$$\left|\bigcup_{i=1}^{N} A_i\right| = \sum_{i=1}^{N}|A_i| - \sum_{1\le j<i\le N} |A_j \cap A_i| +$$

$$+ \sum_{1\le j<i<k\le N} |A_j \cap A_i \cap A_k| \ldots$$

т.е

$$\left|\bigcup_{i=1}^{N} A_i\right| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1\le i_1<\ldots<i_m\le N} \left|\bigcap_{k=1}^{m} A_{i_k}\right|$$

□ База: для $N=2$ работает ¨

Шаг: Пусть для $n \le N$ работает

тогда рассмотрим мн-во

$$A_{N+1}, \quad B = \bigcup_{i=1}^{N} A_i$$

(*)

$$|A_{N+1} \cup B| = |A_{N+1}| + |B| - |A_{N+1} \cap B|$$

По предп-ю индукции для

B:

$$|B| = \left|\bigcup_{i=1}^{N} A_i\right| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1\le i_1<\ldots<i_m\le N} \left|\bigcap_{k=1}^{m} A_{i_k}\right|$$

$$A_{N+1} \cap B = \bigcup_{i=1}^{N} (A_i \cap A_{N+1})$$

$$|B \cap A_{N+1}| = \left| \bigcup_{i=1}^{N} C_i \right| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \le i_1 < \ldots < i_m \le N} \left| \bigcap_{k=1}^{m} C_{i_k} \right| =$$

но $C_{i_k} = A_{i_k} \cap A_{N+1}.$

$$\Rightarrow \bigcap_{k=1}^{m} C_{i_k} = \bigcap_{k=1}^{m} (A_{i_k} \cap A_{N+1}) = \left(\bigcap_{k=1}^{m} A_{i_k} \right) \cap A_{N+1}$$

$$\Rightarrow |B \cap A_{N+1}| = \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \le i_1 < \ldots < i_m \le N} \left| \left(\bigcap_{k=1}^{m} A_{i_k} \right) \cap A_{N+1} \right| =$$

А теперь подставим в $(*)$:

$$(*) = |A_{N+1}| + |B| - |B \cap A_{N+1}| =$$

$$= |A_{N+1}| + \sum_{m=1}^{N} (-1)^{m+1} \sum_{1 \le i_1 < i_2 < \ldots i_m \le N} \left| \bigcap_{k=1}^{m} A_{i_k} \right| -$$

$$-\sum_{m=1}^{N}(-1)^{m+1}\sum_{1\le i_1<i_2<\dots<i_m\le N}\left|\left(\bigcap_{k=1}^{m}A_{i_k}\right)\cap A_{N+1}\right| =$$

$$=\sum_{m=1}^{N}(-1)^{m+2}\sum_{1\le i_1<\dots<i_m\le N}\left|\left(\bigcap_{k=1}^{m}A_{i_k}\right)\cap A_{N+1}\right|$$

] $s = m+1.$

$$\sum_{s=2}^{N+1}(-1)^{s+1}\sum_{1\le i_1<\dots<i_{s-1}\le N}\left|\bigcap_{k=1}^{s-1}A_{i_k}\cap A_{N+1}\right|.$$

Объединим:

$$\left|A \underset{N+1}{\cup} B\right| = \sum_{m=1}^{N}(-1)^{m+1}\sum_{1\le i_1<\dots<i_m\le N}\left|\bigcap_{k=1}^{m}A_{i_k}\right| +$$

$$+\left|A_{N+1}\right| + \sum_{s=2}^{N+1}(-1)^{s+1}\sum_{i<\dots<i_{s-1}}\left|\bigcap_{k=1}^{s-1}A_{i_k}\cap A_{N+1}\right|$$

Заметим, что первой суммой покрыты всевозм.-е непустые подмн-ва N эл-в. покрыты первой суммой, а $N+1$ – (вкл A_{N+1}) второй и третьей.

$$\Rightarrow \sum_{m=1}^{N+1}(-1)^{m+1}\sum_{1\le i_1<i_2<\dots<i_m\le N+1}\left|\bigcap_{k=1}^{m}A_{i_k}\right| \qquad \blacksquare$$

$$\frac{n!}{k_1!\,(n-k_1)!} \cdot \frac{(n-k_1)!}{k_2!\,(n-k_1-k_2)!}$$

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1} =$$

$$= \frac{(n-1)!^{\backslash (n-k)}}{k!\,(n-k-1)!} + \frac{(n-1)!^{\backslash k}}{(k-1)!\,(n-k)!} =$$

$$= \frac{(n-1)!\,(n-k) + (n-1)!\,k}{k!\,(n-k)!} = \frac{(n-1)!\,n}{k!\,(n-k)!} =$$

$$= \frac{n!}{k!\,(n-k)!} = C_n^k$$

$$\sum_{k=0}^{n} C_n^k = 2^n$$

$$(1+x)^n \sum_{k=0}^{n} C_n^k x^k = 2^n =$$

Возьмем $x = 1$.

$$\sum_{k=0}^{n} (-1)^k C_n^k = 0$$

$$(1+x)^n = \sum_{k=0}^{n} C_n^k x^k = 0$$

$x = -1$

КТО

Пусть $a_1, a_2, \dots, a_n$ попарно взаимно простые числа, $r_1, r_2 \dots r_n : 0 \le r_i < a_i$.
Тогда: $\exists N : \forall i \in \{1, 2, \dots n\} \hookrightarrow N \equiv r_i \pmod{a_i}$
Если N_1, N_2 - реш-я системы, то $N_1 \equiv N_2 \pmod{a_1 \cdot a_2 a_3 \dots a_n}$

$\square$ База: $n = 1$ $\exists N_1 : N_1 \equiv r_1 \pmod{a_1}$ и $\exists N_2$, то $N_1 \equiv N_2 \pmod{a_1}$.

Шаг: Пусть утв-е вып-ся для $n \le k$. Рассмотрим $n = k+1$.

По предположению инд-ции:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ x \equiv r_3 \pmod{a_3} \\ \vdots \\ x \equiv r_k \pmod{a_k} \end{cases}$$

N - решение системы.

Возьмем $d = a_1 \cdot a_2 \cdot \dots \cdot a_k$.

Запишем числа: $N, N+d, N+2d, \dots, N + (a_{k+1} - 1)d$. Заметим, что все эти числа имеют разный остаток при делении на a_{k+1}

От противного: $N + jd \equiv N + id \pmod{a_{k+1}}$

$\Rightarrow jd \equiv id \pmod{a_{k+1}} \Rightarrow j \equiv i \pmod{a_{k+1}}$

Противоречие. $\Rightarrow$ все $|a_{k+1}|$ число - ост-ки при дел на a_{k+1}.

Значит, среди них найдется такое $N + jd = r_{k+1}$. Заметим, что $\forall i \in \{1, \dots, k\}$

$\Rightarrow N + jd \equiv r_i \pmod{a_i}$, т.к. $d \vdots a_i$

Пусть $\exists N_1, N_2$ подходят.

Но тогда $\forall i \in [1,k]$:
$$N_1 \equiv r_i \pmod{a_i}$$
$$N_2 \equiv r_i \pmod{a_i}$$

$$\Rightarrow N_1 - N_2 \equiv 0 \pmod{a_i}$$

$$\Rightarrow N_1 - N_2 \equiv 0 \pmod{d}$$
$$N_1 - N_2 \equiv 0 \pmod{a_{k+1}}$$

■

И прополнятся 20-е годы...

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

k \ n	1	1.	1	1
1	2	3	4	5
1	3	6	10	15
1	4	10	20	35
1	5	$\boxed{15}$	35	
1	6	21		

n, k

1 1

1 2 1

1 3 3 1

1 4 6 4 1

Числа Фибоначчи $0, 1, 1, 2, 3, 5, \dots$

$F_n = F_{n-1} + F_{n-2}$ Порядок – 2.

нет свободного члена

Лин. однор. рекур. ур-е порядка k — это ур-е, задающее посл-ть $\{a_n\}$, в которой каждый член послед-ти $(n \geq k)$ выр-ся или линейной комбинации к пред-х членов с пост. коэф-ми, и свободного член отсутств-т

$$a_n = c_1 \cdot a_{n-1} + c_2 a_{n-2} + \dots c_k \cdot a_{n-k},$$

- $c_1, \dots c_k = const$, $c_i \neq 0 \ \forall i \in \{1, \dots k\}$

Числа Фибоначчи - лин однор-е ур-е порядка 2 с коэф. $c_1 = 1$, $c_2 = 1$.

$r^n = r^{n-1} + r^{n-2} \quad | : r^{n-2}$

Характер-ское ур-е: $r^2 = r + 1$

$r^2 - r - 1 = 0$.

$D = 1 + 4 = 5 = \sqrt{5}^2$. $\Rightarrow r = \frac{1 \pm \sqrt{5}}{2}$

$\varphi = \frac{1+\sqrt{5}}{2}$, $\psi = \frac{1-\sqrt{5}}{2}$

$$F_n = A \cdot \varphi^n + B\psi^n$$

$\underline{n=0}$: $A + B = 0$

$\underline{n=1}$: $A\varphi + B\psi = 1$

$\Rightarrow A\varphi - A\psi = 1$

$A(\varphi - \psi) = 1$

$\frac{1 + \sqrt{5} - 1 + \sqrt{5}}{2} = \sqrt{5}$

$\Rightarrow A = \frac{1}{\sqrt{5}}$, $B = -\frac{1}{\sqrt{5}}$

$$\Rightarrow F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

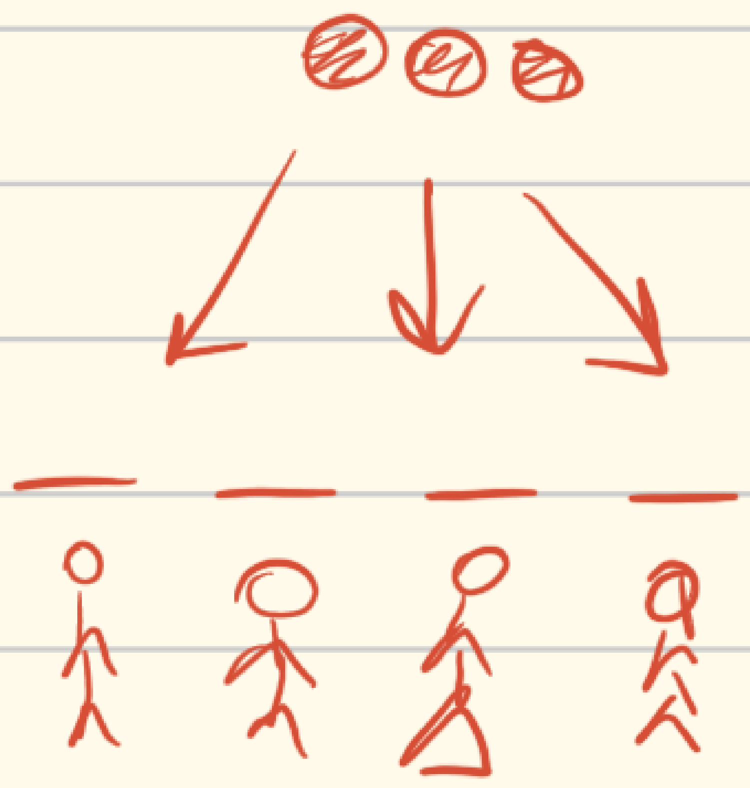
Еще пример: $x_{n+2} = 3x_{n+1} + 4x_n$

$\lambda^2 = 3\lambda + 4$.

$\lambda^2 - 3\lambda - 4 = 0$ $\quad D = 9 + 16 = 25 = 5^2$

$$\lambda = \frac{3 \pm 5}{2} = \left[\begin{array}{l} 4 \\ -1 \end{array}\right.$$

Task 1. $C_8^4 \cdot 4^3$



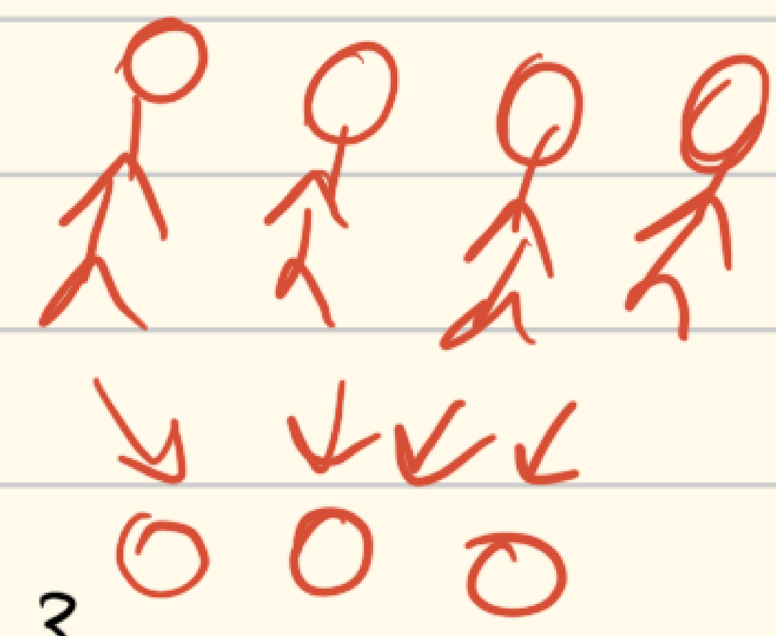
3^2

Но НЕ НАОБОРОТ!

$21 \times 8 = 168$

$600 : 28$: -42, 180

$600 : 35 = 17$: -35, 250



типа 4 чела на 1 роль? лол.

$35 \times 7 = 245$

Task 2

Числа от 1 до 600, которые делятся на 3, 5, 7 (или)

$600 : 7$: -56, 40

$$\frac{600}{3} = 200 \qquad \frac{600}{15} = 40 \qquad \frac{600}{105} = 5$$

$$\frac{600}{5} = 120 \qquad \frac{600}{35} = 17$$

$$\frac{600}{7} = 87 \qquad \frac{600}{21} = 28$$

$70 + 80$ $\qquad 2 - 2$

$320 + 87 - 40 - 17 - 28 + 5 = 327 - 2 =$

$= \underline{325}.$

В худшем случае мы вытащим
4 и они все разные будут
$\Rightarrow 5$

а) $(2-3x)^{10} = \sum\limits_{k=1}^{10} C_{10}^{k}\,(-3x)^{k}\cdot 2^{n-k}$

~~при~~ $k=7$

$$C_{10}^{7}\,(-3)^{7}\cdot x^{7}\cdot 2^{3} =$$

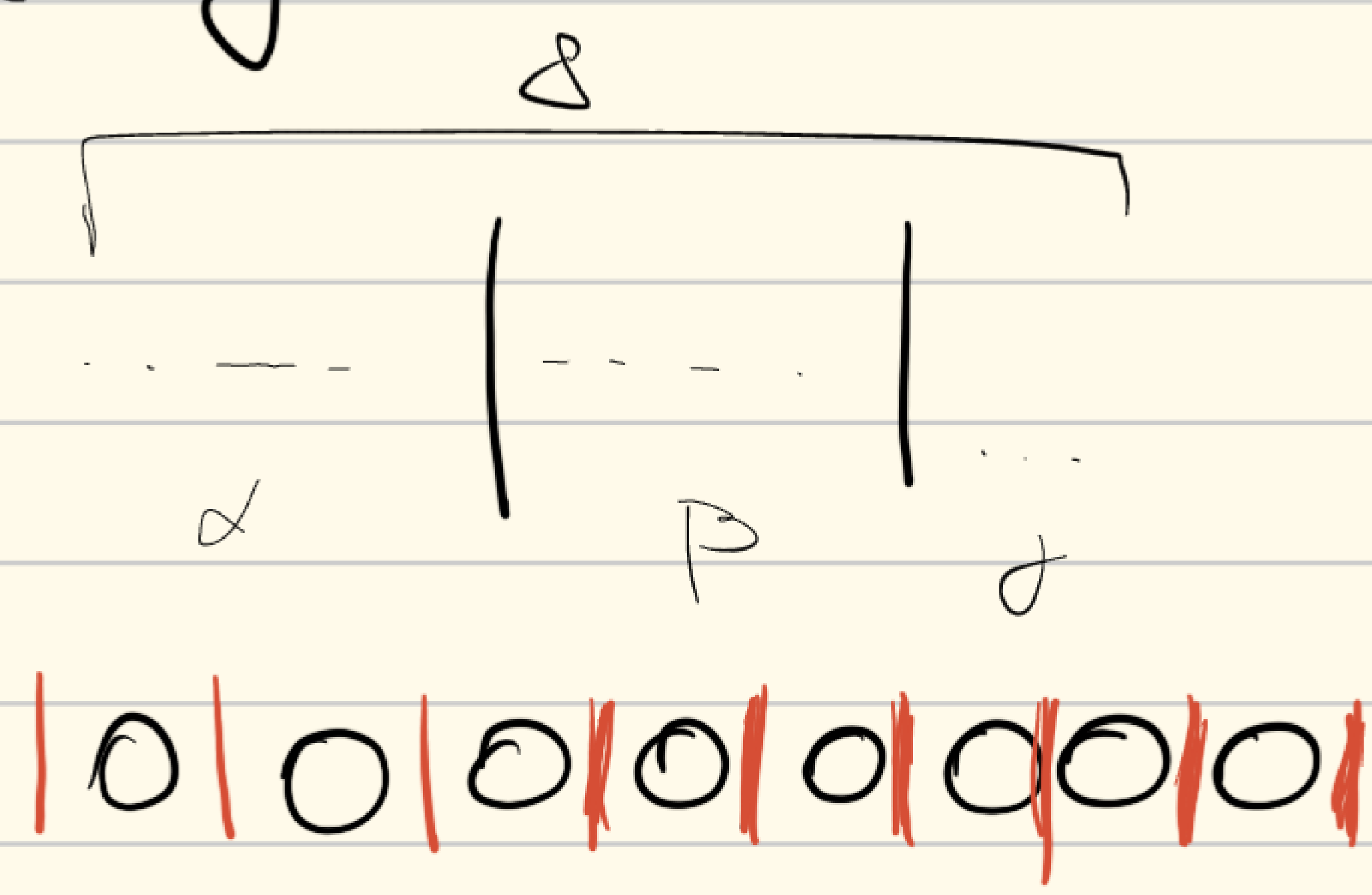
$$= \frac{10!}{7!\,3!}\cdot(-3)^{7}\cdot 8$$

б) Сколько разл. слагаемых $x^{\alpha}y^{\beta}z^{\gamma}$ появится при раскрытии скобок в выр-нии $(x+y+z)^{8}$

Имеем 8 скобок:

$$(x+y+z)(x+y+z)\dots$$

$\alpha+\beta+\gamma=8.$



Теория Групп

$G = (M, \circ)$ "$\circ$": $M \times M \to M$

1) ассоц-ть: $\forall a, b, c \in G \hookrightarrow (a \circ b) \circ c = a \circ (b \circ c)$.
2) $\exists e \in G: \forall a \in G \hookrightarrow e \circ a = a \circ e = a$
3) $\forall a \in G \; \exists a^{-1} \in G: a \circ a^{-1} = a^{-1} \circ a = e$
4) $\forall a, b \in G \hookrightarrow a \circ b = b \circ a$ - абелевость.

Кольцо $G = (M, +, \circ)$, если:

1) коммут-на по +
2) ассоц-вна по $\circ$
3) дистрибутивность $\forall a, b, c \hookrightarrow a \circ (b + c) = a \circ b + b \circ c$

Пример: $(\mathbb{Z}m, +_{\mathrm{mod}\, m}, \cdot_{\mathrm{mod}\, m})$ – кольцо

Поле $G = (M, +, \circ)$ - это, когда:
1) коммутативна по +
2) $M \setminus \{0\}$ коммут-на по $\circ$ ($(M \setminus \{0\}, \circ)$ обр. группу по $\circ$, причем абелеву)
3) дистрибутивность

Пример: $\mathbb{R}$.

Порядок группы - кол-во эл-в в ней. $\left(\mathbb{Z}_k, +_{\mathrm{mod}\, k}\right)$ $\mathrm{ord}(G) = k$
" G

$(a \circ b) \circ c = a \circ (b \circ c)$ - мультипл.
$(a + b) + c = a + (b + c)$ - адд-ное

Таблица Кэли - таблица для записи рез-в применения операции ко всем парам эл-в.

$\circ$	e	a
e	e	a
a	a	e

Note: $\forall$ группа порядка 2 изоморфны

Порядок эл-та - это наим. целое $m \in \mathbb{N}_0$, т., что $a^m = e$ $(a \in G)$.

В конечной группе порядки эл-в конечны.

Рассм. степени эл-та a: $a^1, a^2, \dots$ Т.к. G- группа, то все степени a лежат в G. Пусть $|G| = N$. $a^1, a^2, \dots a^{N+1}$. Все лежат в G, но там всего N эл-в, а у нас $N+1$. $\Rightarrow$ по принципу Дирихле $\exists i,j \in [1, N+1]: a^i = a^j \mid \cdot a^{-i}$

$a^j \cdot a^{-i} = e \Rightarrow a^{j-i} = e$.

$j - i \geq 1. \Rightarrow j - i = m$

Гомоморфизм.

Def **Гомоморфизм** групп из группы G в G' - это такое отображение φ:

$$\varphi: G \to G', \quad G = (M, \circ)$$
$$G' = (M', *)$$

что $\forall a, b \in G \hookrightarrow \varphi(a \circ b) = \varphi(a) * \varphi(b)$.

Свойства гомоморфизма:

1) $\varphi(e) = e'$
2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3) $a^m = e \Rightarrow \varphi(a^m) = e'$
$\varphi(a)^m = e'$ (по опр. гомоморфизма)

① $\forall a \in G \hookrightarrow \varphi(a \circ e) =$
$= \varphi(a) * \varphi(e) =$
$= \varphi(e) * \varphi(a) = \varphi(e \circ a)$
$\Rightarrow \varphi(e) = e'$

порядок элемента $\varphi(a)$ явл-ся делителем порядка эл-та a.

② $\forall a \in G \hookrightarrow$
$\varphi(a \circ a^{-1}) = \varphi(a) * \varphi(a^{-1}) =$
$= \varphi(a^{-1}) * \varphi(a) = \varphi(a^{-1} \circ a)$
$\varphi(a \circ a^{-1}) = e'$

1. $a^n = e$, $n = |a|$ - наим. $\in \mathbb{N}_0$
2. $\varphi(a)^n = \varphi(a^n) = \varphi(e) = e'$
3. $x = \varphi(a)$ в гр. H удовл. условию:
$x^n = e'$
4. Если для эл-та x в группе выполнено $x^k = e$, то порядок $ord(x)$ делит k.

Пусть $ord(x) = m$
$\Rightarrow k = m \cdot q + r, \ 0 \le r < m.$

$\Rightarrow e = x^k = x^{m \cdot q + r} = x^r$

т.к. $r < m$ и $x^r = e$, то по минимальности m получаем $r = 0$. $\Rightarrow m$ - делитель k.

Пример: $ord(a) = 6$, но $a^3 \in \ker\varphi$.
$\varphi(a)^3 = \varphi(a^3) = e'$
$ord(\varphi(a)) = 3$, либо делителем 3, если a^1 или a^2 тоже лежат в $\ker\varphi$

$ord(a) \vdots ord(\varphi(a))$

Сюръективность гомоморфизм

$\varphi: G \to G'$ такой, что:

$\forall b \in G' \hookrightarrow \exists a \in G: \varphi(a) = b.$

т.е. $\mathrm{Im}\varphi = G' = \varphi(G)$

Изоморфизм $\cong$ - гомоморфизм, явл-ся биекцией.

Св-во: $\varphi: G \to G', \ \psi: G' \to G$

Теорема Кэли

Пусть G - конечная группа, $|G| = N$.

$\exists H < S_n : G \cong H$. Всякая конечная группа изоморфна некоторой подгруппе группы перестановок из n элементов.

$\square$ Пронумеруем элементы $g_1, g_2, \dots g_N$
Рассмотрим левые сдвиги $L_a, a \in G$.

$g_1 \to a g_1$
$g_2 \to a g_2$
$\vdots$
$g_N \to a g_N$

Все эл-ты лежат в G.
Они все различны.
$\square$ Пусть $ag_1 = ag_2 \mid \cdot a^{-1}$ слева
$g_1 = g_2$. против-е $\blacksquare$

L_a - перестановка эл-в $g_1 g_2 \dots g_N$
Рассмотрим $\forall a \in G$ L_a и заметим, что они обр-т перестановку:

1) L_e - тождеств-я перестановка по опр
2) $\forall a, b \in G \hookrightarrow L_a \circ L_b = L_{ab}$ по опр.
3) $\forall a \in G \ \exists a^{-1} \in G \Rightarrow L_a \circ L_{a^{-1}} = L_e$
4) $\forall a, b, c \in G \hookrightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c) \Rightarrow$

$$L_a \circ (L_b \circ L_c) = L_a \circ L_{bc} = L_{abc} = L_{ab} \circ L_c = (L_a \circ L_b) \circ L_c$$

Докажем, что эта группа изоморфна G. Действительно, мы доказали, что L_a - это биекция $\forall a \in G$. А также доказали, что $L_a \circ L_b = L_{ab} \Rightarrow$ по опред-ю $G \cong L_G$. т.к. $|L_G| = N$ и $L_G < S_N$, а также L_G - группа отн-но той же групповой операции, что и S_n (т.е. отн-но композиции) $\hookrightarrow$ то чтд $\blacksquare$

Группа перестановок

Перестановка – биекция конечного мн-ва на себя.

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \dots & N \\ \pi(1) & \pi(2) & \pi(3) & & \pi(N) \end{pmatrix}$$

$$\sigma \circ \pi := \begin{pmatrix} 1 & 2 & \dots & N \\ \sigma(\pi(1)) & \sigma(\pi(2)) & & \sigma(\pi(N)) \end{pmatrix}$$

Циклом длины K перестановки длины n назовем послед-ть эл-в, где каждый переходит в след-й, а последний – в первый.

$$(a_1\ a_2 \dots a_k) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$$

Note Цикл – это биекция K-эл-го мн-ва на себя. => это эл-т группы перестановок.

Подгруппы

$H < G$, если H — гр. отн. той же операции и $H \subseteq G$.

$$\Updownarrow$$

$$\begin{cases} H \subseteq G \\ \forall a, b \in H \hookrightarrow a \circ b \in H \\ \forall a \in H \hookrightarrow a^{-1} \in H \end{cases}$$

Критерий $H < G$

$$H < G \iff \begin{cases} \forall a, b \in H \hookrightarrow a \circ b^{-1} \in H \\ H \subseteq G \end{cases}$$

Теорема

Пусть дана произвольная группа G и $\exists\, a \in G:\ \operatorname{ord}(a) = n \in \mathbb{N}$.

Тогда $H := \{a^0, a^1, \dots a^{n-1}\} < G$.

$\square$ $H \subseteq G$, т.к. все степени $a \in G$ по опр. Применим критерий подгруппы:

$$\forall i, j \in \mathbb{N}_0 \hookrightarrow a^i \cdot a^j = a^{i+j} \in H.$$

$$a^{i+j} = a^n \cdot a^r = a^r,\ \underset{\geq 0}{r} \leq n-1$$

$$\forall a^i \in H\ \exists a^{n-i}:\ a^i \cdot a^{n-i} = a^0 = e. \blacksquare$$

Смежные классы

<u>Def</u> Пусть $H < G$. Возьмем $g \in G$.

Б.г., что gH – левый смежный класс с представителем g, если

$$gH = \{g \circ h \mid h \in H\}$$

<u>St</u>. Смежные классы не пересек-ся или совп-ют.

□ Пусть $\exists z \in aH \cap bH$. =>

$\exists h_a;\ h_b \in H$: $z = a \circ h_a = b \circ h_b$

$$a \circ h_a = b \circ h_b \quad \Big| \cdot h_a^{-1} \text{ справа}$$

$$a = b \circ \underbrace{h_b \circ h_a^{-1}}_{\in H} = b \circ \tilde{h}_1$$

$$\in H \Rightarrow h_b \circ h_a^{-1} = \tilde{h}_1$$

$\forall t \in aH \hookrightarrow t = a\tilde{h}_2 = b\tilde{h}_1 \circ \tilde{h}_2 = b\tilde{h}_3$

=> $t \in bH$. Значит, классы совпали ■

$\mathbb{Z} > 3\mathbb{Z}$. Смеж. классы по $3\mathbb{Z}$:

$0 + 3\mathbb{Z}$

$1 + 3\mathbb{Z}$

$2 + 3\mathbb{Z}$

Теорема Лагранжа

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

число левых (правых) смеж. классов.

□ 1) $|gH| = |H|$

2) $\forall g \in G \hookrightarrow g \in gH$ $(e \in H)$

3) смеж. классы не пересек. или совпадают. ■

Норм. подгр-па $H \triangleleft G$, если $\forall g \in G \hookrightarrow$
$\longleftrightarrow gH = Hg$.

элементы не обязаны коммутировать!

Фактор группа

Рассм. $H \triangleleft G$. Введем операцию:

$$(aH) * (bH) = (a \circ b)H$$

St. Мн-во смеж. классов обр. группу отн. этой операции G/H

□ $\forall a, b, c \in G \hookrightarrow (aH) * (bH) * (cH) =$
$= (aH) * ((b \circ c)H) = (a \circ b \circ c)H = ((a \circ b)H) * cH$
по наследованной от G ассоц-ти.

eH - нейтр. $(eH) * (bH) = (e \circ b)H = bH$.

$\forall a \in G \; \exists a^{-1} \in G \Rightarrow (aH) * (a^{-1}H) =$
$= eH$. Нормальность нужна.

чтобы не зависеть от представителя: $a_1 \in aH = a_1H$.

$\square$ $(a_1H) * (b_1H) = (a_1 \circ b_1)H$.
Покажем, что $(a_1 \circ b_1)H = (a \circ b)H$

Покажем что $(a_1 \circ b_1) \in (a \circ b)H$.

$a_1 \in aH,\quad b_1 \in bH \Rightarrow \exists h_1, h_2:$
$a_1 = ah_1,\ b_1 = bh_2$

$$\Rightarrow a_1 \circ b_1 = a \circ \underbrace{h_1 \circ b}\circ h_2$$

Вспоминаем, что $H \triangleleft G \Rightarrow$
$\forall g \in G \hookrightarrow gH = Hg \Rightarrow$
$\forall h \in H\ \exists \tilde{h} \in H:\ h \circ b = b \circ \tilde{h}$
Найдём $\tilde{h}_1 \in H:\ h_1 \circ b = b \circ \tilde{h}_1$

$$\Rightarrow a_1 \circ b_1 = a \circ b \circ \underbrace{\tilde{h}_1 \circ h_2}_{\in H}$$

$\Rightarrow a_1 \circ b_1 \in (a \circ b)H$. $\blacksquare$

Def Образ гомоморфизма $\operatorname{Im}\varphi = \varphi(G)$

Теорема $\operatorname{Im}\varphi = \varphi(G) < G'$

$\square$ Из опред-я $\operatorname{Im}\varphi \subseteq G'$. Применим критерий подгруппы. Рассм-м $c, d \in \varphi(G)$:
по опр образа $\exists a, b \in G:\ \varphi(a) = c,\ \varphi(b) = d$

Рассм-м $(c * d^{-1})$:

$$c * d^{-1} = \varphi(a) * \varphi(b^{-1}) = \varphi(a \circ b^{-1}) \in \operatorname{Im}\varphi$$

$\Rightarrow \operatorname{Im}\varphi < \varphi(G)$ по крит-ю $\blacksquare$

Def Ядро гомоморфизма $\operatorname{Ker}\varphi = \{g \mid g \in G, \varphi(g) = e'\}$

Теорема $\operatorname{Ker}\varphi < G$.

□ По опред-ю $\operatorname{Ker}\varphi \subseteq G$
Тогда по крит-ю подгруппы $\forall a, b \in \operatorname{Ker}\varphi \longleftrightarrow$
$\longleftrightarrow a * b^{-1} \in \operatorname{Ker}\varphi$.

Рассм-м
$a, b \in \operatorname{Ker}\varphi$. $\varphi(a) = e$
$\varphi(b^{-1}) = (\varphi(b))^{-1} = e^{-1} = e$.

$\Rightarrow b^{-1} \in \operatorname{Ker}\varphi$. Тогда $a * b^{-1} \in \operatorname{Ker}\varphi$.

$\Rightarrow \operatorname{Ker}\varphi < G$. ■

Теорема $\operatorname{Ker}\varphi \triangleleft G$

$gH = Hg \quad | \cdot g^{-1}$ спр.
$gHg^{-1} = H \Rightarrow$
$\forall h \in H \hookrightarrow ghg^{-1} \in H$

□ Уже док-ли, что $\operatorname{Ker}\varphi < G$.
Рассм $g \in G$. $g\operatorname{Ker}\varphi$
$|g\operatorname{Ker}\varphi| = |(\operatorname{Ker}\varphi)g| = |\operatorname{Ker}\varphi|$

Пусть $t \in g\operatorname{Ker}\varphi$. $\Rightarrow$
$\exists h \in \operatorname{Ker}\varphi$: $t = g \circ h$
Рассм-м $g \circ h \circ g^{-1}$
$\varphi(g \circ h \circ g^{-1}) = \varphi(g) * g(h) * g(g^{-1})$
Заметим, что $\varphi(h) = e'$, ведь $h \in \operatorname{Ker}\varphi$.
$\Rightarrow \varphi(g) * e' * (\varphi(g))^{-1} = e'$

$\Rightarrow g \circ h \circ g^{-1} \in \operatorname{Ker}\varphi$. $| \cdot g$ справа

$g \circ h \in \operatorname{Ker}\varphi \circ g$

$\begin{cases} t \in \operatorname{Ker}\varphi \circ g. \\ t \in g\operatorname{Ker}\varphi \end{cases}$ Но t и g были выбраны
произвольно $\Rightarrow \operatorname{Ker}\varphi \triangleleft G$ ■

Уже почти...

Рассмотрим $G/\operatorname{Ker}\varphi$

St. $a, b \in G$, $a, b \in$ одному смеж. классу $\operatorname{Ker}\varphi$ $\Leftrightarrow$ их образы совпадают.

т.е $a, b \in g\operatorname{Ker}\varphi \Leftrightarrow \varphi(a) = \varphi(b)$.

т.е. $\varphi(g) \Leftrightarrow g\operatorname{Ker}\varphi$

$\Rightarrow$

$\square$ Рассмотрим произв-е $a, b \in g\operatorname{Ker}\varphi$

$\exists h_a, h_b \in \operatorname{Ker}\varphi$: $a = gh_a$, $b = gh_b$

Но тогда $\varphi(a) = \varphi(g \circ h_a) = \varphi(g) * \varphi(\underset{e'}{h_a})$

$\varphi(b) = \varphi(g \circ h_b) = \varphi(g) * \varphi(\underset{e'}{h_b})$

$\Leftarrow$

Пусть $\varphi(a) = \varphi(b)$. Тогда расс-м:

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

$\Rightarrow (a \circ b^{-1}) \in \operatorname{Ker}\varphi$.

$$a = (a \circ b^{-1}) \circ b \in (\operatorname{Ker}\varphi) b = b(\operatorname{Ker}\varphi)$$

$e \in \operatorname{Ker}\varphi \quad | \cdot a$

$\begin{cases} a \in a\operatorname{Ker}\varphi \\ a \in b\operatorname{Ker}\varphi \end{cases} \Rightarrow a, b \in a\operatorname{Ker}\varphi$.

$\blacksquare$

теорема о гомо что-то там...

Теорема

$$\mathrm{Im}\,\varphi \cong G/\mathrm{Ker}\,\varphi.$$

Гомоморфный образ группы изоморфен фактор-группе по ядру гомоморфизма!

□ Док-м биекцию между $\mathrm{Im}\,\varphi$ и $G/\mathrm{Ker}\,\varphi$.

$$f: \varphi(g) \longleftrightarrow g\,\mathrm{Ker}\,\varphi$$

$$F(\varphi(g)) = g\,\mathrm{Ker}\,\varphi$$

$$F(\varphi(a) * \varphi(b)) = F(\varphi(a \circ b)) = (a \circ b)\,\mathrm{Ker}\,\varphi.$$

$$F(\varphi(a)) \times F(\varphi(b)) = a\,\mathrm{Ker}\,\varphi \times b\,\mathrm{Ker}\,\varphi = (a \circ b)\,\mathrm{Ker}\,\varphi.$$

$$\Rightarrow f(\varphi(a) * \varphi(b)) = f(\varphi(a)) \times f(\varphi(b)).$$

$\Rightarrow f$ - гомоморфизм.

Но f - биекция $\Rightarrow$ изоморфизм. ■