 2.

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

Lemma 27. *Любая перестановка σ раскладывается в произведение транспозиций соседних индексов.*

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

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. ☐

Lemma 28. $\tau = \sigma(i\ i+1) \Rightarrow |I(\tau) - I(\sigma)| = 1$

Lemma 29. *Если $\sigma = \tau_1 \cdot \tau_2 \ldots \cdot \tau_k, \quad \forall i : \tau_i$ — транспозиция соседних индексов, то*

$$\varepsilon(\sigma) \equiv k \mod 2.$$

Theorem 27. $\varepsilon : S_n \to \mathbb{Z}/2\mathbb{Z}$ *— гомоморфизм групп.*

Доказательство.

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

Проверим требуемые свойства:

$\varepsilon \equiv k \mod 2, \quad \varepsilon(\rho) \equiv n - k \mod 2$

$\varepsilon(\sigma\rho) \equiv m \mod 2 \equiv \varepsilon(\sigma) + \varepsilon(\rho) \mod 2$

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

$\varepsilon((i_1, \ldots i_k)) = \varepsilon((1, \ldots k)) \equiv k - 1 \mod 2$ ☐

Вопрос 31 Определение кольца, подкольца, идеала, прямое произведение колец

i Кольцо

Def 53. Кольцо — множество R, на котором заданы операции $+, \times$, обладающие следующими свойствами $\forall a, b, c \in R$:

$a + b = b + a$ (коммутативность сложения)

2. $a + (b + c) = (a + b) + c$ (ассоциативность сложения)
3. $\exists 0 \in R : a + 0 = 0 + a = a$ (нейтральный элемент по сложению)
4. $\forall a \in R \; \exists b \in R : a + b = b + a = 0$ (обратный элемент по сложению)
5. $(a \times b) \times c = a \times (b \times c)$ (ассоциативность умножения)
6. $\begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}$ (дистрибутивность)

Кольцо является кольцом с единицей, если

$$\exists e \in R \; \forall a \in R : a \times e = e \times a = a.$$

Кольцо является коммутативным кольцом, если

$$\forall a, b \in R : a \times b = b \times a.$$

Property.

1. *Нейтральный по сложению единственный.*
2. *Обратный элемент по сложению существует и единственен для любого элемента кольца.*
3. *Нейтральный по умножению единственен, если существут.*
4. $\forall a \in R : a \times 0 = 0$
5. $-b = (-1) \times b$
6. $(-a) \times b = (-ab)$
7. $(-a) \times (-b) = (ab)$

ii Подкольцо

Def 54. Подмножество $A \subset R$ называется подкольцом R, если A само является кольцом относительно операций, определенных в в R.

Designation. Говорят, что R — расширение кольца A.

Property.

1. *Ноль и единица кольца являются нулем и единицей в подкольце.*
2. *Подкольцо наследует свойство коммутативности.*
3. *Пересечение любого набора подколец — подкольцо.*

Def 55. Пусть X — подмножество кольца R. Подкольцом, порожденным множеством X, называется наименьшее подкольцо в R, содержащее X.

Lemma 30. *Подкольцо, порожденное X, состоит из всевозможных сумм элементов вида $x_1 \times \ldots x_k$, где $k \in \mathbb{N}$, $x_i \in X \cup \{1\}$ (если имеется ввиду кольцо без 1, то $x_i \in X$).*

iii Идеалы

Def 56. Аддитивная подгруппа I кольца R называется **левым (правым) идеалом**, если $\forall r \in R,\ x \in I: rx \in I$ ($xr \in I$).

Двусторонний идеал — идеал, являющийся левым и правым.

Property.

1. *Пересечение любого числа идеалов — идеал.*

Def 57. (Левым, правым или двусторонним) **идеалом, порожденным подмножеством** X кольца R, называется наименьший (левый, правый или двусторонний) идеал, содержащий X.

Идеал коммутативного кольца, порожденный одним элементом, называется **главным идеалом**.

Designation. Левый идеал, порожденный множеством X, обозначается $\sum\limits_{x\in X} xR$ (правый — $\sum\limits_{x\in X} Rx$). Если R — коммутативное кольцо, то идеал, порожденный $X \subseteq R$ обозначают (X).

Lemma 31. *(Левый, правый или двусторонний) идеал, порожденный X, состоит из всевозможных сумм элементов вида (rx, xr или rxs), где $r, s \in R,\ x \in X \cup \{1\}$ (если имеется ввиду кольцо без 1, то $x_i \in X$).*

iv Прямое произведение колец

Def 58. **Произведение колец** R и S — множество пар $(r, s),\ r \in R,\ s \in S$ с покомпонентными операциями $\forall r_1, r_2 \in R,\ s_1, s_2 \in S$:

$(r_1, s_1) + (r_1, s_2) = (r_1 + r_2, s_1 + s_2)$

- $(r_1, s_1) \cdot (r_1, s_2) = (r_1 r_2, s_1 s_2)$

Вопрос 32 Гомоморфизмы колец, ядро, образ, слои

Def 59. Пусть R, A — кольца. Функция $f : R \to A$ называется **гомоморфизмом колец**, если

$$\begin{matrix} f(a+b) = f(a) + f(b) \\ f(a \cdot b) = f(a) \cdot f(b) \end{matrix} \quad \forall a, b \in R.$$

Для гомоморфизмов колец с единицей будем требовать также, чтобы $f(1_R) = 1_A$.

Def 60. $f : R \to A$ — гомоморфизм.

Образ гомоморфизма f — $\operatorname{Im} f = \{f(x) \mid x \in R\}$
Ядро гомоморфизма f — $\operatorname{Ker} f = f^{-1}(0)$
Мономорфизм — инъективный гомоморфизм.
Эпиморфизм — сюрьективный гомоморфизм.
Изоморфизм — биективный гомоморфизм.

Если между двумя кольцами существует изоморфизм, они называются **изоморфными**.

Lemma 32. *Пусть $f : R \to A$ — гомоморфизм колец. Тогда $f(0) = 0$, и $\forall x \in R : f(-x) = -f(x)$.*

Если f — гомоморфизм колец с единицей, и $x \in R^*$, то $f(x) \in A^*$ и $f^{(x^{-1})} = f(x)^{-1}$.

Lemma 33. *Пусть $f : R \to A$ — гомоморфизм, $x \in R$, $y = f(x)$. Тогда $f^{-1}(y) = x + \operatorname{Ker} f$.*

Гомоморфизм инъективен тогда и только тогда, когда его ядро равно $\{0\}$.

Lemma 34. *Образ гомоморфизма колец является подкольцом, а ядро — двусторонним идеалом.*

Вопрос 33 Факторкольцо, существование эпиморфизма с данным ядром

Theorem 28. *Для любого двустороннего идеала I кольца R существует кольцо A и эприморфизм $\pi : R \to A$, ядро которого равно I.*

Доказательство. Так как I — подгруппа аддитивной группы кольца, то можно рассмотреть факторгруппу R/I. Зададим умножение:

$$(r + I) \cdot (s + I) = rs + I, \qquad r, s \in R.$$

Если $r + x \in r + I$ и $s + y \in s + I$ — другие представители классов,

$$(r + x)(s + y) = rs + (ry + xs + xy) \in rs + I.$$

Следовательно, определение корректно. Операции в R/I удовлетворяют свойствам кольца, так как операции в R удовлетворяют.

Отображение π зададим аналогично группам: $\pi(x) = x + I$ — это гомоморфизм, причем сюрьективный. Найдем его ядро:

$$\pi(x) = e_{R/I} = e + I = I \iff x \in I.$$

Значит, $\operatorname{Ker} \pi = I$. □

Def 61. Кольцо R/I называется **фактокольцом** R по I, а отображение $\pi = \pi_I$ — **канонической проекцией** или **гомоморфмзмом редукции по модулю** I.

Вопрос 34 Универсальное свойство факторкольца и теорема о гомоморфизме

Theorem 29 (Универсальное свойство факторкольца)**.** *Пусть R, R' — кольца, I — двусторонний идеал в R, $f : A \to R'$. Если $I \subseteq \operatorname{Ker} f$, то существует единственный гомоморфизм $g : R/I \to R'$ такой, что $f = f \circ \pi$.*

Если $\operatorname{Ker} f = I$, то g инъективен. Если f сюрьективен, то g сюрьективен.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & R' \\
R/I \arrow[ur, "g"'] &
\end{tikzcd}$$

Доказательство. Пусть $x \in R$. $f = g \circ \pi \implies$

$$g(x + I) = f(x) \tag{2}$$

Если y — другой представитель $x+I$, то $y = x+a$ для некоторого $a \in I$, и $g(y+I) = f(y) = f(x)+f(a) = g(x)$, так как $a \in I \subseteq \operatorname{Ker} f$. Проверим $g(xy + I) = g(x + I)g(y + I)$:

$$g(xy + I) = f(xy) = f(x)f(y) = g(x + I)g(y + I).$$

Также

$$g((x+y)+I) = f(x+y) = f(x) + f(y) = g(x+I) + g(y+I).$$

Следовательно, формула 2 корректно определяет отображение g. Оно является гомоморфизмом (проверили выше). Очевидно, что g единственно, так как удовлетворяет $f = g \circ \pi$.

Если композиция сюрьективна, то g обязан быть сюрьективным, так как применяется последним.

Если $\operatorname{Ker} f = I$,

$$x + I \in \operatorname{Ker} g \iff x \in \operatorname{Ker} f = I \iff x + I = 1_{R/I}.$$

□

Вопрос 35 Определение комплексных чисел, арифметические операции, геометрическое представление

i Определение и арифметика

Def 62. Факторкольцо $\mathbb{C} = \mathbb{R}[t]\diagup(t^2+1)$ называется полем комплексных чисел.

Композиция отображений $\mathbb{R} \hookrightarrow \mathbb{R}[t] \twoheadrightarrow \mathbb{C}$ является гомоморфизмом колец с единицей. Так как $\mathbb{R}$ — поле, то она инъективна, ее ядро — идеал в $\mathbb{R}$, который тривиален. Будем отождествлять элементы поля $\mathbb{R}$ с их образами под действием этого мономорфизма и считать, что $\mathbb{R}$ — подполе в $\mathbb{C}$:

$$r \in \mathbb{R} \longleftrightarrow r + (t^2+1)\mathbb{R}[t].$$

Обозначим через i смежный класс $t + (t^2+1)\mathbb{R}[t]$. Заметим, что

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

Рассмотрим элемент поля $p \in \mathbb{R}[t]$:

$$\begin{aligned} &p = (t^2+1)\cdot f + (a+bt) \in a + bt + (t^2+1)\mathbb{R}[t] \\ &p + (t^2+1)\mathbb{R}[x] = a + bi \end{aligned}$$

Значит, любой элемент поля может быть однозначно записан в виде $a+bi, \quad a,b \in \mathbb{R}$. Сложение определено по правилу:

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

Так как $i^2 = -1$:

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

Def 63. Пусть $x, y \in \mathbb{R}$ и $z = x + yi$. Тогда $x = \operatorname{Re} z$ — вещественная часть, а $y = \operatorname{Im} z$ — мнимая часть числа z.

Число $\overline{z} = x - yi$ называется комплексно сопряженным к z.

Property.

1. $(a+bi)(a-bi) = a^2 + b^2$
2. $(a+bi) + (a-bi) = 2a$
3. $z \in \mathbb{R} \iff z = \overline{z}$
4. $z \in \mathbb{R} \iff z + \overline{z} \in \mathbb{R}$
5. $z \in \mathbb{R} \iff z\overline{z} \in \mathbb{R}$
6. *Мультипликативный обратный:*

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i.$$

Statement 18. *Отображение* $\mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$ *— автоморфизм поля* $\mathbb{C}$.

ii Геометрическое представление

Def 64. Модуль комплексного числа z — $|z| = \sqrt{a^2+b^2}\sqrt{z\overline{z}}$

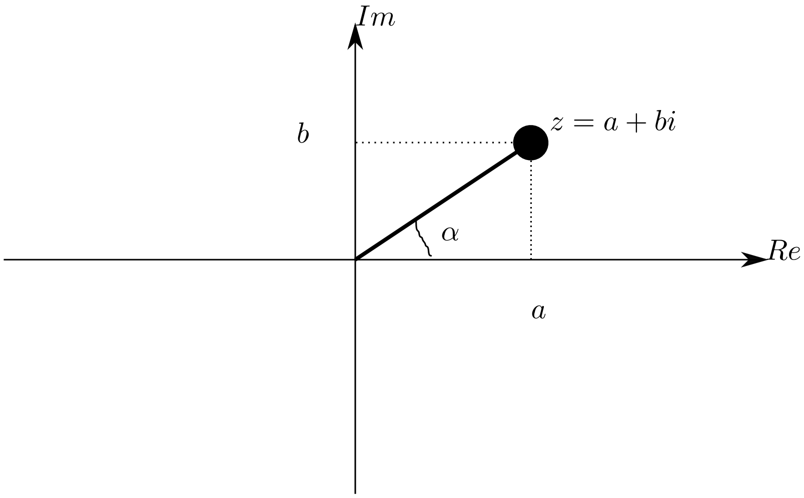

Рис. 1: Комплексное число на плоскости

Def 65. $\arg z \coloneqq \alpha \in \mathbb{R}\diagup 2\pi\mathbb{Z}$

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

Можем выразить через аргумент:

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

Тогда $z = |z| \cdot (\cos\alpha + i\sin\alpha)$

Вопрос 36 Тригонометрическая и показательная форма комплексных чисел. Операции в тригонометрической форме

i Тригонометрическая форма

Тригонометрическая форма: $z = a + bi = r(\cos\varphi + i\sin\varphi)$.

Операции в тригонометрической форме

Умножение:

$$\begin{aligned}
zw &= |z|(\cos\arg z + i\sin\arg z)\cdot|w|(\cos\arg w + i\sin\arg w) = \\
&= |z|\cdot|w|\cdot\Big(\cos(\arg z)\cos(\arg w) - \sin(\arg z)\sin(\arg w) + i\big(\cos(\arg z)\sin(\arg w) + \sin(\arg z)\cos(\arg w)\big)\Big) =. \\
&= |z|\cdot|w|\cdot\Big(\cos(\arg z + \arg z) + i\sin(\arg z + \arg w)\Big)
\end{aligned}$$

Для целого n выполняется **формула Муавра**:

$$z^n = |z|^n\Big(\cos(n\arg z) + i\sin(n\arg z)\Big).$$

Единственность представления комплексного числа в тригонометрической форме и формулу произведения в тригонометрической форме можно выразить так:

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

Так как $\ln : \mathbb{R}^*_{>0} \to \mathbb{R}$ — изоморфизм:

Statement 19. $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z}$

Доказательство. Отображения $z \mapsto (\ln|z|, \arg z)$ и $(r, x) \mapsto e^r(\cos x + i\sin x)$ являются взаимно обратными гомоморфизма ми. □

ii Показательная форма

Statement 20. *Напишем степенные ряды для экспоненты и тригонометрических функций:*

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

$$e^{i\alpha} = \sum_{n=2k}\frac{(i\alpha)^{2k}}{(2k)!} + \sum_{n=2k+1}\frac{(i\alpha)^{2k+1}}{(2k+1)!}.$$

$$e^{i\alpha} := \cos\alpha + i\sin\alpha.$$

$$\varepsilon(\alpha) = e^{i\alpha}$$

Def 66 (Показательная форма комплексного числа)**.**

$$z = |z|\cdot e^{i\cdot Argz}$$

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

2π — период для экспоненты.

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

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

Вопрос 37 Строение мультипликативной группы комплексных чисел, корни из 1, уравнение $z^n = w$

Note. Тут что-то написано с лекций, возможно, этого недостаточно.

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 $\mathbb{R}^*_{>0} \times \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{C}^*$ — изоморфизм.

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

$$Ln : \mathbb{C}^* \to \mathbb{C}/3\pi\mathbb{Z}.$$

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

Statement 21 (вычисление корня n-й степени). *Вычисление корня в аддитивной группе* $\mathbb{C}/2\pi\mathbb{Z}$ *— решение уравнения:*

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

$z^n = 1, \quad z = Lnz$, *далее*

$$nx = 0 \mid 2\pi i\mathbb{Z}.$$

$$z = e^x = e^{\frac{2\pi i k}{n}}.$$

$$z^n \iff z = e^{\frac{2\pi i k}{n}}, k \in \mathbb{Z}/n\mathbb{Z}.$$

$$\Theta_n(Z) = z^k \text{ — гомоморфизм } \mathbb{C} \to \mathbb{C}^*.$$

$$\mu_n = \operatorname{Ker} \Theta_n = \{e^{\frac{2\pi i k}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z}\}.$$

Эти числа делят окружность на n равных частей.

$\mathbb{Z}/n\mathbb{Z} \to \mu_n$
$k + n\mathbb{Z} \mapsto e^{\frac{2\pi i k}{n}}$ — изоморфизм.

Def 67. Образующие элементы μ_n называются превообразными корнями из 1.

Corollary 4. $e^{\frac{2\pi i k}{n}}$ *— превообразный корень тогда и только тогда, когда* $\gcd(k, n) = 1$.

Statement 22. $z^n = w = re^{i\varphi}$. *Одно из решений этого уравнения:* $\left(\sqrt[n]{r} \cdot e^{\frac{i\varphi}{n}}\right)^n$.

А все решения можно записать:

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

Theorem 30 (Основная теорема алгебры). $p \in \mathbb{C}[x],\ \deg p \geqslant 1$

Тогда $\exists \alpha \in \mathbb{C} : p(\alpha) = 0$.

Theorem 31 (Лиувилль). *Любая ограниченная дифференцируемая функция* $\mathbb{C} \to \mathbb{C}$ *— константа.*

Вопрос 38 Евклидовы кольца и кольца главных идеалов

Def 68. Элемент a кольца R называется делителем нуля, если существует $b \in R \setminus \{0\}$ такой, что $ab = 0$.

Область целостности — коммутативное кольцо с единицей без нетривиальных делителей нуля (то есть кроме нуля).

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

Def 69. Пусть задана функция $f : R \to \mathbb{N} \cup \{-\infty\}$, обладающая следующим свойствами:

1. $f(0) < f(r), \quad \forall r \in R \setminus \{0\}$;
2. $\forall a, b \in R,\ b \neq 0\ \exists q, r \in R : a = bq + r \wedge f(r) < f(b)$.

Тогда R — евклидова кольцо с евклидовой нормой f.

Def 70. Кольцо R называется кольцом главных идеалов, если любой идеал в R является главным, то есть имеет вид aR для некоторого $a \in R$.

Область главных идеалов (ОГИ) — область целостности, в которой любой идеал главный.

Theorem 32. *Евклидово кольцо является областью главный идеалов.*

Доказательство. Пусть $I \triangleleft R$ — нетривиальный идеал. Рассмотрим $b \in I$ с минимальной возможной евклидовой нормой.

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

Тогда $\exists q, r \in R$:

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

$$r = \underbrace{a}_{\in I} - \underbrace{bq}_{\in I} \in I.$$

Если $r \neq 0$, то $f(b) \leqslant f(r) < f(b)$. Противоречие.

Значит, произвольный элемент из I делится на b, следовательно, $I \subseteq bR$. С другой стороны, $b \in I \Longrightarrow bR \subseteq I$, из чего следует равенство. ☐

Exs. Примеры евклидовых колей и их норм:

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

Ex. $\mathbb{Z}[\sqrt{-19}]$ — не евклидово кольцо, но кольцо главных идеалов.

Вопрос 39 Взаимно простые идеалы, их пересечение и произведение

Пусть R — кольцо, I, J — идеалы в R.

Statement 23. *Сумма идеалов $I + J = \{a + b \mid a \in I,\ b \in J\}$ является идеалом, причем это наименьший идеал, содержащий $I \cup J$.*

Def 71. **Произведение идеалов** — идеал IJ, порожденный элементами ab по всем $a \in I,\ b \in J$:

$$\left\{ \sum_{i=1}^{k} a_i b_j \middle| k \in \mathbb{N},\ a_i \in I,\ b_j \in J \right\}.$$

Def 72. Идеалы I и J кольца R называются **взаимно простыми**, если $I + J = R$.

Lemma 35. *Если I и J — взаимно простые идеалы, то $IJ = I \cap J$.*

Доказательство.

$\boxed{\subseteq}$ По определению идеала.

$\boxed{\supseteq}$ Пусть $x \in I \cap J$. Так как I и J взаимно просты, то $\exists a \in I,\ b \in J : a + b = 1$. Тогда $x = xa + xb \in (I \cap J)I + (I \cap J)J \subset IJ$

□

Def 73. A, B — кольца. **Декартово произведение** колец — множество

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

с покомпонентными операциями:

$$\begin{array}{c} (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) \end{array}.$$

Theorem 33. *Пусть $I + J = R$. Тогда*

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

Доказательство. Рассмотрим естественный гомоморфизм:

$$\begin{array}{c} \varphi : R \to R/I \oplus R/J \\ r \mapsto (r + I, r + J) \end{array}$$

Посмотрим на ядро φ:

$$\operatorname{Ker} \varphi \ni r \iff \begin{cases} r + I = I \\ r + J \end{cases} \iff r \in I \cap J = I \cdot J$$

Докажем, что φ — сюрьекция:

$$\text{Пусть } \exists a \in I, b \in J : a + b = 1.$$

$$r = br_1 + ar_2 \equiv r_1 \mod I.$$

$$r = br_1 + ar_2 \equiv r_2 \mod J.$$

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

По теореме о гомоморфизме колец

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

□

Вопрос 40 Китайская теорема об остатках

Lemma 36. *Пусть* $J, I_1, \dots I_n$ *— идеалы в* R *и* J *взаимно прост с каждым из* I_i*. Тогда он взаимно прост с их произведением.*

Доказательство. Индукция.

База для $k = 2$.

$$R = J + I_1 = J + I_1 R = J + I_1(J + I_2) = (J + I_1 J) + I_1 I_2 \subseteq J + I_1 I_2 \tag{3}$$

Переход $n - 1 \to n$:

По предположению индукции $J + \underbrace{I_1 + \dots I_{n-1}}_{I} = R$. Нужно доказать , что $J + I \cdot I_n = R$. Проделаем действия из базы **??**.

□

Theorem 34 (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*

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

Note. Здесь дробью обозначается фактор кольцо.

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

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

Дальше по предположению индукции получаем то, что хотим. □

Statement 24. *Если* $x \equiv x_k \mod I_k, \quad k = 1, \dots n$*, то*

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

Note. В целых числах:

$$x \equiv x_k \mod m_k, \quad k = 1, \dots n.$$

Чтобы найти c_k, нужно решить диофантово уравнение:

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

Statement 25 (применение КТО)**.** *В* $F[t]$ *:*

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

равносильно

$$p \equiv y_k \mod (t - x_k).$$

$$p(t) \equiv \sum_{k=1}^{n} y_k \prod \frac{t - x_i}{x_k - x_i} \mod (t - x_i) \dots (t - x_n).$$

Вопрос 41 Существование максимальных идеалов

Def 74. Собственный идеал P 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

Def 75. Собственный идеал I называется **максимальным**, если он не содержится ни в каком другом собственном идеале.

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

Theorem 35. *Любой собственный идеал содержится в каком-то максимальном идеале.*

Доказательство. $J \lhd R$.

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

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

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

так как $\mathcal{Y}$ — линейно упорядочено.

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

$$a \in \bigcup_{I\in\mathcal{Y}} I \Longrightarrow ra \in \bigcup_{I\in\mathcal{Y}} I,\ \forall r \in R.$$

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

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

По лемме Цорна $\mathcal{X}$ содержит максимальный элемент. Пусть это M. Проверим, что M максимальный и среди всех собственных идеалов. Если $M \subseteq N \subsetneq R$, то $N \in \mathcal{X} \Rightarrow N = M$. ☐

Вопрос 42 Факторкольца по простым и максимальным идеалам. Прообразы простых и максимальных идеалов

Def 76. Кольцо называется **областью целостности**, если $\{0\}$ является простым идеалом. Другими словами, R — область целостности, если $R \neq \{0\}$ и $ab \neq 0 \ \forall a, b \in R \setminus \{0\}$.

Lemma 37. *Прообраз простого идеала — простой. Прообраз максимального идеала при эпиморфизме — максимальный.*

Доказательство. Пусть $\varphi : R_1 \to R_2$ — гомоморфизм.

1. Пусть P — простой идеал в R_2. Тогда $ab \in P \Longleftrightarrow a \in P \vee b \in P$. Теперь посмотрим на $\varphi^{-1}(P) = P'$.

$$a'b' \in P' \Longleftrightarrow \varphi(a'b') \in P \Longleftrightarrow \varphi(a')\varphi(b') \in P \Longleftrightarrow \varphi(a') \in P \vee \varphi(b') \in P \Longleftrightarrow a' \in P' \vee b' \in P'.$$

2. Пусть M — максимальный идеал в R_2, φ — эпиморфизм. Обозначим $M' = \varphi^{-1}(M)$. Предположим, что $\exists I \subsetneq M'$. Посмотрим на $\varphi(I)$. $\varphi(I) \supseteq \varphi(M') = M$. Так как M — максимальный идеал, а φ — эпиморфизм, $\varphi(I) = M$.

   Пусть $\exists a \in I : a \notin M'$. Тогда $\varphi(a) = \varphi(b),\ b \in M'$. // дальше надо что-то еще сделать

□

Corollary 5. *Идеал P — простой тогда и только тогда, когда R/P — область целостности. Идеал M — максимальный тогда и только тогда, когда R/M — поле.*

Corollary 6. *Любой максимальный идеал является простым.*

Theorem 36. *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 $p = mr \implies m \in pR \vee r \in pR$. В первом случае $mR = pR$, а втором $r = pa$, то есть $p = map \implies 1 = ma \implies mR = R$. Противоречие. □

Вопрос 43 Неприводимые и простые элементы

Designation. R — область целостности.

Def 77. Элемент $p \in R$ называется **простым**, если pR — простой.

Def 78. Элементы $a, b \in R$ называются **ассоциированными**, если $aR = bR$

Lemma 38. *R– область целостности. a, b — ассоциированные тогда и только тогда, когда $a = b\varepsilon$ для некоторого $\varepsilon \in \mathbb{R}^*$*

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 79. Необратимый элемент $a \in R$ называется **неприводимым**, если из равенства $a = bc$ следует, что b или c ассоциирован с a.

Lemma 39. *Необратимый элемент a неприводим тогда и только тогда, когда Он не раскладывается в произведение необратимых элементов.*

Lemma 40. *Ненулевой необратимый элемент a неприводим тогда и только тогда, когда aR — максимальный в множестве главных идеалов.*

Lemma 41. *Простой элемент неприводим.*

Доказательство. pR — простой идеал, следовательно,

$$ab = p \Rightarrow \left[\begin{array}{l} a \in pR \\ b \in pR \end{array}\right. \Rightarrow \left[\begin{array}{l} aR \subset pR \\ bR \subset pR \end{array}\right. .$$

Но $pR \subset aR \cap bR$. Тогда

$$\left[\begin{array}{l} aR = pR \\ bR = pR \end{array}\right. .$$

Получаем, что p — неприводим. □

Lemma 42. *Пусть R — область главных идеалов, $p \in R \setminus \{0\}$. Тогда следующие условия эквивалентны:*

1. *pR — максимальный идеал;*
2. *pR — простой идеал;*
3. *p неприводим.*

Доказательство.

$\boxed{1 \Longrightarrow 2}$ По следствию **??**

$\boxed{2 \Longrightarrow 3}$ По лемме **??**

$\boxed{3 \Longrightarrow 1}$ Если p неприводим, то по лемме **??** pR максимальный в множестве собственных главных идеалов, так как любой идеал в R является главным, то и в множестве собственных всех собственных идеалов.

□

Вопрос 44 Нёторовы кольца (два определения и их равносильность)

Def 80. Кольцо R называется **нётеровым**, если любое линейно упорядоченное по включению множество идеалов содержит наибольший элемент.

ACC — ascending chain condition (условие обрыва возрастающих цепей)

Lemma 43. *R — нётерово тогда и только тогда, когда любой идеал в R конечно порожден.*

Доказательство.

$\boxed{\Longrightarrow}$ Пусть R — нётерово, $I \triangleleft R$. Возьмем $a_1 \in I$.

$$a_1R = I_1 \neq I \Longrightarrow \exists a_2 \in I \setminus R.$$

Пусть $I_2 := a_1R + a_2R$. Аналогично получим $I_3, \ldots$. Получаем цепочку, которая на может быть бесконечной, значит она где-то оборвется и мы получим, что любой идеал порожден этим набором.

$\boxed{\Longleftarrow}$ $\mathcal{A}$ — линейно упорядоченное множество идеалов. Так как оно конечно порождено:

$$\bigcup_{I \in \mathcal{A}} I = a_1R + \ldots + a_nR.$$

$\exists I_1, \ldots I_n \in \mathcal{A}$, такие что $a_k \in I_k$. Так как $\mathcal{A}$ — линейно упорядочено, существует наибольший из I_k, пусть I_j.

$$a_1, \ldots a_n \in I_j \Longrightarrow a_1R + \ldots + a_nR = I_j.$$

Значит I_j — наибольший из $\mathcal{A}$

□

Вопрос 45 Существование разложения на неприводимые в неторовых кольцах

Theorem 37. *Любой необратимый элемент неторова кольца раскладывается в произведение неприводимых.*

Доказательство. Пусть $r = r_1 \in R$ — необратимый элемент. Если r_1 приводим, то $\exists r_2, r_3 \in R : r_1 = r_2r_3$, причем $r_1R \subsetneq r_2R$ и $r_1R \subsetneq r_3R$.

По индукции найдем для каждого приводимого r_i такие r_{2i}, r_{2i+1}, что $r_i = r_{2i}r_{2i+1}$, причем $r_iR \subsetneq r_{2i}R$ и $r_iR \subsetneq r_{2i+1}R$.

Получили бинарное дерево, каждая ветка которого конечна, так как кольцо R неторово. Следовательно, и все дерево конечно (иначе можно было бы выбирать ветку, которая еще не закончилась бесконечно). Кроме того, листья неприводимы, а r равно их произведению. □

Вопрос 46 Факториальные кольца. Факториальность кольца главных идеалов

Def 81. Область целостности R называется **факториальным кольцом**, если любой ненулевой необратимый элемент раскладывается в произведение неприводимых единственным образом с точностью до ассоциированности.

Theorem 38. *Пусть R — область целостности, в которой любой элемент раскладывается в произведение неприводимых и любой неприводимый элемент порождает простой идеал. Тогда R — факториально.*

Доказательство. Пусть $\varepsilon p_1 \cdot p_2 \ldots \cdot p_n = \theta q_1 \ldots q_m$, где все p_k b q_l неприводимы, ε, θ — обратимы.

Индукция по $\min(n, m)$. Докажем, что $n = m$ и сущестует перестановка S_n такая, что p_k ассоциирован с $q_{\sigma(k)}$ для всех $k \in [1, n]$.

База $m = 0$: правая часть обратима, значит $n = 0$.

Переход: $\min(n, m) > 1$. По условию идеал $p_n R$ простой. Поэтому $\exists l : g_l \in p_n R$. Так как q_l неприводим, то $q_l = \delta p_n$, где δ обратимо. Тогда

$$\varepsilon \cdot p_1 \ldots \cdot p_n = \theta \cdot q_1 \ldots \delta p_n \cdot q_m.$$

Сокращаем p_n:

$$\varepsilon p_1 \ldots p_n - 1 = \theta q_1 \ldots q_{l-1} q_{l+1} \ldots q_m.$$

По индукционному предположению $n - 1 = m - 1$ и существует биекция $\tau : \{1, \ldots n-1\} \to \{1, \ldots l-1, l+1, \ldots m\}$ такая, что p_k ассоциирован с $q_{\tau(k)}$ для всех $k \in [1, n-1]$. Пусть $\forall k \in [1, n-1] : \sigma(k) = \tau(k)$ и $\sigma(n) = l$. Такая перестановка подойдет.

☐

Note. Верно и обратное

Corollary 7. *Область главных идеалов является факториальным кольцом.*

Вопрос 47 Пример нефакториальной области целостности

Ex (пример нефакториальной области целостности)**.** Кольцо $\mathbb{Z}[\sqrt{-3}]$ не является факториальным кольцом, так как

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

Вопрос 48 Наибольший общий делитель и его линейное представление. Алгоритм Евклида

i НОД

Def 82. Пусть R — область главных идеалов, $a, b \in R$. Элемент d называется **наибольшим общим делителем** элементов a и b, если он делит и a, и b, и делится на любой другой делитель a и b.

Другими словами, d — наибольший общий делитель, если dR — наименьший главный идеал, содержащий a и b.

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

Theorem 39. *Пусть R — кольцо главных идеалов. Тогда $\forall a, b \in R \ \exists x, y \in R : ax + by = \gcd(a, b)$.*

Доказательство. Идеал $aR + bR$ является минимальным идеалом, содержащим a, b. По условию он является главным. Значит $aR = bR = dR$, тогда (по определению) $d = \gcd(a, b)$. ☐

Corollary 8. *Пусть R — кольцо главных идеалов. Идеалы aR и bR являются взаимно простыми, если у элементов a и b нет обратимых общих делителей (такие элементы называются* взаимно простыми*).*

Lemma 44. $\forall a, b, c \in R : \gcd(a, b) = \gcd(a - bc, b)$.

Доказательство. $a - bc$ и b содержатся в идеале $aR + bR$, поэтому $(a - bc)R + bR \subseteq aR + bR$. С другой стороны,

$$a = (a - bc) + bc \in (a - bc)R + bR.$$

Тогда $aR + bR \subseteq (a - bc)R + bR$.

Так как $(a - bc)R + bR = aR + bR$, то наименьший главный идеал, содержащий эти идеалы одинаковый. ☐

ii Алгоритм Евклида

Обозначим $r_0 = a$, $r_1 = b$. Пусть $i = 1$. Алгоритм Евклида состоит из следующих шагов:

1. Разделить r_{i-1} на r_i с остатком: $r_{i-1} = r_i q_i + r_{i+1}$;
2. Если $r_{i+1} \neq 0$, увеличить i на 1 и вернуться к первому шагу;
3. Если на k-ом круге $r_{k+1} = 0$, то $\gcd(a, b) = r_k$.

Для нахождения линейного представления НОД пройдем алгоритм Евклида в обратную сторону:

$$\gcd(a, b) = r_k = r_{k-2}x_{k-2} + r_{k-1}y_{k-2}, \text{ где} x_{k-2} = 1, y_{k-2} = -q_{k-1}$$

. Далее подставим в равенство $r_{k-1} = r_{k-3} - r_{k-2}q_{k-2}$:

$$\gcd(a, b) = r_{k-3}x_{k-3} + r_{k-2}y_{k-3}.$$

Продолжаем далее и получаем:

$$\gcd(a, b) = r_0 x_0 + r_1 y_0 = ax_0 + by_0.$$

iii НОК

Def 83. Пусть $a, b \in R$. Элемент c кольца R называется наименьшим общим кратным элементов a и b, если он делится на a и на b, и делит любое другое общее кратное a и b.

Другими словами, c — НОК, если cR — наиблольший главный идеал, содержащийся в $aR \cap bR$.

Designation. $\operatorname{lcm}(a, b)$ — наименьшее общее кратное.

Lemma 45. *Если R — область главных идеалов, $a, b \in R \setminus \{0\}$, то* $\operatorname{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)}$

Доказательство. Пусть $d = \gcd(a, b)$, $a = a'd$, $b = b'd$. По теореме о линейном представлении НОД существуют $x, y \in R : ax + by = d$. Так как R — область целостности, а $d \neq 0$, можем сократить:

$$a'x + b'y = 1.$$

Если $c \in aR \cap bR$, то $c = ca'x + cb'y \in ba'R + ab'R = a'b'dR$. Следовательно, $aR \cap bR \subseteq a'b'dR$. Обратное включение очевидно. Значит $a'b'd = \frac{ab}{\gcd(a, b)}$. ☐

Вопрос 49 Локализация: уникальное свойство, примеры мультипликативных множества

i Локализация

Def 84. $S \subseteq R$, S — мультипликативное подмножество, если:

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

Def 85. Пусть S — мультипликативное подмножество кольца R. Локализацией кольца R в S называется кольцо $S^{-1}R$ вместе с локализационным гомоморфизмом $\lambda_S : R \to S^{-1}R$, удовлетворяющее следующим свойствам:

(1) для любого $s \in S$ элемент $\lambda_S(s)$ обратим в $S^{-1}R$;

(2) для любого гомоморфизма $\varphi : R \to A$, при котором $\varphi(s) \in A^*$ для всех $s \in S$, существует единственный гомоморфизм $\psi : S^{-1}R \to A : \psi \circ \lambda_S = \varphi$.

Note. Если R —- область целостности, то $\{0\}$ — простой идеал. Локализация в этом идеале будет полем, которое называется полем частных кольца R.

Theorem 40 (Универсальное свойство локализации)**.** *Пусть R — область целостности, $S = R \diagup \{0\}$. Тогда $F = S^{-1}R$ является полем, а гомоморфизм локализации $\lambda_S : R \rightarrowtail$ инъективен. При этом λ_S удовлетворяет следующему универсальному свойству: для любого поля K и мономорфизма $\varphi : R \rightarrowtail K$ существует единственный мономорфизм $\psi : F \rightarrowtail K$ такой, что $\varphi = \psi \circ \lambda_S$.*

ii Примеры

1. Для $s \in R$ положим $\langle s \rangle = \{s^n \mid n \in \mathbb{N}_0\}$. Локализация $\langle s \rangle^{-1}R$ обозначается через R_s и называется главной локализацией в элементе s.

2. Если P — простой идеал R, то $R \diagup S$ — мультипликативное подмножество. Локализация $R_P := (R \diagup P)^{-1}$ называется локализацией кольца R в простом идеале P.

3. S — множество всех элементов R, не являющихся делителями нуля. Тогда $S^{-1}R$ называется полным кольцом частных кольца R.

4. $R = K[x]$, где K — кольцо, S — множество унитарных многочленов.

Вопрос 50 Конструкция локализации

Определим отношение эквивалентности «$\sim$» на множестве $R \times S$:

$$(r_1, s_1) \sim (r_2, s_2) \Longleftrightarrow \exists s \in S : s s_2 r_1 = s s_1 r_2.$$

Проверим, что это отношение эквивалентности:

$\boxed{\text{Рефлексивность}}$ $e s_1 r_1 = e s_1 r_1 \Longrightarrow (r_1, s_1) \sim (r_1, s_1)$

$\boxed{\text{Симметричность}}$ $(r_1, s_1) \sim (r_2, s_2) \Longleftrightarrow \exists s \in S : s s_2 r_1 = s s_1 r_2 \Longleftrightarrow (r_2, s_2) \sim (r_1, s_1)$

$\boxed{\text{Транзитивность}}$ $(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3) \iff \exists s, s' \in S : sr_1s_2 = sr_2s_1 \wedge s'r_2s_3 = s'r_2s_2$. Домножим на $s's_3$ первое и на ss_1 второе:

$$\underbrace{s'ss_2}_{\in S} r_1s_3 = s'sr_2s_1s_3 = \underbrace{ss's_2}_{\in S} r_3s_1.$$

Значит, $(r_1, s_1) \sim (r_3, s_3)$.

Пусть $S^{-1}R = R \times S/\sim$. Класс эквивалентности, содержащий (r, s) обозначается $\frac{r}{s}$.

Определим отображение $\lambda_S : R \to S^{-1}R$ формулой $\lambda_S(r) = \frac{r}{1}$.

Theorem 41. *Пусть S — мультпликативное подмножество кольца R. Определим операции на $S^{-1}R$ так:*

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2} \quad \text{и} \quad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_1r_2 + s_2r_1}{s_1s_2}.$$

Тогда $S^{-1}R$ является локализацией кольца R в мультипликативном подмножестве S с локализационным гомоморфизмом λ_S.

Доказательство. Докажем, что определение операций не зависит от выбора представителей классов эквивалентности. Пусть

$$\frac{r_1'}{s_1'} = \frac{r_1}{s_1} \text{ и } \frac{r_2'}{s_2'} = \frac{r_2}{s_2}.$$

Это значит, что $\exists s, s' \in S :$

$$sr_1s_1' = sr_1's_1 \text{ и } s'r_2s_2' = s'r_2's_2.$$

Перемножим равенства:

$$ss'r_1s_1'r_2s_2' = ss'r_1's_1r_2's_2.$$

Откуда

$$\frac{r_1r_2}{s_1s_2} = \frac{r_1'r_2'}{s_1s_2'}.$$

Далее

$$ss'(r_1s_2 + r_2s_1)s_1's_2' = ss'(r_1s_2s_1's_2' + r_2s_1s_1's_2') = ss'(r_1's_2s_1s_2' + r_2's_1s_1's_2) = ss'(r_1's_2' + r_2's_1')s_1s_2.$$

Значит

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

Теперь проверим, что операции коммутативны, ассоциативны и дистрибутивны:

1. Коммутативность
   (a) Сложение
   $$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2} = \frac{r_2}{s_2} + \frac{r_1}{s_1}.$$
   (b) Умножение
   $$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2} = \frac{r_2}{s_2} \cdot \frac{r_1}{s_1}.$$
2. Ассоциативность
   (a) Сложение
   $$\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) + \frac{r_3}{s_3} = \frac{r_1s_2 + r_2s_1}{s_1s_2} + \frac{r_3}{s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3}$$
   $$\frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right) = \frac{r_1}{s_1} + \frac{r_2s_3 + r_3s_2}{s_2s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3}.$$

(b) Умножение

$$\left(\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}\right)\cdot\frac{r_3}{s_3}=\frac{r_1r_2r_3}{s_1s_2s_3}=\frac{r_1}{s_1}\cdot\left(\frac{r_2}{s_2}\cdot\frac{r_3}{s_3}\right).$$

3. Дистрибутивность

$$\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)\cdot\frac{r_3}{s_3}=\frac{r_1s_2+r_2s_1}{s_1s_2}\cdot\frac{r_3}{s_3}=\frac{r_1r_3s_2+r_2r_3s_1}{s_1s_2s_3}=\frac{r_1r_3}{s_1s_3}+\frac{r_2r_3}{s_2s_3}=\frac{r_1}{s_1}\cdot\frac{r_3}{s_3}+\frac{r_2}{s_2}\cdot\frac{r_3}{s_3}.$$

Нейтральный элемент по сложению: $\frac{0}{1}=\frac{0}{s}$.

Обратный к $\frac{r}{s}$: $\frac{-r}{s}$.

λ_S — гомоморфизм.

Первое свойство локализации: $\lambda_S(s)\cdot\frac{1}{s}=\frac{s}{1}\cdot\frac{1}{s}=\frac{s}{s}=1$.

Пусть $\varphi : R\to A$ — гомоморфизм из второго свойства. Определим $\psi : S^{-1}R\to A$ равенством $\psi(\frac{r}{s})=\varphi(r)\varphi(s)^{-1}$.

Если $\frac{r'}{s'}=\frac{r}{s}$, то $\exists s''\in S : s''r's=s''rs'$ и $\varphi(s'')\varphi(r')\varphi(s)=\varphi(s'')\varphi(r)\varphi(s')$. Домножим на $\varphi(s'')\varphi(s)^{-1}\varphi(s')^{-1}$:

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

Следовательно, определение ψ корректно.

Так как $\varphi(1)=1$, $\varphi=\psi\circ\lambda_S$. Кроме того ψ — гомоморфизм.

Проверим, что ψ задается однозначно. Так как $\varphi=\psi\circ\lambda_S$, $\psi(\frac{r}{1})=\varphi(r)$. Так как ψ — гомоморфизм:

$$\varphi(r)=\psi\left(\frac{r}{1}\right)=\psi\left(\frac{r}{s}\cdot\frac{s}{1}\right)=\psi\left(\frac{r}{s}\right)\cdot\varphi(s).$$

По условию $\varphi(s)$ обратимо, следовательно, $\psi(\frac{r}{s})=\varphi(r)\varphi(s)^{-1}$. Значит, ψ однозначно определено. ☐

Вопрос 51 Поле частных евклидова кольца и разложение на простейшие дроби

Def 86. Пусть R — евклидово кольцо с евклидовой нормой f, F — его поле частных. Простейшей дробью называется элемент $\frac{r}{s^n}\in F$, где $r,s\in R$, s неприводим, и $f(r)<f(s)$.

Statement 26. *F — поле частных R. $a,b,c\in R$, где $\gcd(b,c)$ Дробь $\frac{a}{bc}$ раскладывается в сумму двух дробей со знаменателями b и c.*

Доказательство. По теореме о линейном представлении НОД $\exists x,y\in R : 1=bx+cy$. Из чего следует, что $\frac{a}{bc}=\frac{abx+acy}{bc}=\frac{ax}{c}+\frac{ay}{b}$. ☐

Note. Пусть

$$b=p_1^{k_1}\cdot\ldots\cdot p_m^{k_m},\qquad p_i\in R\text{ — неприводимы.}$$

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

Corollary 9. *Пусть R — кольцо главных идеалов.*

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

Theorem 42. *Любой элемент поля частных F евклидова кольца R раскладывается в сумму элемента из R и простейших дробей.*

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

Индукция по k.

База ($k = 0$):

$$r = pb + x \Longrightarrow \frac{r}{p} = b + \frac{c}{p}.$$

Переход ($k - 1 \to k$): Пусть f — евклидова норма. Разделим r на p с остатком: $r = sp + q, \quad f(q) < f(p)$.

Тогда

$$\frac{r}{p^k} = \frac{s}{p^{k-1}} + \frac{q}{p^k}.$$

Вторая дробь — простейшая, а первая по предположению индукции раскладывается в сумму простейших и элемента из R.

□

Вопрос 52 Определение алгебры над кольцом. Алгебра многочленов и ее универсальное свойство

Designation. R — коммутативное кольцо с единицей.

Def 87. **Многочленом** p **от одной переменной** t **над** R называется конечный набор $(\alpha_0, \ldots \alpha_n)$, записанный в виде $p(t) = \alpha_0 + \alpha_1 t + \ldots + \alpha_n t^n$. При этом **степень многочлена** равна $n = \deg p$.

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

Def 88. Пусть V — векторное пространство над полем F, снабженное операцией умножения $V \times V \to V$. Тогда V является **алгеброй над полем** F, если $\forall x, y, z \in V, \ \alpha, \beta \in F$:

1. $(x + y)z = xz + yz$
2. $x(y + z) = xy + xz$
3. $(\alpha x)(\beta y) = (\alpha\beta)(xy)$

Def 89. $F[t]$ — **множество всех многочленов** от переменной t в поле F. С операциями сложения и умножения является алгеброй над F.

Определим полиномиальную функцию $\tilde{p} : A \to A$ формулой

$$\tilde{p}(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n.$$

Def 90. A– алгебра над F , если A — кольцо и F — модуль и $r(a_1 a_2) = (ra_1)a_2$.

По другому: $\begin{array}{l} \varphi : R \to A \\ \varphi(r) = r \cdot 1_A \end{array}$

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

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

задает на A структуру R- модуля.

Note. В определении A не обязательно является коммутативным.

Def 91. A, B алгебры над R. $\Theta : A \to B$ — 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 92. A — R-алгебра, $a \in A, p \in R[t], \quad p(t) = \alpha_0 \cdot 1 + \ldots + \alpha_n \cdot t^n$.

$$\varepsilon_a(p) = p(a) \coloneqq \alpha_0 + \ldots + \alpha_n a^n.$$

$\varepsilon_a : R[t] \to A$ — гомоморфизм подстановки.

Statement 27 (Универсальное свойство кольца многочленов)**.** *$\forall a \in A$ существует единственный гомоморфизм R-алгебры $\varepsilon : R[t] \to A : t \mapsto a$.*

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

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

☐

Вопрос 53 Многочлены от одной переменной: деление с остатком, теорема Безу, количество корней многочлена

Designation. Далее F — поле.

Theorem 43. *кольцо многочленов $F[t]$ над полем F — евклидово с евклидовой нормой* deg.

Theorem 44 (Безу)**.** *Пусть $\alpha \in F$, $p \in F[t]$.*

1. *Остаток от деления многочлена p на $t - \alpha$ равен $p(\alpha)$.*
2. *Элемент α является корнем многочлена p тогда и только тогда, когда p делится на $t - \alpha$.*
3. *Многочлен степени n не может иметь больше, чем n корней.*

Вопрос 54 Конечная подгруппа мультипликативной группы поля

Theorem 45. *Любая конечная подгруппа мультипликативной группы поля циклическая.*

Доказательство. Пусть F — поле, $G \leqslant F^*$, $|G| = n$.

$\exp G = k \Longrightarrow \forall g \in G : g^k = 1$, то есть все элементы G корни многочлена $t^k - 1 \Longrightarrow |G| \leqslant k$. А он имеет на больше k корней. k делит $|G| \Longrightarrow \exp G = |G|$. Следовательно, G — циклическая. ☐

Theorem 46. *Пусть $t_0, y_0, \ldots t_n, y_n \in F$, причем $t_i \neq t_j$ $\forall i \neq j$. Существует единственный многочлен p степени не выше n, удовлетворяющий условиям $p(t_i) = y_i$ $\forall i \in [0, n]$. Этот многочлен можно найти по формуле*

$$p(t) = \sum_{i=0}^{n} y_i \frac{\prod_{j \neq i}(t - t_j)}{\prod_{j \neq i}(t_i - t_j)}.$$

Доказательство. По теореме Безу условия $p(t_i) = y_i$ равносильны условиям $p \equiv y_i \mod (t - t_i)$. По китайской теореме об остатках существует единственный по модулю $w(t) = \prod\limits_{i=0}^{n} (t - t_i)$ многочлен, удовлетворяющий этим сравнениям.

Единственный многочлен $\deg \leqslant n$ — остаток от деления любого такого многочлена на w. □

Вопрос 55 Функция Эйлера. Теорема Эйлера

Так как $\mathbb{Z}$ — евклидово кольцо, то оно является областью главных идеалов. По лемме **??** любой ненулевой простой идеал является максимальным, значит $\mathbb{Z}/p\mathbb{Z}$ — поле тогда и только тогда, когда $p \in \mathbb{P}$.

Если $n_1, \dots n_t$ — попарно взаимно просты, то имеет место китайская теорема об остатках:

$$\frac{\mathbb{Z}}{n_1 \dots n_t \mathbb{Z}} \cong \frac{\mathbb{Z}}{n_1 \mathbb{Z}} \oplus \dots \frac{\mathbb{Z}}{n_t \mathbb{Z}}.$$

Def 93. Порядок мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^*$ обозначается $\varphi(n)$. Функция $\varphi : \mathbb{N} \to \mathbb{N}$ называется функцией Эйлера.

Lemma 46. *Образ числа* $n \in \mathbb{Z}$ *обратим в кольце* $\mathbb{Z}/n\mathbb{Z}$ *тогда и только тогда, когда* $\gcd(n, m) = 1$. *Таким образом,* $\varphi(n)$ *равна количеству чисел от* 0 *до* n*, взаимно простых с* n*.*

Доказательство. Пусть $\overline{m}$ — образ m в $\mathbb{Z}/n\mathbb{Z}$. $\overline{m}$ обратим тогда и только тогда, когда $\exists \overline{x} \in \mathbb{Z}/n\mathbb{Z} : \overline{m} \cdot \overline{z} = 1$. Если $x \in \mathbb{Z}$ — прообраз $\overline{x}$, то вместо $\overline{m} \cdot \overline{x} = 1$ можем записать $mx \in 1 + n\mathbb{Z}$, то есть идеалы $m\mathbb{Z}$ и $n\mathbb{Z}$ взаимно просты. По следствию **??** $\gcd(m, n) = 1$. □

Lemma 47. *Если кольцо* R *с единицей (не обязательно коммутативное) является прямой суммой колец* $R_1 \oplus \dots R_k$*, то* $\mathbb{R}^* \cong R_1^* \times \dots R_k^*$. *Если* R^* *конечна, то* $|R^*| = |R_1^*| \cdot \dots |R_k^*|$.

Theorem 47.

- *Если* $\gcd(a, b) = 1$*, то* $\varphi(ab) = \varphi(a)\varphi(b)$.
- *Если* $p \in \mathbb{P}$, $k \in \mathbb{N}$*, то* $\varphi(p^k) = p^k - p^{k-1}$.
- *Пусть* $p_1, \dots p_l$ *— различные простые числа,* $k_1, \dots k_l \in \mathbb{N}$, $n = \prod_{i=1}^{l} p_i^{k_i}$. *Тогда*

$$\varphi(n) = \prod_{i=1}^{l} \left(p_i^{k_i} - p_i^{k_i - 1} \right) = n \prod_{i=1}^{l} \frac{p_i - 1}{p_i}.$$

Theorem 48 (теорема Эйлера). *Если* $\gcd(a, n) = 1$*, то* $a^{\varphi(n)} \equiv 1 \mod n$.

Доказательство. Так как a взаимно просто с n, $\overline{a}$ обратим в $\mathbb{Z}/n\mathbb{Z}$ и принадлежит $(\mathbb{Z}/n\mathbb{Z})*$. $\overline{a}$ порождает в $\mathbb{Z}/n\mathbb{Z}$ циклическую подгруппу, порядок которой делит $\varphi(n)$ по теореме Лагранжа.

$$\overline{a}^{\varphi(n)} = \overline{1} \Longrightarrow a^{\varphi(n)} \equiv 1 \mod n1 \mod n1 \mod n.$$

□

Вопрос 56 Экспонента группы $(\mathbb{Z}/p^k\mathbb{Z})^*$ при $p \neq 2$

Theorem 49. *Группа* $(\mathbb{Z}/p^k\mathbb{Z})^*$ *циклическая для любого* $p \neq 2$, *и* $\exp(\mathbb{Z}/p^k\mathbb{Z})^* \,\vdots\, (p-1)p^{k^{p-1}}$.

Доказательство. Пусть $p \in \mathbb{P} \wedge p \neq 2$. Поле $\mathbb{Z}/p\mathbb{Z}$ — факторкольцо кольца $\mathbb{Z}/p^k\mathbb{Z}$ по идеалу, порожденному p.

Пусть $\pi : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ — каноническая проекция. $f : (\mathbb{Z}/p^k\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ — гомоморфизм мультипликативных групп, который сюрьективен, так как все числа от 1 до $p-1$ взаимно просты с p^k и, следовательно, их классы вычетов обратимы.

По теореме **??** существует элемент $a \in \mathbb{Z}/p\mathbb{Z}$ порядка $p-1$. Тогда порядок его прообраза в $(\mathbb{Z}/p^k\mathbb{Z})^*$ делится на $p-1$. Следовательно, экспонента группы $(\mathbb{Z}/p^k\mathbb{Z})^*$ делится на $p-1$.

Докажем, что при $k \geqslant 2$ экспонента делится на p^{k-1}. По индукции докажем, что элемент $1+p$ имеет порядок p^{k-1}в этой группе.

База ($k=1$): очевидно.

Переход ($k \geqslant 2$): По индукционному предположению $(1+p)^{p^{k-2}} = 1 + p^{k-1}x$, где x не делится на p.

$$(1+p)^{p^{k-1}} = (1+p^{k-1}x)^p = 1 + p \cdot p^{k-1}x + \sum_{i=2}^{p} \binom{p}{i} p^{i(k-1)} x^i.$$

Так как $\binom{p}{i} \,\vdots\, p$, то каждое слагаемое суммы делится на $p^{1+2(k-1)} = p^{k+1}p^{k-2}$. Так как $p \geqslant 2$, сумма равна $p^{k+1}z$, а $(1+p)^{p^{k-1}} = 1 + p^k y$, где $y = x + pz$ не делится на p.

Таким образом, порядок элемента $1+p$ в группе $(\mathbb{Z}/p^k\mathbb{Z})^*$ делит p^{k-1}. По предположению индукции $1+p$ имеет порядок p^{k-1}, также y не делит p, следовательно, порядок $1+p$ равен p^{k-1}.

□

Вопрос 57 Экспонента группы $(\mathbb{Z}/2^k\mathbb{Z})^*$. Теорема Кармайкла

Theorem 50 (Кармайкла)**.** $n = 2^k \cdot p_1^{k_1} \ldots p_n^{k_n}$.

- *Если* $k \geqslant 3$,
$$\exp(\mathbb{Z}/n\mathbb{Z})^* = \operatorname{lcm}_{i, p_i \neq 2} \left(2^{k-2},\ p_i^{k_i} - p_i^{k_i - 1}\right),$$
- *иначе*
$$\exp(\mathbb{Z}/n\mathbb{Z})^* = \operatorname{lcm}_i \left(p_i^{k_i} - p_i^{k^i - 1}\right).$$

Доказательство. По теореме Эйлера экспонента группы $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$ делит $(p_i^{k_i} = p_i^{k_i-1}$. Кроме того

$$\exp(\mathbb{Z}/n\mathbb{Z})^* = \operatorname{lcm}_i \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*\right).$$

Если $k \geqslant 2$, можно доказать, что $\exp(\mathbb{Z}/2^k\mathbb{Z})^* = 2^{k-2}$. Докажем, что $(1+4z)2^{k-2} = 1 + 2^k y$, где y имеет ту же четность, что и z. Индукция по k.

База ($k=2$).

Переход ($k \geqslant 3$). По индукционному предположению $(1+4z)^{2^{k-3}} = 1 + 2^{k-1}x$, где $x \equiv z \mod 2$.

$$(1+4z)^{2^{k-2}} = (1+2^{k-1}x)^x)^2 = 1 + 2 \cdot 2^{k-1}x + 2^{2k-2}x^2 = 1 + 2^k(x + 2^{k-2}x^2).$$

Так как $k \geqslant 3$, $y = x + 2^{k-2}x^2 \equiv x \equiv z \mod 2$. Если z нечетно, порядок $1+4z$ в группе $(\mathbb{Z}/2^k\mathbb{Z})^*$ равен равен $k-2$.

С другой стороны, при любом t имеем $(1+2t)^2 = 1+4z$, где $z = t + t^2 \,\vdots\, 2$. Поэтому (так как $y \,\vdots\, 2$)

$$(1+2t)^{2^{k-2}} = (1+4z)^{2^{k-3}} = 1 + 2^{k-1}y \equiv 1 \mod 2^k.$$

Следовательно, порядок любого элемента группы $(\mathbb{Z}/2^k\mathbb{Z})^*$ делит 2^{k-2}.

Из этого следует уточнение при $k \geqslant 3$. □

Вопрос 58 Интерполяция по Лагранжу и связь ее с КТО

Theorem 51. *Пусть* $t_0, y_0, \dots t_n, y_n \in F$, *причем* $t_i \neq t_j$ $\forall i \neq j$. *Существует единственный многочлен* p *степени не выше* n, *удовлетворяющий условиям* $p(t_i) = y_i$ $\forall i \in [0, n]$. *Этот многочлен можно найти по формуле*

$$p(t) = \sum_{i=0}^{n} y_i \frac{\prod_{j\neq i}(t - t_j)}{\prod_{j\neq i}(t_i - t_j)}.$$

Доказательство. По теореме Безу условия $p(t_i) = y_i$ равносильны условиям $p \equiv y_i \mod (t - t_i)$. По китайской теореме об остатках существует единственный по модулю $w(t) = \prod\limits_{i=0}^{n}(t - t_i)$ многочлен, удовлетворяющий этим сравнениям.

Единственный многочлен $\deg \leqslant n$ — остаток от деления любого такого многочлена на w. □

Итерационный способ. На k-ом шаге строится многочлен степени $\leqslant k-1$, удовлетворяющий первым k условиям.

- На первом шаге $p_0(t) = y_0$.
- Пусть уже построен p_k, удовлетворяющий условиям $\deg p_k \leqslant k-1$ и $p_k(t_i) = y_i \quad \forall i \in [0, k-1]$.

$$p_{k+1}(t) = p_k(t) + \lambda(t - t_0) \cdot \ldots (t - t_{k-1}).$$

λ можно найти из условия $p_{k+1}(t_k) = y_k$, так как первые k уже выполнены.

□

Вопрос 59 Формальная производная и ее свойства

Def 94. Пусть R — коммутативное кольцо с единицей. Формальной производной многочлена $p(t) = a_n t^n + \ldots + a_1 t + a_0 \in R[t]$ называется многочлен $p'(t) = a_n n t^{n-1} + \ldots a_1$.

Property.

1. $(\alpha v)' = \alpha v'$
2. $(u+v)' = u' + v'$
3. $(uv)' = u'v + v'u$
4. $(f(g(t)))' = f'(g(t)) \cdot g'(t)$

Вопрос 60 Кратность корня и ее поведение при дифференцировании

Def 95. Число $\alpha \in F$ имеет кратность k в многочлене $p \in F[t]$, если k — наибольшее натуральное число, для которого p делится $(t-\alpha)^k$.

Используя теорему Безу, можно переформулировать это определение: α имеет кратность k в p, если $p(t) = (t-\alpha)^k g(x), \quad g(\alpha) \neq 0$.

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

Theorem 52. *Пусть α — корень многочлена p кратности k. Если $k \neq 0$ в поле F, то кратность α в p' равна $k-1$.*

Доказательство. По условию $p(t) = (t-\alpha)^k g(t)$. Возьмем производную

$$\big((t-\alpha)^k g(t)\big)' = k(t-\alpha)^{k-1} g(t) + (t-\alpha)^k g'(t) = (t-\alpha)^{k-1}(kg(t) + (t-\alpha)g'(t)).$$

Второй сомножитель в точке α не равен нулю, следовательно, если $k \neq 0$, кратность α уменьшилась на один, так как $kg(\alpha) + (\alpha-\alpha)f'(\alpha) \neq 0$. ☐

Theorem 53 (о рациональных корнях многочлена, без доказательства)**.** *Пусть $p(t) = a_n t^n + \ldots + a_0$ — многочлен с целыми коэффициентами. Тогда рациональными корнями p могут быть только числа вида $\frac{c}{d}$, где $a_0 \,\vdots\, c,\ a_n \,\vdots\, d$.*