~~MicroCup evolution~~ ~~Игорь Журавлёв~~

~~pavy76@mail.ru~~

C

ГРУППЫ. КОМБИНАТОРИКА.

группы преобразований

Опр. (абстрактной группы) группа – множество с заданной бинарной операцией (• – умножение), удовлетворяющей аксиомам

а) $\forall a, b, c \in G: (ab)c = a(bc)$

б) $\exists$ие единицы $\exists e \in G \ \forall a \in G \quad a \cdot e = e \cdot a = a$

в) $\forall a \in G \ \exists a^{-1} \in G \mid a \cdot a^{-1} = a^{-1} \cdot a = e$

Опр: преобразование мн-ва X – это взаимноодн. отобр $\overrightarrow{X \text{ на } X}$

пример: тожд. преобр. (единичное) преобр.

$$e = e_X \qquad x \mapsto x \quad \forall x \in X$$

• для $\forall$ преобр $f: X \to X \ \exists$ обратное:

$$f: x \to y \Rightarrow f^{-1}: y \to x$$

f^{-1} – преобразование т.к. $\begin{matrix} x_1 \xrightarrow{f} y_1 \\ \ne \quad f \quad \\ x_2 \to y_2 \end{matrix} \not\Rightarrow$ и т.д.

• композиция преобр X – снова преобр X

$$X \xrightarrow{f} X \xrightarrow{g} X \qquad (gf)(x) = g(f(x))$$

$$\begin{matrix} x_1 & \longrightarrow & y_1 & \longrightarrow & z_1 \\ \ne & f & \ne & g & \ne \\ x_2 & \longrightarrow & y_2 & \longrightarrow & z_2 \end{matrix}$$

Опр: (группа преобр)
множество Γ преобр. мн-ва X образует гр. преобр, если

1 $\quad e_X \in G$

2 $\quad f \in G \Rightarrow f^{-1} \in G$

3 $\quad f$ и $g \in G \Rightarrow f \circ g \in G$

ТЕОРЕМА: Гр. преобразований явл-я абстрактной гр. от

доказательство: $\exists (G; \circ)$ – гр. преобр X, проверим акс группы:

1) ассоц.? $(f, g) h = f(gh)$: возьмем x

$$\left.\begin{matrix} ((fg)h)x = (fg)(h(x)) = f(g(h(x))) \\ (f(gh))x = f((gh)x) = f(g(h(x))) \end{matrix}\right] \Rightarrow \text{выполн}$$

2) $e = e_X$: (тожд. отобр)

$(f(e))(x) = f(e(x)) = f(x)$, $\forall x$

$(ef)(x) = e(f(x)) = f(x)$, $\forall x$

$\Rightarrow fe = ef = f$.

3) $ff^{-1} = e_X$, аналогично $f^{-1}f = e_X$

ч.т.д.

примеры:

① гр. всех преобр $X \to S(X)$, X-бесконечно $\Rightarrow$ $S(X)$ - очень большая группа

Если $|X| = n < \infty$, то $S(X) = S_n(X)$ - группа подстановок (перест.) n-элем мн-ва

$|S_n| = n!$

② пусть V - вект. пр-во над K $\Rightarrow$ след. мн-ва образуют группы преобр.

$GL(V)$ = {все обратимые лин операторы на V}

~сохр л.н. векторов.

$SL(V)$ = {все лин опер. с опр '1' ($\det = 1$)}

~если $V = \mathbb{R}^n$ - евкл. пр-во $\Rightarrow$ эти преобр сохр объем у тел.

$O(V)$ = {все орт. операторы на евкл. пр-ве V}

~сохр. длин, углы, ...

$U(V)$ = {все унит. операт. на эрм. пр-ве V}

~сохр. эрмит. метрика

$GA(V)$ = {все обратимые аффинные преобр пр-ва V}

$f(x) = Ax + b$; A-лин, $\det B \neq 0$, $b \in V$

$Is(V)$ = {все движ изометрии евкл. пр-ва V}

$f(x) = Ax + b$; A-орт. оператор

для GA: $f(x) = Ax + b$
$$\left(\begin{array}{ccc|c} & A & & b \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

Упр: проверить, что пример (2-1) - группы

ГРУППЫ ПОДСТАНОВОК - РАЗЛОЖЕНИЯ НА ЦИКЛЫ

→ Пусть $X = \{1, 2, \dots n\}$, тогда подстановка на X записывается 2мя строками

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \quad \pi: i_k \to j_k \ \forall k$$

запись неоднозначна $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$ $n!$ записей

→ тожд подст.

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

→ обратная подст. $\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}^{-1} = \begin{pmatrix} j_1 & \dots & j_n \\ i_1 & \dots & i_n \end{pmatrix}$

→ пример умножения подст.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$(g \quad (f(x)))$

умножение некоммутативно!

$$f(g(x)) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Опр: для подстановки $\pi \in S_n$ обозн.

$F_\pi = \{i \in X \mid \pi(i) = i\}$

$T_\pi = \{i \in X \mid \pi(i) \neq i\}$

мн-ва неподвижных и перемещаемых элементов из X

(fix, transformation)

ясно, что $\begin{cases} F_\pi \cap T_\pi = \varnothing \\ F_\pi \cup T_\pi = X \end{cases}$

Опр: подстановка σ из S_n - цикл длины s если множество перемещаемых символов T_σ допускает нумерацию

$T_\sigma = \{i_1, i_2, \dots, i_s\}$, такую что под действ. σ

$i_1 \to i_2 \quad i_2 \to i_3 \dots \quad i_s \to i_1$

краткая запись цикла $\sigma = (i_1 i_2 \dots i_s)$ - s записей.

Опр: подстановки наз-ся независимыми, если они не имеют общих перемещ. символов

$T_\sigma \cap T_\pi = \varnothing$ (или $T_\sigma \subset F_\pi$)

ЛЕММА. Независимые подстановки коммутируют.

Доказательство: Пусть $T_\sigma \cap T_\pi = \varnothing$

$$\sigma(\pi(x)) = \begin{cases} i, \text{ если } i \notin T_\sigma \text{ и } T_\pi \\ \pi(i), \text{ если } i \in T_\pi \\ \sigma(i), \text{ если } i \in T_\sigma \end{cases}$$

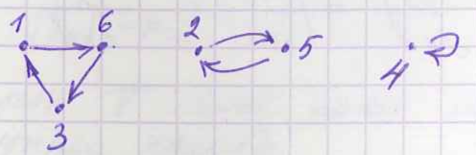
отсюда $\pi \circ \sigma = \sigma \circ \pi$

ч.т.д.

ТЕОРЕМА: всякая нетожд. подст. единств. способом разлагается в пр-е независ. циклов

пример:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25)(4)$$



доказат-во: 1) ∃ие: пусть $\pi \in S_n$, $\pi \neq \varepsilon$, тогда

$$\exists\, i_1 \in X \mid i_2 = \pi(i_1) \neq i_1$$

продолжим. X-конечен =>

$$\underset{}{i_1} \xrightarrow{\pi} \underset{\neq i_1}{i_2} \xrightarrow{\pi} \underset{\neq i_1,\ \neq i_2}{i_3} \xrightarrow{\pi} \dots \to \underset{\neq i_1, i_2 \dots i_{s-1}}{i_s} \xrightarrow{\pi} i_k, \text{ где } \underline{k \leq s}$$

если $k \neq 1$, то это противоречит взаимнооднозн. отобр.

$\pi: i_{k-1} \to i_k$
$i_s \to i_k$

=> $k=1$, обозначим ц-л $\sigma_1 = (i_1 i_2 \dots i_s)$

Пусть $\pi' = \sigma^{-1}\pi$ =>

$\pi'(i_k) = i_k$ $(1 \leq k \leq s)$ — наш цикл!

$T_{\pi'} = T_\pi \setminus \{i_1 \dots i_s\}$, далее индукция по числу перемещаемых символов

$$\pi' = \underbrace{\sigma_2 \sigma_3 \dots \sigma_q}_{\text{попарно нез. цикл}} = \sigma_1^{-1}\pi$$

$\pi = \underbrace{\sigma_1 \sigma_2 \dots \sigma_q}$ — требуемое разложение

2) единств. следует из леммы

Опр: Две подст. π и π' наз-ся подобными или сопряженными в S_n, если ∃ подст. $\sigma \in S_n$:

$$\pi' = \sigma \pi \sigma^{-1}$$

ТЕОРЕМА: 2 подст. сопряжены в S_n <=> они имеют одинаковое цикловое строение т.е одинак кол-во независ. циклов каждой длины.

доказательство:

(⇐) $\pi = (i_1 i_2 \dots i_s)(j_1 j_2 \dots j_t)(\dots)\dots(\,)(\,)\dots$ (1)

$\pi' = (i_1' i_2' \dots i_s')(j_1' j_2' \dots j_t')(\ )\dots(\,)(\,)\dots$ (2)

положим

$$\sigma = \begin{pmatrix} i_1 i_2 \dots i_s, j_1 j_2 \dots j_t \dots \\ i_1' i_2' \dots i_s', j_1' j_2' \dots j_t' \dots \end{pmatrix} \quad (3)$$

тогда $\pi' = \sigma \pi \sigma^{-1}$

$$\begin{tikzcd} i_1 \arrow[r, "\pi"] \arrow[d, "\sigma"'] & i_2 \arrow[d, "\sigma"] \\ i_1' \arrow[r, "\pi'"'] & i_2' \end{tikzcd}$$

(⇒) (1) и (3) ⇒ $\pi' = \underbrace{\sigma \pi \sigma^{-1}}$ (2)

ч.т.д.

Следствие 1: Число классов сопрян. подстановок в S_n равно числу разбиений (монотонных) n в сумму натуральных чисел.

$$n = n_1 + n_2 + \dots n_q, \quad n_1 \geq n_2 \geq \dots \geq n_q \geq 1$$

РАЗЛОЖЕНИЕ НА ТРАНСПОЗИЦИИ

Опр: транспозиция — цикл длины 2

$T = (ij)$ $i \neq j$

Опр: Декремент подстанов. — разность между числом перемещаемых символов и числом независимых циклов длины ≥2 в каноническом разложении (по циклам

$\pi = (123)(4567)(8)$ $d(\pi) = 7 - 2 = 5 = 8 - 3$

Опр: ~~Длина~~ Знак подстановки — пр-е знаков перестановок верх и нижней строки в записи подстановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \operatorname{sgn}\pi = \operatorname{sgn}(1234) \cdot \underset{}{\overset{\text{3 инверсии}}{\operatorname{sgn}(1432)}} = (+1)\cdot(-1) = \underline{-1}$$

ТЕОРЕМА 1) Всякая подстановка разл. в про-ие транспозиций, число которых равно декременту подстановки

2) Знак пр-ия подстановок равен про-ию знаков сомножителей

3) Если под-ка $\pi = \tau_1 \tau_2 \dots \tau_k$; τ-транспозиц.

$\Rightarrow sgn\, \pi = (-1)^k$

доказательство:

1) Достаточно для циклов надо ?

$(i_1 i_2 \dots i_{s-1} i_s) \overset{?}{=} (i_1 i_2)(i_2 i_3)(i_3 i_4) \dots (i_{s-1} i_s) \cancel{(i_s i_1)}$

$\pi = \sigma_1 \sigma_2 \dots \sigma_q \quad \ell(\sigma_i) = s_i \Rightarrow$

$\Rightarrow$ кол-во транспоз. $\sum_{s=1}^{q}(s_i - 1) = \sum_{i=1}^{q} s_i - q = d(\pi)$

2) $\underbrace{\begin{pmatrix} j_1 j_2 & \dots & j_n \\ k_1 k_2 & \dots & k_n \end{pmatrix}}_{\sigma} \underbrace{\begin{pmatrix} i_1 i_2 & \dots & i_n \\ j_1 j_2 & \dots & j_n \end{pmatrix}}_{\pi} = \underbrace{\begin{pmatrix} i_1 i_2 & \dots & i_n \\ k_1 k_2 & \dots & k_n \end{pmatrix}}_{\sigma \cdot \pi}$

отсюда вычисляем знак

$sgn\,(k_1 k_2 \dots k_n) \cdot sgn\,(j_1 \dots j_n)^2 \cdot sgn\,(i_1 i_2 \dots i_n) =$

$= sgn\,(k_1 \dots k_n) \cdot sgn\,(i_1 \dots i_n)$

3) ввиду 2: $sgn\,(\tau_1 \dots \tau_n) = \prod_{i=1}^{n} (sgn\, \tau_i) = (-1)^k$

ч.т.д.

следствие 1: четность под-ки = четность её декремента

следствие 2: при $n \geq 2$ все четные подст. A_n обр. группу относит. умнож. подст. с порядком $\frac{n!}{2}$

док-во:

$\pi \in A_n$ $\quad \pi \leftrightarrow \tau\pi$ $\quad \rightarrow$ биекция $\Rightarrow$ столько четн.
$\tau = (1, 2)$ $\quad$ четн $\leftrightarrow$ нечетн $\quad$ столько нечетн

ПОДГРУППЫ

Опр: пусть G-группа $A, B \subset G$ -под-ва

обозначим: $AB = \{a, b \mid a \in A, b \in B\}$

$A^{-1} = \{a^{-1} \mid a \in A\}$

под-во H гр G - подгр G, если:

1) $e \in H$
2) $H \times H \in H$ замкнутость относит $\times$ и обращ.
3) $H^{-1} \in H$

заметим
$e \in H$, $HH = H$, $H^{-1} = H$ $\quad$ Обозн. $H \leq G$

доказ-во: 3) $a = (a^{-1})^{-1}$, $a \in H$ и т.д.

2) $a = ea \Rightarrow H = H$

пример: $A_n \leq S_n$

ТЕОРЕМА 1) "$\cap$" $\forall$ семейства подгрупп - подгруппа

2) Если $H \leq G$, $a \in G \Rightarrow aHa^{-1} = \{aba^{-1} \mid b \in H\}$ - подгруппа G - сопряженная с H

3) Если $A \subset H$ $A \neq \emptyset$

$\langle A \rangle := \{a_1^{\varepsilon_1}, a_2^{\varepsilon_2} \dots a_k^{\varepsilon_k} \mid a_i \in A,\ \varepsilon_i = \pm 1,\ k \geq 1\}$

наим. подгруппа, содержащая A

доказательство: 1) $\exists$ $H_i \leq G$ $\quad i \in I$,

$H := \bigcap_i H_i$, проверим замкн. H отн $(1, \times, $ обр.$)$

а) $e \in \forall H_i \Rightarrow e \in H$
б) если $a, b \in H \Rightarrow a, b \in H_i \ \forall i \Rightarrow$

$\Rightarrow ab, a^{-1} \in H_i \ \forall i \Rightarrow ab, a^{-1} \in H = \bigcap_i H_i$

2) $e = aea^{-1} \in aHa^{-1}$

$aha^{-1}, a f a^{-1} \in H \Rightarrow aha^{-1} \cdot a f \cdot a^{-1} = a \underbrace{hf}\, a^{-1} \Rightarrow \in H$

$(aba^{-1})^{-1} = ab^{-1}a^{-1} \in H$

3) $e = a \cdot a^{-1} \in \langle A \rangle$

$a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} \cdot b_1^{\sigma_1} \dots b_e^{\sigma_e}$

почему наименьшая, содерж. A

$a = aa^{-1}a \in \langle A\rangle \Rightarrow A \in \langle A\rangle$

если $H \in G \Rightarrow H \ni A$

то тогда $H \supset \langle A\rangle$!

ч.т.д.

Опр: Если $\langle A\rangle = G$, то A наз-ся мн-ом, порождающим элементы.

$\langle A\rangle$ — подгруппа, порожд. мн-ом A.

ПРИМЕР. $S_n = \langle T\rangle$ T-мн-во всех транспозиций

РАЗБИЕНИЕ НА СМЕЖНЫЕ КЛАССЫ

Опр: Пусть H — подгруппа G, тогда мн-во

$aH := \{a\cdot h \mid h\in H\}$, левый

$Ha := \{ha \mid h \in H\}$ правый.

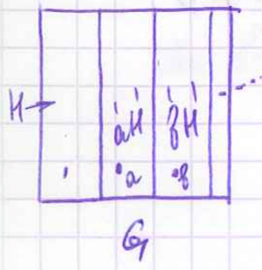
называются лев/правым смежным классом H с предст. a

$a \in aH$ и $a \in Ha$ $(a \to ae \Leftrightarrow ea)$

ТЕОРЕМА. 1) левые (правые) группы дают разбиение группы

2) $\forall$ 2 левых (правых) класса равномощны

3) Число левых кл. = число пр. кл. = <u>индекс</u> подгр. H в G и обозн. $|G:H|$



доказательство:

1) введем на G отн. эквив. смежности по подгр H

$a \sim b \Leftrightarrow a^{-1}b \in H$

это — эквивалентность

1) $a\sim a$ т.к. $a^{-1}a = e \in H$

2) $a \sim b \Rightarrow b\sim a$ т.к. $b^{-1}a = \underset{H}{(a^{-1}\cdot b)^{-1}} \in H$

3) $a\sim b,\ b\sim c \Rightarrow a \sim c$

т.к. $a^{-1}c = a^{-1}b\cdot b^{-1}c \in H$

Класс эквивал. содерж. эл-та:

$x: a\sim x \Leftrightarrow a^{-1}x = h \in H \Leftrightarrow x = a\cdot h \in H$

~ для правых классов — аналогично

$a\sim b \Leftrightarrow ab^{-1} \in H$ и т.д.

2) соотв. $h \leftrightarrow ah$ — биекция: если $ah_1 = ah_2 \mid \cdot a^{-1} \Rightarrow h_1 = h_2$

$\Rightarrow |H| = |aH|$

аналогично $|Ha| = |aH|$

3) Соотв. $x \to x^{-1}$ — взаимнооднозн. $\Rightarrow$ вз-одн. соот.

$aH \leftrightarrow (a\cdot H)^{-1} = H^{-1}a^{-1} \underset{H=H^{-1}}{=} Ha^{-1}$

следствие 1 (Т Лагранжа)

для конечн. гр G и $\forall$ её подгр H

$|G| = |H|\cdot|G:H|$

в частности $|H|$ нацело делит $|G|$

пор подгр. — порядок гр.

ЦИКЛИЧЕСКИЕ ГРУППЫ, ПОРЯДОК ЭЛ-ТА.

Опр: Натур. число n называется порядком элемента g для G, если $g^n = e$, $g^r \ne e$ при $0<r<n$

Обозн. $n = \operatorname{ord} g$. Если $g^n \ne e\ \forall n\in\mathbb{N} \Rightarrow \operatorname{ord} g := \infty$

ЛЕММА 1) Если $\operatorname{ord} g = n$, то $g^k = e \Leftrightarrow n \mid k$

2) $g^k = g^l \Leftrightarrow k \equiv l \pmod n$

3) $\operatorname{ord} g^k = \frac{n}{НОД(n,k)}$

$\}$ $\operatorname{ord} g = n$

доказательство:

1) Пусть $k = n\cdot q + r$, $0 \le r < n$

$g^k = (g^n)^q\cdot g^r = e^q\cdot g^r = g^r = e \Leftrightarrow r = 0 \Leftrightarrow n\mid k$

2) $g^k = g^l \Leftrightarrow g^{k-l} = e$ (см 1) $n \mid (k-l) \Leftrightarrow k \equiv l \pmod n$

3) Пусть $d = НОД(n,k) \Rightarrow n = n'd$, $k = k'\cdot d$; $n' \perp k'$ (взаимнопрост)

отсюда: $(g^k)^l = e \overset{1}{\Leftrightarrow} n \mid kl \Leftrightarrow$

$\underbrace{n'}d \mid \underbrace{k'}d \cdot \ell \Rightarrow n' \mid k' \cdot \ell \underset{n' \perp k'}{\Leftrightarrow} n' \mid \ell$

$\Rightarrow \operatorname{ord} g^k = n' = \frac{n}{d} = \frac{n}{\text{НОД}(n,k)}$

лемма доказана.

~~ТЕОРЕМА:~~

Опр: группа, порожд-ая 1одним эл-ом – циклическая

$G = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$

~~$\forall$ цикл~~

ТЕОРЕМА: $\forall$ цикл. гр-па изоморфна

либо $(\mathbb{Z}, +)$, либо $(\mathbb{Z}_n; +)$

доказательство:

1. пусть $G = \langle g \rangle$ и пусть $\operatorname{ord} g = \infty \Rightarrow$
$\Rightarrow g^k \neq e \ \forall k \neq 0$, тогда $g^k \leftrightarrow k$ – изоморфизм между G и $(\mathbb{Z}, +)$
2. если $G = \langle g \rangle$ и $\operatorname{ord} g = n < \infty$, то
$g^k \leftrightarrow k \pmod n$ – взаимнооднозн. – изоморфизм между G и $(\mathbb{Z}_n, +)$; $0 \le k, \ell < n$

следствие (тп 1 и лагр.-на)

1) всякая гр. простого порядка явл. циклической

доказательство:

$\exists$ $|G| = p$ – прост.

$|G| > 1$ $\exists g \in G$, $g \neq e$, пусть $H := \langle g \rangle$, тогда $H \le G$

$|H| > 1$, т.к $H \ni g, e$ (как minimum), но Тп Лагранжа порядок $|H| \mid |G|$ (делит) $= p$ – пр. $\Rightarrow$

$\Rightarrow |H| = p = |G|$, $H \subset G \Rightarrow$

$\Rightarrow H = G \Rightarrow G = \langle g \rangle$

следствие 2 Пусть $|G| = n < \infty \Rightarrow g^n = e \ \forall g \in G$

доказательство: $H = \langle g \rangle \Rightarrow$

$H = \{ g, g^2 \ldots g^k = e \mid k - \min \}$

$k = \operatorname{ord} g = |H|$, но Тп Лагранжа $|H| \mid |G| \Rightarrow$

$\Rightarrow n = k \cdot \ell$, где $\ell \in \mathbb{N} \Rightarrow g^n = (g^k)^\ell = e^\ell = e$

следствие 3. [Малая Тп Ферма]

Если p-пр. число и $a \in \mathbb{N}$, $p \nmid a$ (не делит), то

$a^{p-1} \equiv 1 \pmod p$

доказательство

Т.к p-прост. число, то $\mathbb{Z}_p$-поле, его мультипл. группа (по умн. $\to \mathbb{Z}_p^*$)

$\mathbb{Z}_p^* = \{ a \in \mathbb{Z}_p \mid a \not\equiv 0 \pmod p \} \Rightarrow$

$\Rightarrow |\mathbb{Z}_p^*| = p - 1 \Rightarrow$ но сл. 2 для $\forall \tilde{a} \in \mathbb{Z}_p^*$:

$(\tilde{a})^{p-1} = e$, т.е

$a^{p-1} \equiv 1 \pmod p$

следствие 4 [Формула Эйлера]

$\exists$ $n \in \mathbb{N}$ и $\varphi(n)$ – кол-во нат. чисел "$\le n$" и "$\perp n$" "φ-функция Эйлера". Тогда $a \perp n$, то

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

доказательство:

$\exists$ $\mathbb{Z}_n$ – к. вычет. по mod n, $\mathbb{Z}_n^*$ – группа его обратимых элементов, тогда утв-ся, что

$|\mathbb{Z}_n^*| = \varphi(n)$;

ур-ие $ax \equiv 1 \pmod n$ – разрешимо в $\mathbb{Z} \Leftrightarrow$

$n \mid (ax - 1) \Leftrightarrow \exists y \ \ ax - 1 = n \cdot y \Leftrightarrow$

$\Leftrightarrow \begin{cases} \exists x, y \in \mathbb{Z}: \\ ax - n \cdot y = 1 \end{cases}$ – лин. диоф ур-ие (x, y – неиз.) – разрешимо в кольце $\mathbb{Z} \Leftrightarrow$

$\Leftrightarrow \text{НОД}(a, n) \mid 1 \Rightarrow \text{НОД}(a, n) = \pm 1 \Rightarrow a \perp n$

можно считать, что $a \le n$, $a \ge 0$

По след. 2: $\bar{z} \in \mathbb{Z}_n^* \Rightarrow (\bar{z})^{\varphi(n)} = \bar{1} \Leftrightarrow$

$\Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod n$

ДЕЙСТВИЕ ГРУППЫ НА МНОЖЕСТВО

Опр: гр. G действует на X, если задано отобр. $G \times X \to X$,

$(g,x) \mapsto gx \in X$, со св-ми:

1) $(gh)x = g(h(x))$

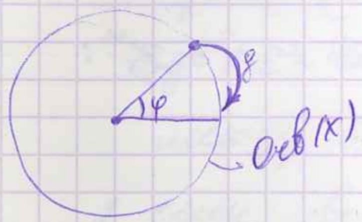
2) $ex = x$ $\quad \forall g,h \in G \quad \forall x \in X$

пример: гр. преобр. X дейст. на X

$(g,x) \mapsto gx$

мн-во $Orb(x) = \{gx \mid g \in G\}$ наз-ся G орбитой эл-та x

мн-во $Stab(x) = \{g \in G \mid gx = x\}$ наз-ся стабилизатор x



пример: 1) $X = G$, левое регулярн. дейст. гр G

$(g,x) \to g \cdot x$

2) $X = G$, правое рег. дейст.

$(g,x) \to x \cdot g^{-1}$

$(gh)x = x(gh)^{-1} = xh^{-1}g^{-1} = g \cdot (xh^{-1}) = g(h \cdot x)$

3) действие G на G сопряжением

$(g,x) \mapsto gxg^{-1}$

Упр. Найти орбиты (x) $Orb(x)$ и $Stab(x)$ при 1-3

ТЕОРЕМА (о мощности орбиты)

Пусть $G:X$ (g на x), тогда

1) G-орбиты в X разбивают X

2) Stabилизаторы точек одной орбиты сопряжены в гр G и имеют один порядок

3) мощность орбиты = индексу стабилизатора точки орбиты

$|Orb(x)| = |G : Stab(x)|$

доказательство: 1) введем отн $\sim$

$x \sim y \quad \exists g \in G: gx = y$

экв-сть? : 1) $x = x$ т.к. $ex = x$ $\quad x \sim x$ $\quad$ Р

2) $x \sim y \Rightarrow y \sim x$ т.к. $\quad$ С

$gx = y \Rightarrow y = g^{-1}x$

3) $x \sim y \quad y \sim z \Rightarrow x \sim z$ $\quad$ Т

$gx = y$, $hy = z \Rightarrow hgx = z$

2) экв класс '$\sim$'

$\tilde{x} = \{y \mid x \sim y\} \Rightarrow \{y \mid y = gx, \text{ где } g \in G\} =$

$= \{gx \mid g \in G\} = Orb(x)$

2) $Stab(x) = \{g \in G \mid gx = x\}$ — подгруппа

П $y = gx$, $H = Stab(x)$ $\quad K = Stab(y)$

уб-ся, что $K = gHg^{-1}$, проверим:

$(gHg^{-1})y = gHx = gx = y$

$\Rightarrow \boxed{gHg^{-1} \in Stab(y) = K}$

т.к. $x = g^{-1}y$, то аналогично:

$g^{-1}K(g^{-1})^{-1} \subset H$

$g^{-1}Kg^{+1} \subset H \Rightarrow$

$\boxed{K \subset gHg^{-1}} \Rightarrow K = gHg^{-1}$

т.к. соотв. $h \Leftrightarrow ghg^{-1}$ — биекция $\Rightarrow$

$|K| = |H|$

3) $gx = g'x \Leftrightarrow x = g^{-1}g'x \Leftrightarrow g^{-1}g' \in Stab(x) =: H$

$\Leftrightarrow gH = g'H$

$\Rightarrow$ разл. эл-ов в $Orb(x)$ столько, сколько разл. левых классов подгр H в G, а это и есть индекс подгр. H

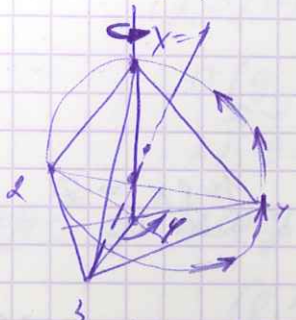
ч.т.д.

следствие: Если кон гр. G дейст на мн-ве X ⇒

$$|G| = |Stab(x)|\cdot|Orb(x)|$$

доказ-во $|G| = \overbrace{|H|} \cdot \overbrace{|G:H|}$ — теорема Лагранжа

пример: найдем порядок группы вращений прав. тетраэд.



G - гр. поворотов тетр T

$Orb(x) = 4$ (4 верш)

$Stab(x) = \{e, \varphi_{\frac{2\pi}{3}}, \varphi^2\}$

$|G| = |Stab(x)|\cdot|Orb(x)| = 3\cdot 4 = 12$

ут-ся, что G изом. A_4 (подст. из 4х символ.)

G содержит в себе

$\{(123)(134)(243)(\dots)\dots\}$ - все тройные

$\{(12)(34)$ и т.д $\}$ - про-е 2х циклов независимых

$\{(1)(2)(3)(4)\}$ - тожд.

$|H| = \underset{\text{тройные}}{4\cdot 2} + 3 + 1 = 12$

$|A_4| = \frac{4!}{2} = 12 \quad A_4 \cong H$

ТЕОРЕМА БЕРНСАЙДА И ПОЙА О ЧИСЛЕ ОРБИТ

Опр: Пусть $G:X$, обозначим X/G - мн-во G-орбит в X

Если $g \in G$, то обозначим

$$Fix(g) = \{x \in X \mid gx = x\}$$

теорема Бернсайда

Пусть конечн G дейст. на кон X ⇒ кол-во G-орбит такое:

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

доказательство: Пусть $F := \{(g,x) \mid g\in G\ x\in X\ gx=x\}$

Подсчитаем $|F|$ двумя способами.

Ясно, что во-первых

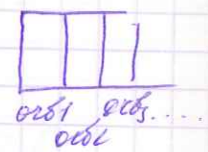
$$|F| = \sum_{g\in G}|Fix(g)|$$

с другой стороны

$$|F| = \sum_{x\in X}|Stab(x)|$$

Пусть $X_1 X_2 \dots X_n$ - все различные G-орбиты X, тогда:

$$|F| = \sum_{x\in X}|Stab(x)| = \sum_{i=1}^{n}\sum_{x\in X_i}|Stab(x)| =$$



$= (\text{теор о мощн. орбит}) =$

$$= \sum_{i=1}^{n}|X_i|\cdot\frac{|G|}{|X_i|} = \sum_{i=1}^{n}|G| = n\cdot|G|$$

/* $|G| = |Stab(x)|\cdot|Orb(x)|$ */

$$\Rightarrow |X/G| = n = \frac{|F|}{|G|} = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

ч.т.д.

Следствие (т. Пойа)

Пусть конечн гр. G дейст на кон. мн-во X, пусть Y - конечн мн-во $|Y| = m$, пусть

$$\Phi = \{\varphi: X\to Y \mid \varphi \text{ - функция}\}$$

Тогда G действует на Φ по правилу

$$(g\circ\varphi) = \varphi(g^{-1}x) \quad \forall x\in X$$

это действие.

$$((gh)\circ\varphi)(x) = \varphi((gh)^{-1}x) = \varphi(h^{-1}(g^{-1}(x))) =$$

$$= (h\circ\varphi)(g^{-1}x) = \underline{(g(h\circ\varphi))(x)}, \ \forall x\in X$$

Тогда ут-ся, что $|\Phi/G| = \frac{1}{|G|}\sum_{g\in G} m^{c(g)}$,

где $c(g)$ - число циклов в раз-ии подст-ки

$\pi(g): x \mapsto gx$ на незав. циклы

(если $gx_1 = gx_2 \Rightarrow x_1 = x_2$)

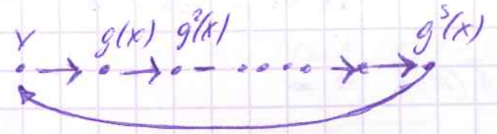
доказательство: ввиду теор Бернсайда дост. доказать

$$|Fix(g)| = m^{c(g)}$$

Если $\varphi \in Fix(g) \Rightarrow g\cdot\varphi = \varphi \Leftrightarrow$

$\Leftrightarrow \varphi(g^{-1}x) = \varphi(x) \quad \forall x\in X \Leftrightarrow$

$\Leftrightarrow$ это означает, что φ пост. на $Orb(x)$ относ $\pi(g)$



$g^{-1}x = x \Rightarrow$ все эл-ты равны, т.е. на цикле в разл. $\pi(g)$

$\pi(g) = \underbrace{(\dots)}_{y_1}\underbrace{(\dots)}_{y_2}(\dots)$

y_1 — m вар-ов, y_2 — m

всего неподв. функций из $Fix(g)$ имеется $m^{c(g)}$

Пример. Найдем число раскрасок (с точностью до поворота) граней тетр. в m цветов.

цикловой тип $\pi(g)$	кол-во эл-ов g такого типа $\pi(g)$	$\lvert Fix(g)\rvert$
$(1)(2)(3)(4)$	1	m^4
$(123)(4)$	8	m^2
$(12)(34)$	3	m^2

$$|\Phi/G| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)| = \frac{1}{12}(m^4+8m^2+3m^2) = \frac{m^4+11m^2}{12} = \frac{m^2(m^2+11)}{12}$$

$m=3$, $|\Phi/G| = 15$

ГОМОМОРФИЗМЫ, НОРМАЛЬНЫЕ ПОДГРУППЫ, ФАКТОР ГРУППЫ

Опр: отобр. $\varphi: G\to G'$ групп G и G' - гомоморфизм, если

$\varphi(ab) = \varphi(a)\cdot\varphi(b)$ $\forall (a,b)\in G$

~~Эл-нты~~

Примеры: 1) $G = S_n$ $G' = \{\{\pm 1\}, \cdot\}$

$\varphi: \pi \to \mathrm{sgn}\,\pi$

2) $G = GL_n(K)$ $G' = (K^* \setminus 0$ отн. $*) = K^*$

гр. умнож. над K — мультипл. гр. поля

Отобр $\varphi: A \to \det A$ - гомоморфизм.

③ Если $G : X$, то отобр

$\pi: G \to S(X)$

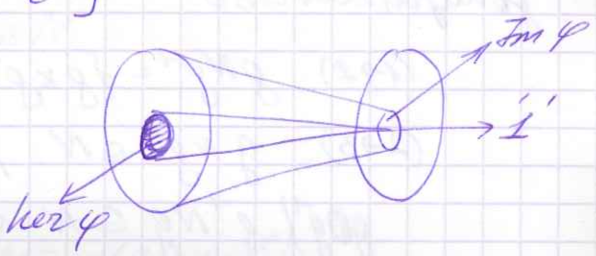
$g \mapsto \pi(g): x \mapsto gx$ - гомоморфизм

Опр: След. мн-ва

образ $\mathrm{Im}\,\varphi = \cancel{\{\varphi(a)\in G \mid \varphi(a)=e\}}\ \{\varphi(a), a\in G\}$

ядро $\mathrm{Ker}\,\varphi = \{a\in G \mid \varphi(a) = e'\}$

гомоморфизм φ



Предложение

$\mathrm{Im}\,\varphi$ и $\mathrm{Ker}\,\varphi$ - подгруппы.

① $\mathrm{Im}\,\varphi$: проверим замкнутость отн. $e, \frac{1}{g}, \cdot$

- Имеем $\varphi(e) = \varphi(e\cdot e) = \varphi(e)\cdot\varphi(e)$, но в группе $x\cdot x = x$ имеет !реш. $e\cdot e = e \Rightarrow$ $\Rightarrow \varphi(e) = e'$
- Кроме того, $e' = \varphi(e) = \varphi(a\cdot a^{-1}) = \varphi(a)\cdot\varphi(a^{-1}) \Rightarrow$ $\Rightarrow [\varphi(a)]^{-1} = \varphi(a^{-1}) \in \mathrm{Im}\,\varphi$
- $\varphi(a)\cdot\varphi(b) = \varphi(ab) \in \mathrm{Im}\,\varphi$ $\Rightarrow$ $\mathrm{Im}\,\varphi$ - подгр.

② $\mathrm{Ker}\,\varphi$

- Т.к. $\varphi(e) = e' \Rightarrow e$ принадл. $\mathrm{Ker}\,\varphi$
- Если $\varphi(a) = e$, то $\varphi(a^{-1}) = (\varphi(a))^{-1} = [e']^{-1} = e'$, $a\in\mathrm{Ker}\,\varphi \Rightarrow a^{-1}\in\mathrm{Ker}\,\varphi$
- Если $\varphi(a) = \varphi(b) = e' \Rightarrow \varphi(ab) = e'$ $\Rightarrow a,b\in\mathrm{Ker}\,\varphi \Rightarrow ab\in\mathrm{Ker}\,\varphi$

ч.т.д.

ЗАМЕЧАНИЕ: Ядро удовл-ет доп св-ву

$g\in G$, $a\in\mathrm{Ker}\,\varphi \Rightarrow g\cdot a\cdot g^{-1}\in\mathrm{Ker}\,\varphi$:

$\varphi(gag^{-1}) = \varphi(g)\cdot\varphi(a)\cdot\varphi(g)^{-1} = \varphi(g)\cdot e\cdot\varphi(g)^{-1} = e$

замкнутость отн. сопр.

ЛЕММА. Для подгр N гр G след усл равносильны

1) $\forall g\in G \ \forall x\in N \quad g\cdot g^{-1}\in N$

2) $\forall g\in G \quad gNg^{-1}\in N$

3) $\forall g\in G \quad gNg^{-1}=N$

4) $\forall g\in G \quad gN=Ng$

Такая подгр-па наз-ся нормальной.

доказательство

(1→2) $gNg^{-1}=\{gxg^{-1} \mid x\in N\}\in N$

(2→3) $gNg^{-1}\in N$, заменим g на g^{-1} =>

$g(g^{-1})\, g^{-1}Ng\in N \Leftrightarrow N\subseteq gNg^{-1}$

(3→4) домножим на g.

(4→1) $\forall g\in G \ \forall x\in N \quad gx\in gN=Ng$ =>

$\exists \ x'\in N: gx=x'\cdot g$

$gxg^{-1}=x'\in N$ ч.т.д

Обозначение: $N \triangleleft G$

Примеры: $\operatorname{Ker}\varphi \triangleleft G$

$A_n \triangleleft S_n$

$SL_n(K) \triangleleft GL_n(K)$

ТЕОРЕМА 1 Пусть N - нормальная подгр. гр. G =>

=> ① мн-во G/N всех смежных классов N в G образует гр. относит. умн. классов

$aN\times bN=abN$

② отобр. $\varphi: a\mapsto aN$ явл. гомоморфизмом G/N с ядром N и образом G/N

такой гомоморфизм наз-ся естественным, а G/N наз-ся фактор-группой группы G по нормальн подгр. N

доказательство:

1) Имеем:

→ $aN\cdot bN=ab\underbrace{b^{-1}Nb}_{N}N=abN^2=abN$

→ $aN\cdot bN=a(Nb)N=abNN=abN$

умножение классов асс-на, ∃ 1 и a^{-1}

~ $(aN\cdot bN)cN=(ab)cN=a(bc)N=aN(bN\cdot cN)$

~ $eN=N \ : eN\cdot aN=aN$

~ $a^{-1}N$ - очевидно

2) Гомоморфизм

$\varphi(ab)=abN=aN\cdot bN=\varphi(a)\cdot\varphi(b)$

$\operatorname{Ker}\varphi=\{a\in G \mid aN=N\}=\{a\in G,\ a\in N\}=N$

$\operatorname{Im}\varphi=\{aN \mid a\in G\}=G/N$

ТЕОРЕМА 2 Пусть $\varphi: G\to G'$ - гомом. => ч.т.д.

=> $G/\operatorname{Ker}\varphi\cong \operatorname{Im}\varphi$

Как известно образ груп по законам конгруэнц. изоморфен фактор-гр. по ядру гомом.

док-во: Обозначим $N=\operatorname{Ker}\varphi$

Установим соотв.:

$aN\leftrightarrow\varphi(a)$

Это соотв взаимнооднозначно:

$aN=bN \Leftrightarrow a^{-1}b\in N=\operatorname{Ker}\varphi \Leftrightarrow$

$\Leftrightarrow \varphi(a^{-1}b)=e' \Leftrightarrow \varphi(a)^{-1}\varphi(b)=e \Leftrightarrow \varphi(a)=\varphi(b)$

Соотв. сохр. операции:

$\left.\begin{matrix} aN\leftrightarrow\varphi(a)\\ bN\leftrightarrow\varphi(b)\end{matrix}\right\} \Rightarrow \underbrace{aN\cdot bN=abN}\leftrightarrow\varphi(ab)\leftrightarrow\underbrace{\varphi(a)\cdot\varphi(b)}$

=> ч.т.д.

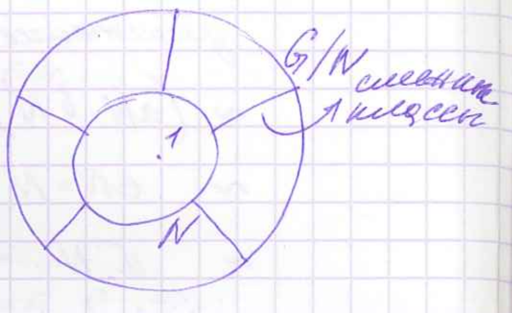
следствие:

пример: $S_n/A_n^{\text{чётные}} = \mathbb{Z}_2 = \{\pm 1\}$

$GL_n(K)/SL_n(K) = K^*$ — ненулевые элементы поля

Опр: Группа G — простая $\Leftrightarrow$ не $\exists$ нормальных подгрупп $N \ne G$, $N \ne \{e\}$

Иначе G — составное



Опр. Пусть A, B — мульт. гр.

Мн-во

$$A\times B = \{(a,b) \mid a\in A \ b\in B\}$$

умножение

$$(a,b)\cdot(a',b') = (aa', bb')$$

образует мультипл. группу, которая наз-ся прямым произв. гр. A и B и обозн.

$(A\times B)$

аналог. опр.

$A_1\times A_2\times A_3$, $A^n = \underbrace{A\times\ldots\times A}_{n}$

если аддитивная операц

$A\oplus B$ прямая сумма $\quad \bigoplus_i A_i$

ТЕОРЕМА

$A,B \triangleleft G$ $\quad A\cap B=\{e\}$

$A\cdot B = G \Rightarrow G\cong A\times B$

доказательство:

установим соот. между $A\times B$ по правилу

$G\ni g = ab \longleftrightarrow (a,b)\in A\times B$

покажем взаимнооднозначность

$a'b' = ab \Leftrightarrow a^{-1}a' = b(b')^{-1} \in A\cap B = \{e\}$

$\Leftrightarrow (a^{-1}a' = b(b')^{-1} = e) \Leftrightarrow (a'=a, b'=b) \Leftrightarrow$

$\Leftrightarrow (a',b') = (a,b)$

Чтобы проверить, что это гомоморфизм, докажем, что $ab = ba$ $\forall a\in A \ \forall b\in B$

Пусть $aba^{-1}b^{-1}$ — "коммутатор"

$$\Rightarrow aba^{-1}b^{-1} = a\underset{\in B}{(ba^{-1}b^{-1})} = \underset{\in A}{(aba^{-1})}b^{-1} \in A\cap B = \{e\}$$

Теперь:

$g = ab \longleftrightarrow (a,b)$

$g' = a'b' \longleftrightarrow (a',b')$

$\Downarrow$

$g\cdot g' = aba'b' = aa'bb' \longleftrightarrow (aa', bb')$

доказано.

пример Если p и q — взаимнопр. натур. числа, то

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p\times\mathbb{Z}_q$$

доказ-во: $\mathbb{Z}_{pq} = \langle z\rangle$ $\quad \operatorname{ord} z = pq$

Пусть $A = \langle z^q\rangle \Rightarrow \operatorname{ord}(z^q) = |A| = \frac{pq}{\text{НОД}(pq,q)} = p$

Пусть $B = \langle z^p\rangle \Rightarrow |B| = q$

A и $B \triangleleft \mathbb{Z}_{pq}$ т.к. $\mathbb{Z}_{pq}$ — абелева, а в абелевой $\forall$ гр. нормальна

$A\cap B = e$ т.к. порядок перес. делит и пор A и пор B (Th Лагранжа)

$p\ne q \Rightarrow |A\cap B| = 1$

$\forall$ эл-т есть произ:

для $\forall$ k — целого $\exists$ целые x, y:

$px + q\cdot y = k$ (лин. диоф. ур-ие) — разрешимо

$\Leftrightarrow$ НОД$(p,q) = 1 \mid k \Rightarrow$ верно $\Rightarrow$

$$\Rightarrow z^k = z^{px+qy} = z^{px}\cdot z^{qy} = \underset{A}{(z^p)^x}\cdot\underset{B}{(z^q)^y}$$

$\mathbb{Z}_6 \cong \mathbb{Z}_2\cdot\mathbb{Z}_3$

ПРИВЕДЕНИЕ ЦЕЛОЧИСЛ. МАТР. КАНОН. (ДИАГ) ВИДУ.

Опр: След. преобр. систем строк (столбцов) целочисл матр. наз-ся эл-ными

I. К одной стр. прибавл. др., умнож. на скаляр $\lambda \in \mathbb{Z}$

II Перестановка строк (столб)

III Умнож. строки (столбца на обратимый скаляр из $\mathbb{Z}$ т.е на ± 1

ТЕОРЕМА: Всякую целоч. матр. эл. систем строк и столбцов можно привести к канон. диаг. виду.

$$D = \left(\begin{array}{cc|c} d_1 & 0 & 0 \\ 0 & d_n & \\ \hline 0 & & 0 \end{array}\right) \qquad d_i \in \mathbb{N}, \quad d_i \mid d_{i+1} \ \forall i$$

Числа d_i - инвариант. множителей матр A и задаются матр A однозначно

доказательство:

(I) $A = (a_{ij})$, $a_{ij} \in \mathbb{Z}$

Если $A = 0$, то очевидно.

Пусть $A \neq 0$, имеет n столбцов

$a = \min\{|a_{ij}| \mid a_{ij} \neq 0 \ \ i,j > 0\}$

используем индукцию по паре параметров

$- n, a -$

Сл.1 Пусть $a = a_{ij}$ делит нацело все эл-ы матрицы A

Тогда переставим его на место (1,1) и эл-преобр I получим нули под ним и справа

$$A \to \left(\begin{array}{c|c} a & c \\ \hline b & \ddots \end{array}\right) \to \left(\begin{array}{c|c} a & 0000 \\ \hline 0 & \\ 0 & A' \\ 0 & \\ 0 & \end{array}\right) \quad A' \text{- индукция.}$$

$A' \rightsquigarrow D \Rightarrow A \rightsquigarrow D$

~~$\exists b = a_{ke}$~~:

случай 2: $\exists\, b = a_{ke} \mid a \nmid b$

2.1) b и a - в одном столбце или строке

$b = aq + r$, $\left.\begin{array}{l} r \geq 0 \\ r < a \end{array}\right\}$ остаток

$$\begin{bmatrix} — b — \\ \\ — a — \end{bmatrix} \times(-q) \ +$$

получится

$$\begin{bmatrix} — \overset{r}{b - aq} — \\ — a — \end{bmatrix} \qquad (n, a) \to (n, r)$$

$r < a \Rightarrow$ индукция.

2.2) b и a в разных строках

a делит все эл-ы своей строки и столбца

$$\left[\begin{array}{c|c} - b - & \\ \hline & - a - \end{array}\right] \xrightarrow{I} \left[\begin{array}{c|c} - b & \begin{smallmatrix} 0\\0\\0\\0 \end{smallmatrix} \\ 0000 & a\,0000 \\ & \begin{smallmatrix} 0\\0\\0 \end{smallmatrix} \end{array}\right] \to \left[\begin{array}{c} b \\ \vdots \\ 0000\, a\, 000 \\ \vdots \end{array}\right] \text{— случай 2.1}$$

$\times 1$ $+$

(II) Единственность инвариантных множителей:

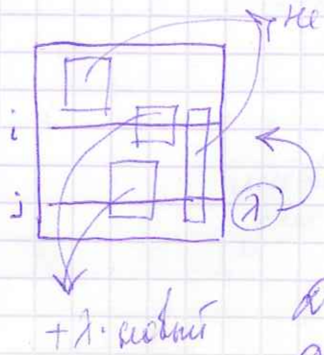
Пусть

$D_k = $ НОД {все миноры порядка k из A_k}

утверждаем, что D_k не изм. при эл. матр A

Действительно, преобр II и III миноры порядка k могут изменить знак, но НОД не изменится.

При преобр I миноры либо не изм, либо к одному минору порядка k прибавится др. минор, умнож. на целое число,



НОД - const.

$$A \xrightarrow{I\ II\ III} D = \left(\begin{array}{cc|c} d_1 & 0 & 0 \\ & d_2 & \\ 0 & d_n & \\ \hline 0 & & 0 \end{array}\right)$$

$D_k(A) = D_k(D) \ \forall k$

$D_{n+1} = D_{n+k} = \ldots = 0$

$D_1(A) = d_1 = D_1(D)$

$D_2(A) = D_2(D) = d_1 d_2 \qquad D_3(A) = d_1 d_2 d_3 \ldots$

$d_1 = D_1(A)$

$d_2 = \dfrac{D_2(A)}{D_1(A)}$ и т.д. $\quad d_i \Rightarrow$ ИНВАРИАНТ.

$d_3 = \dfrac{D_3(A)}{D_2(A)} \dots$

ч.т.д.

следствие

Опр: матр. A из $M_n(\mathbb{Z})$ наз-ся унимодулярной, если она обратима и A^{-1} целочисл.

Следствие 1: След. утв. $(\Leftrightarrow)$

1) A - унимодулярна
2) $\det A = \pm 1$
3) $A \xrightarrow{\text{эл}} E$

доказат-во:

$(1\to 2)$ $A \cdot A^{-1} = E$ $\quad A, A^{-1}$ - целоч $\Rightarrow$

$$\underset{\mathbb{Z}}{\det A} \cdot \underset{\mathbb{Z}}{\det A^{-1}} = 1 \Leftrightarrow \left[\begin{array}{l}\det A = 1\\ \det A = -1\end{array}\right.$$

$(2\to 3)$ Если $A \to D = \mathrm{Diag}(d_1 \dots d_m, 0 \dots 0) \Rightarrow$

$\Rightarrow \det A = \pm \det D$

$\pm 1 \Rightarrow \det D = 1$

$m = n$ и $d_1 \dots d_n = 1 \Rightarrow d_i = 1 \Rightarrow D = E$

$(3\to 1)$ Ввиду предыд. $\det A = \pm \det D = \pm 1$

$$\Rightarrow A^{-1} = \underbrace{\frac{1}{\det A}}_{\in \mathbb{Z}} \underset{\in\mathbb{Z}}{(A_{ij})} \in \mathbb{Z}$$

Следствие 2 Для всех матр $A \in M_n(\mathbb{Z})$

$\exists$ унимод. матр. L и R кор-и $|$

$LAR = D = \mathrm{Diag}(d_1 \dots d_n)$

$d_i \in \mathbb{N}$ $\quad d_i \mid d_{i+1}$ $\forall i$

Док-во: D получ. из A эл.пр.

I рода над $\mathbb{Z}$, каждое такое преобр эквивалент. умножению на трансвекцию

$T_{ij}(\lambda)$ $\quad \lambda \in \mathbb{Z}$ $\quad$ (L - трансвек слева, R - спр.)

в итоге

$$\underset{L}{(L_k \dots L_1)} A \underset{R}{(R_1 \dots R_l)} = D$$

$\det L = 1 \quad \det R = 1$

унимодулярны

СЛЕДСТВИЕ 3 $\forall$ целочисл сист. ур-ий (линейных)

$Ax = B$ $\exists$ алгоритм, определяющий совместность системы над $\mathbb{Z}$ и дающий полное описание мн-ва решений над $\mathbb{Z}$

доказательство:

По сл. 2 $\exists$ унимод. матр R и L | $LAR = D$ - диагональн

Сист. $Ax = B$ равнос. над $\mathbb{Z}$ системе

$$\underbrace{LAR}_{D}\underbrace{R^{-1}x}_{y} = \underbrace{LB}_{C}$$

целоч. т.к. R - унимодулярна

$\Rightarrow Dy = C$, D - диагональна

$$\begin{cases} d_1 y_1 = c_1 \\ \vdots \\ d_m y_m = c_m \\ 0 = c_{m+1} \\ \vdots \\ 0 = c_n \end{cases}$$

решение над $\mathbb{Z}$ сущ $\Leftrightarrow$ $\begin{cases} d_1 \mid c_1 \dots d_m \mid c_m \text{ и} \\ c_{m+1} = c_{m+2} = \dots = c_n = 0 \end{cases}$

мн-во всех решений для y: $\begin{pmatrix} c_1/d_1 \\ \vdots \\ c_m/d_m \\ y_{m+1} \\ \vdots \\ y_n \end{pmatrix}$ $\quad y_i \in \mathbb{Z}$ $\forall i = m+1 \dots n$

мн-во реш. для x: $x = Ry \in \mathbb{Z}^n$

ч.т.д.

алгоритм

$$\{\left(\begin{array}{c|c} A & B \\ \hline E & \end{array}\right) \xrightarrow[\text{1ых } S \text{ строк и первых } n \text{ столбцов}]{\text{I II III э.п.}} \left(\begin{array}{c|c} LAR & LB \\ \hline ER & \end{array}\right) = \left(\begin{array}{c|c} D & C \\ \hline R & \end{array}\right), \quad ER = R$$

СВОБОДНЫЕ АБЕЛЕВЫ ГРУППЫ КОНЕЧНОГО РАНГА И ИХ ПОДГРУППЫ

Опр: Абелева группа аддитивная F — свободная, если она обладает базисом $e_1 \dots e_n$

т.е таким набором упор. эл-ов $e_1 \dots e_n$ |

$\forall$ эл-нт x, из F имеет единст. предст.

$x = x_1 e_1 \dots x_n e_n \quad x_i \in \mathbb{Z}$

пример: $F = \mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$

$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix} \quad e_n = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$ — св. базис

Опр: Если мощность базиса n, то говорят, что

F — св. абелева ранга n

упр: Если $rk F = n \Rightarrow F \cong \mathbb{Z}^n$

$x \to \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ч.т.д.

ЛЕММА (о базисах)

Пусть $e_1 \dots e_n$ — базис св. аб. гр. F

Пусть $e_1' \dots e_n'$ — набор эл-ов из F и $e_j' = \sum_{i=1}^n e_i c_{ij} \quad c_{ij} \in \mathbb{Z}$

$C = (c_{ij}) \quad 1 < i,j < n$ — целочисл.

тогда $e_1' \dots e_n'$ — базис $F \Leftrightarrow$ C — унимодулярна

док-во: ($\Rightarrow$) Т.к $e_1' \dots e_n'$ — базис $F \Rightarrow$

(*) $e_j = \sum e_i' c_{ij}'$ — целочисл

Пусть $C' = (c_{ij}') \Rightarrow CC' = E$

$C^{-1} = C' \Rightarrow$ она целочисл $\Rightarrow$ унимодулярна

($\Leftarrow$) Как и для векторных пр-в

если X_e и X_e' — координаты "вектора" x в ст. и нов. базисах

$$\exists \quad x = \sum_{j=1}^n e_j x_j \overset{(*)}{=} \sum_{j=1}^n \Big(\sum_{i=1}^n e_i' c_{ij}'\Big) x_j =$$

$$= \sum_{i=1}^n \underbrace{\Big(\sum_{j=1}^n c_{ij}' \cdot x_j\Big)}_{\text{новые коэффициенты}} e_i'$$

обозначим $x_i' = \sum_{j=1}^n c_{ij}' \cdot x_j \in \mathbb{Z}$ т.к $x_j \in \mathbb{Z}$ и $c_{ij}' \in \mathbb{Z}$

Равносильно $X = \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix} = \begin{pmatrix} c_{11}' & \dots & c_{1n}' \\ c_{n1}' & & c_{nn}' \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C' X_e$

$C' = C^{-1}$, X_e — единст. C — единст. $\Rightarrow C^{-1}$ — единст. $\Rightarrow$

$X_e' = C^{-1} X_e$ — единст.

ч.т.д

ТЕОРЕМА (о подгруппах)

Всякая подгр. N св. аб. гр F ранга n сама свободна ранга $m \leq n$, более того

F и N обладают <u>соглас. базисами</u>

$F: e_1' \dots e_m', e_{m+1}' \dots e_n'$

$N: d_1 e_1' \dots d_m e_m' \mid d_i \in \mathbb{N}$ и $d_i | d_{i+1}$

доказательство:

$N = \langle a_1, a_2, \dots, a_N \rangle \qquad a_j = \sum_i e_i a_{ij}, \; a_{ij} \in \mathbb{Z}$

$F = \langle e_1 \dots e_n \rangle$ — базис

$A = (a_{ij}) \quad$ i — строки $1 < i < n$, j — столбцы $1 < i < N$

$(a_1 \dots a_N) = (e_1 \dots e_n) A$

по сл. 2 $\exists$ унимод. мат L и R | $LAR = \overset{D}{Diag(d_1, \dots d_n, 0, 0 \dots)}$

Тогда $(a_1 \dots a_N) R = (e_1 \dots e_n) \underbrace{L^{-1} L}_{E} AR$

$a_1' \dots a_N' \qquad \underbrace{\qquad\qquad}_{\text{другой базис}}$

$\boxed{L}\,\boxed{A} \quad \boxed{R^{1}}$

$$\begin{cases} a_1' = e_1' d_1 \\ a_m' = e_m' d_m \\ a_{m+1}' = a \dots = a_N = 0 \end{cases}$$

учтём

1) $e_1' \dots e_n'$ - базис F т.к. L' унимодулярна и $e_1 \dots e_n$ - базис (по лемме)

2) $\langle a_1' \dots a_m' \rangle = \langle a_1' \dots a_N' \rangle = \langle a_1 \dots a_N \rangle$ - т.к. R- унимодулярна, $= N$

3) $d_1 e_1' \dots d_m e_m'$ - базис N, т.к.

$\sum\limits_{i=1}^{m} \lambda_i (d_i e_i') = 0 \iff \lambda_i \cdot d_i = 0, \forall i$

$d_i \in N \Rightarrow \lambda_1 = \dots = \lambda_m = 0$

отсюда единст. выраж. ч/з $d_1 e_1' \dots d_n e_n'$

4) согласованность базисов очевидна, уже есть

ч.т.д.

РАЗЛОЖЕНИЕ КОНЕЧНОПОРОЖД. АБЕЛЕВЫХ ГРУПП В ПР Σ ЦИКЛИЧЕСКИХ

ТЕОРЕМА: Пусть G - кон.пор. абелева гр $\Rightarrow$

G - прямая Σ циклических групп

$G = \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m} \oplus \underbrace{\mathbb{Z}_\infty \oplus \dots \oplus \mathbb{Z}_\infty}_{r}$

$d_i \in \mathbb{N}$ и $d_i | d_{i+1}$

доказательство:

Пусть $G = \langle g_1 \dots g_n \rangle$ $n < \infty$

Пусть F - своб. абелева гр. ранга n с базисом $e_1 \dots e_n$

Отображение $\sum\limits_{i=1}^{n} x_i e_i = x \xrightarrow{\varphi} \sum\limits_{i=1}^{n} x_i g_i$, $x_i \in \mathbb{Z}$, $\in F$, $\in G$

φ - гомоморфизм групп

- это отобр. т.к. из св. базиса x_i ! корректно

$\varphi(\sum x_i e_i + \sum y_i e_i) = \varphi(\sum (x_i + y_i) e_i) =$

$= \sum (x_i + y_i) g_i = \sum x_i g_i + \sum y_i g_i = \varphi(x) + \varphi(y)$

Ясно, что $\operatorname{Im} \varphi = G$ т.к. $G = \langle g_1 \dots g_n \rangle$,

Пусть $N = \ker \varphi \Rightarrow G = \operatorname{Im} \varphi \cong F/(\ker \varphi) = F/N$

По Т о подгр-пах $F = \langle e_1' \dots e_n' \rangle$ $N = \langle d_1 e_1' \dots d_m e_m' \rangle$

$d_i | d_{i+1} \in \mathbb{N}$

ЛЕММА (задача о факторизации)

Пусть $N_i \trianglelefteq G_i$, $i = 1 \dots n$

обозначим $G = \bigoplus\limits_{i=1}^{n} G_i$ $N = \bigoplus\limits_{i=1}^{n} N_i \leq G$

Тогда $\Rightarrow$ $G/N \cong (G_1/N_1) \oplus \dots \oplus (G_n/N_n)$

доказательство:

Отобр. $\varphi: (g_1 \dots g_n) \longmapsto (g_1 + N_1, \dots, g_n + N_n)$

- гомоморфизм G на $\bigoplus\limits_{i=1}^{n} (G_i / N_i)$ с ядром N

ч.т.д.

окончание док-ва теоремы

$G = F/N = \langle e_1' \rangle \oplus \dots \oplus \langle e_n' \rangle) / (\langle d_1 e_1' \rangle \oplus \dots \oplus \langle d_m e_m' \rangle)$

лемма $= (\langle e_1' \rangle / \langle d_1 e_1' \rangle \oplus \dots \oplus \langle e_m' \rangle / \langle d_m e_m' \rangle \oplus \langle e_{m+1}' \rangle \oplus \dots \oplus \langle e_n' \rangle \cong$

$\cong \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$

ч.т.д.

$n - m = r$?

ЕДИНСТВЕННОСТЬ РАЗЛОЖЕНИЯ К.П. АБ. ГР. В ПР. СУММУ БЕСКОН. И ПРИМАРНЫХ ЦИКЛИЧЕСКИХ.

Опр: группа наз-ся примарной, если её порядок - ст. простого числа

ТЕОРЕМА $\forall$ кон. пор. аб. гр - единст. образом (с точностью до изоморфизма) разлаг. в прям Σ беск. цикл и примарных цикл. групп.

док-во: 1) $\exists$-ие: достаточно разложить цикл. группу порядка d в Σ примарных циклических.

Пусть $d = p_1^{k_1} \dots p_s^{k_s}$ p_i - прост k_i - натур.

используем индукцию по s

$s = 1$) - очевидно

$s > 1$) - обозначим $p = p_1^{k_1}$ $q = p_2^{k_2} \dots p_s^{k_s} \Rightarrow p \perp q$

Имеем $\mathbb{Z}_d = \mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$ т.к. $p \perp q$ $= \underbrace{\mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z} \dots \oplus}_{\text{индукция}}$

2) "!-ость"

Введем в гр G (абелевой) след. под-ва:

1) $T(G) = \{g \in G \mid \operatorname{ord} g < \infty\}$ — периодическая часть гр. G

2) $T_p(G) = \{g \in G \mid \exists k \ \operatorname{ord} g = p^k\}$ — p-периодическая часть гр G (p — простое, $k(g)$)

3) $pG = \{px \mid x \in G\}$ — p-кратная гр G

они под-сл

Утв-се, что все (1-3) подгруппы:

1) пусть $ng = 0$, $mh = 0 \Rightarrow$

$(m+n)(g \pm h) = 0$

2) $p^k g = 0$, $p^\ell h = 0 \Rightarrow$

$\Rightarrow (g+h)(p^{k+\ell}) = 0$

3) $\forall x, y \in G \quad px \pm py = p(x \pm y)$

Утв-се что, если соотв $g \leftrightarrow g'$ - изоморфизм G и G'

то $T(G) \xleftrightarrow{\simeq} T(G')$

$T_p(G) \xleftrightarrow{\simeq} T_p(G')$

$p(G) \xleftrightarrow{\simeq} p(G')$

это следует из сохр. порядка эл-та при изоморфизме

$g \quad g'$ 'равное в равное'

$g^2 \quad (g')^2$

$\vdots \quad \vdots$

$g^n = 1 \quad (g')^n = 1$

ЛЕММА 1. Пусть $a \leftrightarrow a'$ - изоморфизм G и G'

Пусть $N \triangleleft G$, $N' \triangleleft G'$, $a \in N \Leftrightarrow a' \in N'$, тогда

$G/N \simeq G'/N'$

доказательство: $aN \leftrightarrow a'N'$ - это и будет изоморф. между G/N и G'/N'

1) $aN = bN \Leftrightarrow a^{-1}b \in N \Leftrightarrow (a^{-1}b)' \in N' \Leftrightarrow (a')^{-1}(b)' \in N' \Leftrightarrow$

$\Leftrightarrow a'N' = b'N'$

2) $\left.\begin{matrix} aN \leftrightarrow a'N' \\ bN \leftrightarrow b'N' \end{matrix}\right\} \Rightarrow abN \leftrightarrow (ab)'N = a'N' \cdot b'N'$

Если $G = T(G) \oplus \mathbb{Z}^r$

то $\mathbb{Z}^r \simeq G/T(G)$

Если $G' = T(G') \oplus \mathbb{Z}^{r'}$

то $\mathbb{Z}^{r'} \simeq G'/(T(G'))$

Ввиду леммы $\mathbb{Z}^r \simeq \mathbb{Z}^{r'}$

$$\mathbb{Z}^r/p\mathbb{Z}^r \simeq \mathbb{Z}^{r'}/p(\mathbb{Z}^{r'})$$

$$\mathbb{Z}_p^r \qquad \mathbb{Z}_p^{r'}$$

$p^r = |\mathbb{Z}_p^r| = |\mathbb{Z}_p^{r'}| = p^{r'} \Rightarrow r = r'$, мы доказали что при изоморфизме число ∞ слагаемых совпадает.

Имеем: $T(G) = \bigoplus_p T_p(G)$

$T(G') = \bigoplus_p T_p(G')$

$T_p(G) \simeq T_p(G') \quad \forall p$-прост.

Имеем: $T_p(G) = \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{s_1} \oplus \underbrace{\mathbb{Z}_{p^2} \oplus \cdots \oplus \mathbb{Z}_{p^2}}_{s_2} \oplus$

$\oplus \underbrace{\mathbb{Z}_{p^k} \oplus \cdots \oplus \mathbb{Z}_{p^k}}_{s_k}$

Надо доказать, что набор чисел задается группой $T_p(G) = G$ однозначно!

- Рассмотрим подгруппы и их раз-ие в Σ примар. циклических.

$G > pG > p^2G > \dots > \dots$

$pG = \underbrace{\mathbb{Z}_1 \oplus \cdots \oplus \mathbb{Z}_p}_{s_1} \oplus \underbrace{\mathbb{Z}_{p^2} \oplus \cdots \oplus \mathbb{Z}_{p^2}}_{s_2} \oplus \dots$

$|G| = p^{s_1}(p^2)^{s_2} \dots = p^{s_1 + 2s_2 + 3s_3 + 4s_4 \dots}$

$\log_p |G| = s_1 + 2s_2 + \dots + \dots$

Аналогично:

$\log_p|pG| = \quad S_2 + 2S_3 + \ldots$

$\log_p|p^2G| = \quad S_3 + 2S_4 + \ldots$

левые части зависят только от G и числа p, переменные правой части однозначно выражаются ч/з них.

ПРИМЕР: Число различных (до изом) абелевых групп порядка 1000

$1000 = 2^3 5^3$

если $|G| = 1000$ то $G \simeq T_2(G) \oplus T_5(G)$

$$T_2(G) = \left[\begin{array}{l} \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_4 \\ \mathbb{Z}_8 \end{array}\right.$$

$$T_5(G) = \left[\begin{array}{l} \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\ \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \\ \mathbb{Z}_{125} \end{array}\right.$$

Всего 9 групп (3×3)

ч.т.д.

ОСНОВЫ ТЕОРИИ ЧИСЕЛ ....

ТЕОРЕМА ЛАМЕ́

ТЕОРЕМА Пусть a, b натур числа $a > b$

Пусть l число цифр в десятичном разложении меньшего числа $b \Rightarrow$ число шагов (делений с остатком) в Алгоритме Евклида для вычисл НОД не превосходит числа $5l$

т.е не больше чем $5(\log_{10} b + 1)$

$10^{l-1} \left[< b < 10^l \iff \lg(b) < l \right]$

$\underbrace{l-1 < \lg b < l}$

$l < \log_{10} b + 1$

доказательство: сопоставление ч/з ср-ие посл-сти Фибоначчи

$f(0) = 0$
$f(1) = 1$
$f(n+1) = f(n) + f(n-1)$

[	0	1	1	2	3	5	8	13	21	34	55	89 ...	]
N	0	1	2	3	4	5	6	7					

и послед-сти делений с остатком

ЛЕММА 1 $F_{n+5} > 10F_n$; $n \geq 2$

доказательство: индукция.

$n = 2$ ⊕
$F_7 = 13 > 10 = 10F_2$

$n-1 \Rightarrow n$ $(n > 2)$

$$F_{n+5} = F_{n+4} + F_{n+3} = 2F_{n+3} + F_{n+2} =$$
$$= 3F_{n+2} + 2F_{n+1} =$$
$$= 5F_{n+1} + 3F_n =$$
$$= 8F_n + \underbrace{5F_{n-1}}_{>0} \gtrless 8F_n + 4F_{n-1} > 10F_n$$

$$\begin{cases} F_n = F_{n-1} + \underbrace{F_{n-2}} < 2F_{n-1} \\ 4F_{n-1} > 2F_n \end{cases}$$

ЛЕММА 2 $F_{n+5\ell} > 10^{\ell} F_n$, $n \geq 2$

док-во. инд (ℓ)

$\ell = 1$ — л.1

$\ell - 1 \Rightarrow \ell$

$$F_{n+5\ell} = F_{n+5(\ell-1)+5} \underset{л.1}{>} 10 F_{n+5(\ell-1)} \overset{инд.}{>} 10 \cdot 10^{\ell-1} F_n = 10^{\ell} F_n$$

док-во

Т1. Установим связь с посл-стью делений в алг Евкл

$$a = b \cdot q_1 + r_2$$
$$b = r_2 \cdot q_2 + r_3$$
$$r_1 = r_3 q_3 + r_4$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

$$\begin{cases} a = bq_1 + r_2 \\ b = r_2 q_2 + r_3 \\ r_2 = r_3 q_3 + r_4 \\ \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n+1} = r_n q_n \end{cases}$$

$$\underset{r_0}{a} > \underset{r_1}{b} > r_2 > r_3 > r_4 > \ldots > r_{n-1} > r_n \geq 1$$

Тогда

F_0	F_1	F_2	F_3	F_4	F_5
0	1	1	2	3	5

$$r_n \geq 1 = F_2$$
$$r_{n-1} \geq 2 = F_3$$
$$r_{n-2} = r_{n-1} \underbrace{q_{n-1}}_{\geq 1} + r_n \geq r_{n-1} + r_n \geq F_3 + F_2 = F_4 = 3$$

$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1} \geq F_3 + F_4 = F_5$$

Продолжая, получим:

$$b = r_1 \geq F_{n+1}$$

а теперь: $\exists$ число шагов $n > \underbrace{5\ell}$ $\Rightarrow$

$n \geq 5\ell + 1$

$$\Rightarrow b \geq F_{n+1} = F_{5\ell+2} \overset{по\ л(2)}{\geq} 10^{\ell} \cdot F_2 = 10^{\ell} \Rightarrow$$

$$\Rightarrow b > 10^{\ell}$$ ↯

Т Ламé доказана!

КОНЕЧНЫЕ НЕПРЕРЫВНЫЕ ДРОБИ (ЦЕПНЫЕ)

Пусть a, b — нат.числа $a > b$

По алг. Евклида:

$$a = b q_1 + r_2$$
$$b = r_2 q_2 + r_3$$
$$r_2 = r_3 q_3 + r_4$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n \qquad r_n = \text{нод}(a, b)$$

$$\Rightarrow \frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{r_2/r_3}} \overset{(3)}{=} q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots}} =$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots\, q_{n-1} + \cfrac{1}{q_n}}}}}$$

это и есть непр-ая (цепная) дробь

Если оборвать вычисл на шаге k то

$$\frac{P_k}{Q_k} = q_1 + \cfrac{1}{\ddots \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}$$

— это как подх дроб.

Св-ва

1) $[q_1 q_2 \ldots q_k] = q_1 + \dfrac{1}{[q_2 \ldots q_k]}$ = ②

Теорема о соответствии

Пусть $q_1 \ldots q_k$ непол эл-ы поле $\Rightarrow$

$$\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \ldots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}$$

$$\Rightarrow \frac{P_k}{Q_k} = [q_1 \ldots q_k]$$

док-во:

$k=1$: очев. $\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow \frac{q_1}{1} = [q_1]$

По опр: $P_1 = q_1 \quad P_0 = 1$
$Q_1 = 1 \quad Q_0 = 0$

Пусть
$$\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} X_{k-1} & X_{k-2} \\ Y_{k-1} & Y_{k-2} \end{pmatrix}$$
$$\frac{X_{k-1}}{Y_{k-1}} = [q_2 \dots q_k]$$

Тогда:
$$\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X_{k-1} & X_{k-2} \\ Y_{k-1} & X_{k-2} \end{pmatrix} =$$
$$= \begin{pmatrix} q_1 X_{k-1} + Y_{k-1} & * \\ X_{k-1} & * \end{pmatrix}$$

$\Rightarrow P_k = q_1 X_{k-1} + Y_{k-1}$
$Q_k = X_{k-1}$
$\Rightarrow \frac{P_k}{Q_k} = q_1 + \frac{Y_{k-1}}{X_{k-1}} = q_1 + \frac{1}{X_{k-1}/Y_{k-1}}$

по инд $= q_1 + \frac{1}{[q_2 \dots q_k]} = [q_1 \dots q_k]$

следствие 1: $\begin{cases} P_k = q_k P_{k-1} + P_{k-2} \\ Q_k = q_k Q_{k-1} + Q_{k-2} \end{cases}$

доказат-во:

берем $\cancel{\frac{P_k}{Q_k}}$ $\begin{pmatrix} P_k & * \\ Q_k & * \end{pmatrix} = \underbrace{\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots}\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} =$

$$= \begin{pmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{pmatrix} \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$$

Отсюда табл подх-их дробей

k	0	1	2
q_k	//////	q_1	q_2
P_k	1	q_1	
Q_k	0	0	q_2

сачим:

следствие 2: $Q_k \geq 2^{\frac{k-2}{2}}$, при $k \geq 2$, числа Q_k мон $\uparrow$ и

доказ-во:

индукция по k,

$k=2$: $Q_2 = q_2 \geq 1 = 2^{\frac{2-2}{2}}$ $+$

инд. пер.

$(k-1) \to (k)$

$Q_k = q_k Q_{k-1} + Q_{k-2} \geq$

$\geq Q_{k-1} + Q_{k-2} \geq 2 Q_{k-2} \overset{\text{инд}}{\geq} 2 \cdot 2^{\frac{(k-2)-2}{2}} = 2^{\frac{k-2}{2}}$ $+$

следствие 3: $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k$ (*)

док-во. $\det \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} = (-1)^k$ по сл. 1.

следствие 4: $P_k \perp Q_k \ \forall k$

очевидно сл. из сл. 3.

$\text{НОД}(P_k, Q_k) \mid \pm 1 \Rightarrow P_k \perp Q_k$

следствие 5: $\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k \cdot Q_{k-1}}$

доказат-во: из сл. 3.

деление на $(Q_k Q_{k-1})$ (*)

следствие 6: $\frac{a}{b} = \frac{P_n}{Q_n} = q_1 + \sum_{k=2}^{n} \frac{(-1)^k}{Q_k Q_{k-1}}$

доказ-во: $\frac{a}{b} = \frac{P_n}{Q_n} = \frac{P_1}{Q_1} + \left(\frac{P_2}{Q_2} - \frac{P_1}{Q_1}\right) + \left(\frac{P_3}{Q_3} - \frac{P_2}{Q_2}\right) +$

$+ \dots + \left(\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right)$;

ИРРАЦ. ЧИСЛА И БЕСК. НЕПР. ДРОБИ

Как обобщить алг Евкл для прибл. ир-ого числа

$\alpha \in \mathbb{R}, \alpha \notin \mathbb{Q}$

$$\alpha = \underset{\in \mathbb{Z}}{[\alpha]} + \underset{0 \le \cdot < 1}{\{\alpha\}}$$

$[\alpha] \quad \alpha$, $\{\alpha\}$

$[\alpha]$ — ближ. слева

Тогда $\{\alpha\} \notin \mathbb{Q}$

теперь $\alpha = \underset{[\alpha]}{q_1} + \underset{\{\alpha\}}{\frac{1}{\alpha_1}}$, где q_1 – целое, $\alpha_1 > 1$

тогда $\alpha_1 = q_2 + \frac{1}{\alpha_2}$ $\quad q_2$ – целое, даже $\mathbb{N}$

$\alpha_2 > 1$

$\alpha_2 = q_3 + \frac{1}{\alpha_3}$ $\quad q_3 \in \mathbb{N}$ $\alpha_3 > 1$

и т.д.

В итоге возникает ∞ непр. дробь

$$[q_1\, q_2\, q_3 \dots] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\dots}}}$$

Отметим, что по Th о соответствии

$$\alpha = [q_1; q_2 \dots q_{k-1}\, \alpha_{k-1}] =$$
$$= [q_1\, q_2 \dots q_k, \alpha_k]$$

Опр Числа $\delta_k = \frac{P_k}{Q_k} = [q_1 q_2 \dots q_k]$ —

— подх дробь к числу α

ЛЕММА: α расположена между двумя: k-ой и $k-1$-ой дробью (подх)

$\delta_{k-1} \quad \alpha \quad \delta_k$ $\longrightarrow$ k нечет $\longrightarrow$ k четн

док-во: рассмотр ф-ию

$$f(x) = [q_1 \dots q_{k-1}, x] =$$
$$= \frac{xP_{k-1} + P_{k-2}}{xQ_{k-1} + Q_{k-2}}$$

Очевидно, что

$$f(\alpha_{k-1}) = \alpha$$

$$\begin{cases} f(q_k) = \frac{P_k}{Q_k} = \delta_k \\ f\left(q_k + \frac{1}{\alpha_k}\right) = \alpha \\ f\left(q_k + \frac{1}{q_{k+1}}\right) = \frac{P_{k+1}}{Q_{k+1}} \end{cases}$$

итого: (проверить)

$$f'(x) = \frac{P_{k-1}(xQ_{k-1} + Q_{k-2}) - (xP_{k-1} + Q_{k-2})Q_{k-1}}{(xQ_{k-1} + Q_{k-2})^2} =$$

$$= \frac{(-1)^{k-1}}{(xQ_{k-1} + Q_{k-2})^2}$$

при $x \geq 0$ имеем: $\operatorname{sgn} f'(x) = (-1)^{k-1}$

Если k-четн $\Rightarrow (-1)$ $\quad f(x)$ мон $\downarrow$

нечет $\Rightarrow (+1)$ $\quad f(x)$ мон $\uparrow$

а) $q_k \quad q_k + \frac{1}{\alpha_k} \quad q_k + \frac{1}{q_{k+1}}$ $\Rightarrow$ $q_{k+1} < \alpha_k$

т.к. $\alpha_k = q_{k+1} + \frac{1}{\alpha_{k+1}}$

$\Rightarrow$ ф-ия мон$\uparrow$ при k-нех. $\quad f(q_k) = \delta_k$

$f\left(q_k + \frac{1}{q_{k+1}}\right) = \delta_{k+1}$

$\delta_k \quad \alpha \quad \delta_{k+1}$

б) k-четн.

$q_k \quad q_k + \frac{1}{\alpha_k} \quad q_k + \frac{1}{q_{k+1}}$ $\Rightarrow$ fn мон $\downarrow$ $\Rightarrow$ $\delta_{k+1} \quad \alpha_k \quad \delta_k$

$\Rightarrow$ $\delta_1 \quad \delta_3 \quad \delta_5 \quad \delta_6 \quad \alpha \quad \delta_4 \quad \delta_2$

Теорема 1. 1) Если $q_1 q_2 q_3 \ldots$ беск. цепн дробь, построенная по ир. числу α, то утв-ся, что α будет совпадать с пределом посл-сти δ_k.

$$\alpha = \lim_{k\to\infty} \delta_k$$

2) Если $[q_1' \ldots q_n']$ — нек беск цепн дробь

и $\lim_{k\to\infty} \delta_k' = \alpha$

т.к. $q_1 = q_1'$ $q_2 = q_2' \ldots$

Док-во: по лемме α расположена между сосед. подх дробями.

1) $|\delta_k - \delta_{k+1}| = \left|\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}}\right| = \frac{1}{Q_k Q_{k+1}} \to 0$ при $k \to \infty$

δ_{2k+1} — беск. воз. посл.

δ_{2k} — беск убыв посл.

2) Пусть усл вып, тогда

$q_1 = q_1' \ldots q_{k-1} = q_{k-1}'$

докажем, что $q_k = q_k'$

пусть $f(x) = [q_1 \ldots q_{k-1}, x] = [q_1', \ldots q_{k-1}', x]$

тогд f либо мон ↑ или ↓ в зав. от k

Имеем:

$\cancel{q_k < \alpha < q_{k+1}}$, ~~которые~~ $\quad \underset{\parallel}{q_k + \frac{1}{\alpha_k}}$

$\cancel{f(q_k)} \quad \cancel{f(q_k + \frac{1}{\alpha_k})} \quad \cancel{f(q_{k+1})}$

Поскольку

$$f\left(q_k + \frac{1}{\alpha_k}\right) = \alpha$$

$$f\left(q_k' + \frac{1}{\alpha_k'}\right) = \alpha$$

$\alpha = [q_1 q_2 \ldots] \Rightarrow \alpha = \lim_{k\to\infty} \frac{P_k}{Q_k}$

$[q_1' q_2' \ldots] \Rightarrow \alpha = \lim_{k\to\infty} \frac{P_k'}{Q_k'}$

$\Downarrow$

$q_i = q_i' \ \forall i$

индукция по k:

$k = 1$ $\quad q_1 = q_1'$?

$$\alpha = q_1 + \frac{1}{\underbrace{(q_2 + \ldots)}_{=\alpha_1}} = \qquad \alpha_1 = [q_2 q_3 \ldots]$$

$$= q_1' + \frac{1}{\alpha_1'} \qquad \alpha_1' = [q_2' q_3' \ldots]$$

$q_i \in \mathbb{Z}$, $q_i > 0$, $q_i \geq 1$ $\quad \alpha_1 = \underset{\geq 1}{q_2} + \frac{1}{\ldots} > 1$; $\alpha_1' > 1 \Rightarrow$

$\Rightarrow q_1 = [\alpha] = q_1'$

$q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots}}$

переход:

$k \to k+1$: $q_1 = q_1'$ $\quad q_k = q_k'$ — дано (1)

пусть $f(x) = [q_1 q_2 \ldots q_k, x]$, тогда

Здесь $\alpha_k = [q_{k+1} q_{k+2} \ldots]$ $\quad \alpha_k' = [q_{k+1}', q_{k+2}' \ldots]$

$\alpha = f(\alpha_k) = f(\alpha_k')$ в силу (1),

f — монот ↑ (строго) при $x > 1$

$q_k + \frac{1}{\alpha_k}$

$\Rightarrow \alpha_k = \alpha_k'$

$$\underset{\geq 1}{q_{k+1}} + \underset{< 1}{\frac{1}{\alpha_{k+1}}} = \underset{\geq 1}{q_{k+1}'} + \underset{< 1}{\frac{1}{\alpha_{k+1}'}}$$

$\Rightarrow q_{k+1} = q_{k+1}'$;