Повторение.

1. $n\mathbb{Z} < \mathbb{Z}, +; a \sim b \leftrightarrow -a + b \in n\mathbb{Z} \leftrightarrow b \in a + n\mathbb{Z}$

   $T_a = \{b : a \sim b\} = a + n\mathbb{Z} = \{a, a+n, a-n, a+2n, a-2n, \dots\}$

   $T_a = [a]_n = \bar{a}_n = [a] = \bar{a} = a$

   $[a] + [b] = [a+b]$

   $[a][b] = ab$

   Теорема 1 $\left.\begin{matrix} a \sim a' \\ b \sim b' \end{matrix}\right\} \rightarrow \begin{cases} [a'+b'] = [a+b] \\ [a'b'] = [ab] \end{cases}$

   ◀$a' = a + nl; b' = b + nk$
   $a' + b' = a + b + n(l+k) \rightarrow [a'+b'] = [a+b]$
   $a'b' = ab + n(ak + bl + nlk) \rightarrow [a'b'] = [ab]$▶

2. $H < G, \cdot$

   Теорема 2 $|T_x| = |T_z| = |H|$

   ◀$xh_1 = xh_2 \rightarrow h_1 = h_2$▶

   Теорема 3 (Теорема Лагранжа) *Если* $|G| = n < \infty \rightarrow |G| \vdots |H|$

   ◀▶

   Следствие из теоремы Лагранжа: $|G| \vdots |x|$

   ◀$x \rightarrow H =< x >, |H| = |x|$▶

$\mathbb{Z}, n\mathbb{Z} \rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{n-1}\}$- кольцо остатсков при делении на n

Теорема 4 $\mathbb{Z}_n$*-поле* $\leftrightarrow n$*-простое*

◀▶

Теорема 5 $\mathbb{Z}_n$ $k-$*обратим в* $\mathbb{Z}_n \leftrightarrow n$ *и* k*-взаимно просты* $\big\{(n,k) = 1\big\}$

Определение 1 *Функция Эйлера*$\{\varphi(n)\}$ *равна количеству натуральных чисел, меньших чем* n *и взаимно простых с* n.

Определение 2 S_n*-группа подстановок(так же называют симметричной группой)*
$x = \{1, 2, 3, \ldots, n\}$, S_n*-мн-во биективных функций* $\varphi : X \to X$
$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ \varphi(1) & \varphi(2) & \varphi(3) & \varphi(4) & \ldots & \varphi(n) \end{pmatrix}$

Примеры: $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$
$\varphi(1) = 2, \varphi(2) = 4, \varphi(3) = 3, \varphi(4) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$
$(\varphi\phi)(1) = \varphi(\phi(1)) = \varphi(4) = 1$
$\varphi^{-1}\varphi = \varphi\varphi^{-1} = e$
$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$
$\varphi^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 3 \\ 4 & 1 & 3 & 2 \end{pmatrix}$
S_n-группа $\quad |S_n| = n!$
Цикл
$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124)(3) = (3)(124)$
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) = (34)(12)$

Независимые циклы-называются циклы, если числа входят в один цикл, но не входят во второй цикл.

Теорема 6 *Независимые циклы коммутируют друг с другом (или* α, β*-независимые циклы* $\to \alpha\beta = \beta\alpha$ *)*

Определение 3 *Циклом длины два называется транспозиция.*

Теорема 7 *Если* $\alpha = (i_1, i_2, \ldots, i_k)$*-цикл длины* $k \to |\alpha| = k$

Теорема 8 *Пусть* $\varphi = \alpha_1\alpha_2 \ldots \alpha_n$*- произведение независимых циклов.*
$\alpha_1 = (i_1, i_2, \ldots, i_k)$
$\alpha_2 = (j_1, j_2, \ldots, j_l) \to |\varphi| = HOK(|\alpha_1|, |\alpha_2|, \ldots, |\alpha_m|)$