# 1 Первообразные корни

$\mathbb{G}$ — группа, $\mathbb{Z}$ — группа, $\mathbb{Z}/\mathrm{m}\mathbb{Z}$ — группа по "+", $\mathbb{H} \subset \mathbb{G}$ подгруппа.

**Обозн:** $\mathbb{H} < \mathbb{G}$.

**Лемма 1.** $\mathbb{H} < \mathbb{G}$, *отношение* $a \sim b <=> \exists h \in \mathbb{H} : a = bh$ *является отношением эквивалентности.*

**Лемма 2.** $\mathbb{H} < \mathbb{G}$, $|\mathbb{H}| < \infty => \forall a, b \in \mathbb{G} : |a\mathbb{H}| = |b\mathbb{H}| = |\mathbb{H}|$

**Определение 1.** $\mathbb{H} < \mathbb{G}$, *если число классов эквивалентности конечно, то оно называется индексом* ($[\mathbb{G} : \mathbb{H}]$).

**Лемма 3.** $|\mathbb{G}| < \infty$, $\mathbb{H} < \mathbb{G} => |\mathbb{G}| = [\mathbb{G} : \mathbb{H}] \cdot |\mathbb{H}|$.

**Определение 2.** *Группа называется циклической, если порождается единственным элементом,* $\mathbb{G} =< a >$.

$\forall g \in \mathbb{G}$, $g = a^k$.

**Определение 3.** *Конечным порядком элемента* $a \in \mathbb{G}$ *называется ннаименьшее* $n \in \mathbb{Z} : a^n = e, n = \operatorname{ord} a$.

**Лемма 4.** $\mathbb{G} =< g >$ — *конечная циклическая группа.*
0) $\operatorname{ord} g = |\mathbb{G}|$;
1) $\forall \mathbb{H} < \mathbb{G}$, $\mathbb{H}$ — *циклическая;*
2) $k \in \mathbb{Z}_+$, $\mathbb{H} =< g^k > => |\mathbb{H}| = \frac{m}{(m,k)}$, $m = |\mathbb{G}|$;
3) $\forall d|m \ \exists! \ \mathbb{H} < \mathbb{G}$, $|\mathbb{H}| = d$, $\forall f|m \ \exists! \ \mathbb{H} < \mathbb{G} : [\mathbb{G} : \mathbb{H}] = f$;
4) $d|m => \exists \ \varphi(d)$ *элементов порядка* $d$;
5) $\exists \ \varphi(m)$ *порождающих(образующих) группу* $\mathbb{G}$, $\mathbb{G} =< g^k >$, $(k, m) = 1$.

**Определение 4.** $f : \mathbb{G}_1 \to \mathbb{G}_2$ — *гомоморфизм, если сохраняет структуру группы (т.е.* $f(e_1) = e_2, f(g_1g_2) = f(g_1)f(g_2)$ *и т.д.).*

**Определение 5.** $\ker f = \{a \in \mathbb{G}_1 : f(a) = e_2\}$, *где* $e_2$ — *единичный элемент в* $\mathbb{G}_2$.

**Пример.** $f : a \to a \bmod n$, как $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
$\ker f = (n)$.

**Лемма 5.** $\ker f < \mathbb{G}$, *причём если* $a \in \mathbb{G}, b \in \ker f$, *то* $aba^{-1} \in \ker f$.

**Определение 6.** $\mathbb{H} < \mathbb{G}$ *называется нормальной, если* $\forall a \in \mathbb{G}, b \in \mathbb{H} : aba^{-1} \in \mathbb{H}$ *(Обозн.* $\mathbb{H} \triangleleft \mathbb{G}$*).*

**Лемма 6.** 1) $\mathbb{H} < \mathbb{G}$ — *нормальная, если* $\forall a \in \mathbb{G} : a\mathbb{H}a^{-1} = \mathbb{H}$;
2) $\mathbb{H} < \mathbb{G}$ — *нормальная* $<=> \forall a : a\mathbb{H} = \mathbb{H}a$.

**Следствие 1.** *Если* $\mathbb{H} < \mathbb{G}$ — *нормальная, то* $\{a\mathbb{H}\}$ — *группа (Обозн.* $\mathbb{G}/\mathbb{H}$*)* $((a\mathbb{H}) \cdot (b\mathbb{H}) = ((ab)\mathbb{H}))$.

**Лемма 7.** $|\mathbb{G}| < \infty$, $\mathbb{H}$ — *нормальная* $=> |\mathbb{G}/\mathbb{H}| = [\mathbb{G} : \mathbb{H}] = \frac{|\mathbb{G}|}{|\mathbb{H}|}$.

**Теорема 1.** *(о гомоморфизме) Если* $f : \mathbb{G} \to \mathbb{H}$ *— гомоморфно, сюрьективно* $=> \mathbb{G}/\ker f \cong \mathbb{H}$.

**Теорема 2.** *(версия для колец) Если* $\psi : \mathbb{R} \to \mathbb{S}$ *— гомоморфизм колец* $=> \ker\psi$ *— идеал* $\mathbb{R}$, $\operatorname{Im}\psi$ *— подкольцо* $\mathbb{S}, \cong \mathbb{R}/\ker\psi$*; если* $\psi$ *— сюрьективно, то* $\mathbb{S} \cong \mathbb{R}/\ker\psi$.

**Теорема 3.** *(КТО)* $(m_i, m_j) = 1$, $1 \leq i \neq j \leq t$, $m = m_1 \cdot ... \cdot m_t$,
$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_t\mathbb{Z}$.

*Доказательство.*

$$\psi_i = \begin{cases} \mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}; \\ a \mapsto a \bmod m_i. \end{cases}$$

$\psi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_t\mathbb{Z}$;
$\psi(a) = (\psi_1(a), ..., \psi_t(a))$;
если $(b_1, ..., b_t) \in \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_t\mathbb{Z}$, то КТО: $\exists a \in \mathbb{Z}$ :

$$\begin{cases} a \equiv b_1(m_1) \\ \vdots \\ a \equiv b_t(m_t) \end{cases},$$

$\psi$ — сюръекция;
$\ker\psi = \{n : \psi(n) = 0\}$;
$\forall i = 1, ..., t$, $n \equiv 0(m_i) <=> m_i | n$, $(m_i, m_j) = 1 => m|n$;
$\ker\psi = (m) =>$(из Т. о гомоморфизме) $\mathbb{Z}/(m) \cong \mathbb{Z}/(m_1) \oplus ... \oplus \mathbb{Z}/(m_t)$. □

**Обозн:** $R$ — кольцо, $R^* = U(R)$ — множество единиц $R$; $U(R)$ — группа.

**Лемма 8.** $R = R_1 \oplus ... \oplus R_t => U(R) \cong U(R_1) \times ... \times U(R_t)$.

*Доказательство.* $U \in U(R)$, $\exists v : uv = 1 \Leftrightarrow \forall i\ u_i v_i = 1 \Leftrightarrow u_i \in U(R_i)$. □

**Следствие 2.** $m = m_1 \cdot ... \cdot m_t$, $(m_i, m_j) = 1$, *то* $U(\mathbb{Z}/m\mathbb{Z}) = U(\mathbb{Z}/m_1\mathbb{Z}) \times ... \times U(\mathbb{Z}/m_t\mathbb{Z})$.

$m = p_1^{a_1} ... p_t^{a_t}$, $U(\mathbb{Z}/m\mathbb{Z}) = U(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times ... \times U(\mathbb{Z}/p_t^{a_t}\mathbb{Z})$.

**Лемма 9.** *(Теорема Лагранжа) Если* $F$ *— поле,* $f \in F[x]$, $\deg f = n$, *тогда* $f$ *имеет не более* $n$ *корней.*

*Доказательство.* Индукция по $n$.
$n = 1$: $f = ax + b$, $-\frac{b}{a}$ — корень;
$n > 1$: если у $f$ нет корней, то доказано;
Пусть $\alpha \in F$, $f(\alpha) = 0$, $f(x) = g(x)(x - \alpha) + r$, здесь не $r(x)$, т. к. $\deg r < 1 => r \in F$.
При $x = \alpha$, $r = 0 => f(x) = q(x)(x - \alpha)$, $\deg q = \deg f - 1 = n - 1$. Если $\beta \neq \alpha$ — другой корень: $0 = f(\beta) = q(\beta)(\beta - \alpha) \neq 0 => q(\beta) = 0$, но по индукции $q$ имеет $\leq n - 1$ корней. □

**Следствие 3.** $f, g \in F[x]$, $\deg f = \deg g = n$, $f(\alpha_i) = g(\alpha_i)$, $1 \leq i \leq n + 1$, $\alpha_1, ..., \alpha_{n+1}$ *— различны, тогда* $f = g$.

Для $F = \mathbb{Z}/p\mathbb{Z}$.

**Лемма 10.** $x^{p-1} - 1 \equiv (x-1)...(x-(p-1))\ (p)$.

*Доказательство.* $x^{p-1} - 1 = (x-1)...(x-(p-1))$;

$f = (x^{p-1} - 1) - (x-1)...(x-(p-1))$ => $\deg f < p-1$;

$f(1) = f(2) = ... = f(p-1) = 0$;

Левая часть $= 0$ по т. Ферма, а правая $= 0$, т. к. $= 0$ => по предыдущему утверждению $f \equiv 0$ и они равны. $\square$

**Следствие 4.** $(p-1)! = -1\ (p)$.

**Лемма 11.** *Если* $d|p-1$, *то* $x^d \equiv 1\ (p)$ *имеет* $d$ *решений.*

*Доказательство.* $p-1 = cd$; $\frac{x^{p-1}-1}{x^d-1} = \frac{(x^d)^c-1}{x^d-1} = (x^d)^{c-1} + ... + x^d + 1 = g(x)$;

$x^{p-1} - 1 = (x^d - 1)g(x) = f(x)g(x)$;

Пусть $f = x^d - 1$ имеет $< d$ корней, $g(x)$ имеет $\leq d(c-1)$ корней;

$x^{p-1} - 1$ имеет $< d + d(c-1) = dc = p-1$ => ?!! с тем, что ровно $p-1$ корней. $\square$

**Теорема 4.** $U(\mathbb{Z}/p\mathbb{Z})$ — *циклическая группа.*

*Доказательство.* Надо доказать, что существует элемент порядка $p-1$.

Пусть $d|p-1$, $\psi(d) = |\{x \in U(\mathbb{Z}/p\mathbb{Z})$, порядка $d\}|$;

$$\begin{cases} x^d \equiv 1\ (p) \\ x^c \not\equiv 1\ (p),\ c < d \end{cases}$$

$\sum_{c|d} \psi(c) = d$;

$\psi(d) = \sum_{c|d} \mu(c)\frac{d}{c} = \phi(d)$ => $\psi(p-1) = d(p-1) = 0$. $\square$

**Определение 7.** *$g$ называется первообразным корнем (ПК) по mod $n$, если $g$ является образующим $U(\mathbb{Z}/n\mathbb{Z})$.*

**Пример.** $U(\mathbb{Z}/\delta\mathbb{Z}) = \{1, 3, 5, 7, 9\}$.

$x^2:\ 1, 9 \equiv 1, 25 \equiv 1, 49 \equiv 1, 81 \equiv 1$ => ПК нет.

**Теорема 5.** *$p > 2$, $U(\mathbb{Z}/p^l\mathbb{Z})$ — циклическая, $U(\mathbb{Z}/2^l\mathbb{Z})$, $U(\mathbb{Z}/4^l\mathbb{Z})$*

*$l \geq 3:\ U(\mathbb{Z}/2^l\mathbb{Z}) = U_0 \times U_1$, $U_0$ — пары 2, $U_1$ — пары $l-2$;*

$\{(-1)^a 5^b,\ a = 0, 1,\ 0 \leq b2^{l-2}\}$.

**Теорема 6.** *По mod $n$ существуют ПК для $n = 2, 4, p^l, 2p^l$.*