Оглавление

0.1. Корни из единицы

Определение 1. K — поле, $\varepsilon \in K$, $n \in \mathbb{N}$
ε называется корнем n-й степени из единицы, если $\varepsilon^n = 1$.
ε — примитивный корень степени n, если $\varepsilon^n = 1$, $\varepsilon^k \neq 1$ при $1 \leq k < n$

Пример. $K = \mathbb{Z}_5(\alpha)$, $\alpha^2 - 3 = 0$

$$\alpha^8 = 3^4 = 81 = 1 \implies \alpha \text{ — корень 8-й степени из единицы}$$

Свойства.

1. Корни n-й степени из 1 образуют абелеву группу по умножению

   Доказательство. Пусть U — множество корней n-й степени.

   - $\varepsilon_1, \varepsilon_2 \in U \implies (\varepsilon_1\varepsilon_2)^n = \varepsilon_1^n\varepsilon_2^n = 1 \cdot 1 = 1 \implies \varepsilon_1\varepsilon_2 \in U$
   - $\varepsilon \in U \implies \left(\frac{1}{\varepsilon}\right)^n = \frac{1^n}{\varepsilon^n} = \frac{1}{1} = 1 \implies \varepsilon^{-1} \in U$

   □

2. $\operatorname{char} k = p \in \mathbb{P} \neq 0$, $n = p^m h$, $h \not\vdots\, p$, ε — корень n-й степени из 1.
   Тогда ε — корень h-й степени из 1.

   Доказательство. Докажем, что если $\varepsilon^{ps} = 1$, то $\varepsilon^s = 1$:

   $$C_p^i = \frac{p!}{(p-i)! \cdot i!} \quad \vdots\, p \text{ при } 1 \leq i \leq p-1 \text{ в } \mathbb{Z}$$

   (т. к. $p! \vdots\, p$, $(p-i)! \cdot i! \not\vdots\, p$)

   $$\operatorname{char} K = p \implies C_p^i = 0 \text{ при } 1 \leq i \leq p$$

   $$(\varepsilon^s - 1)^p = (\varepsilon^s)^p + 0 \cdot (\varepsilon^s)^{p-1} \cdot (-1) + \dots + 0 \cdot \varepsilon^s \cdot (-1)^{p-1} + (-1)^p = \varepsilon^{sp} - 1 = 1 - 1 = 0 \xRightarrow[\text{обл. цел.}]{} \varepsilon^s - 1$$

   □

Пример. $K + \mathbb{Z}_5(\alpha)$, $\alpha^2 - 3 = 0$
Проверим, что α — примитивный корень 8-й степени:

$$\alpha^8 = 1 \implies 8 \,\vdots\, \operatorname{ord} \alpha \implies \operatorname{ord} \alpha = \left[\begin{array}{l} 8 \\ 4 \\ 2 \\ 1 \end{array}\right.$$

Если $\operatorname{ord}\alpha = \left[\begin{array}{l} 4 \\ 2 \\ 1 \end{array}\right.$, то $\alpha^4 = 1$

$$\alpha^4 = 3^2 = 9 = 4 \neq 1$$

Теорема 1 (существование примитивного корня). K — поле, $\quad h \in \mathbb{N}$
$x^h - 1$ раскладывается в K на линейные множители, $\quad h \not\vdots \operatorname{char} K$
Тогда

1. в K есть h различных корней n-й степени из единицы;
2. существует примитивный корень h-й степени из единицы;
3. группа корней h-й степени является циклической и порождается любым примитивным корнем.

Доказательство.

1. $p(x) = x^h - 1$ имеет h корней с учётом кратности
   $p'(x) = hx^{h-1}$ — единственный корень — 0 — не является корнем $p(x)$
2. U — группа корней h-й степени из единицы, $\quad |U| = h$
   Нужно доказать, что $\exists \varepsilon \in U: \quad \operatorname{ord}\varepsilon = h$
   Пусть $h = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}, \quad p_i \in \mathbb{P}$
   Докажем, что $\exists x_1, \dots, x_k \in U: \quad \operatorname{ord}(x_i) = p_i^{a_i}$:
   Докажем для $i = 1$ (остальное — аналогично):
   $$x_1 : \operatorname{ord} x_1 \stackrel{?}{=} p_1^{a_1}$$
   Докажем, что $\exists y: \quad \operatorname{ord} y \vdots p_1^{a_1}$:
   Пусть $\forall y \in U \quad \operatorname{ord} y \not\vdots p_1^{a_1}$
   $$\left.\begin{array}{l} p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \vdots \operatorname{ord} y \\ \operatorname{ord} y \not\vdots p_1^{a_1} \end{array}\right\} \implies \underbrace{p_1^{a_1-1} p_2^{a_2} \dots p_k^{a_k}}_{h'} \vdots \operatorname{ord} y$$
   $$h' \vdots \operatorname{ord} y \implies y^{h'} = 1 \quad \forall y \in U$$
   y — корень кногочлена $x^{h'} - 1 \quad \forall y \in U$
   У него $h > h'$ корней — $\lightning$
   $$\operatorname{ord} y = p_1^{a_1} \cdot t \implies \operatorname{ord}(y^t) = p_1^{a_1}$$
   Подойдёт $x_1 = y^t$. Аналогично x_i
   Докажем, что для $\varepsilon = x_1 x_2 \dots x_k$ выполнено $\operatorname{ord}\varepsilon = h$:
   Положими $b_i \coloneqq \frac{h}{p_i}$, т. е. $b_i = p_1^{a_1} \dots p_i^{a_i - 1} \dots p_k^{a_k}$
   $x_i^{b_i} \neq 1$ т. к. $b_i \not\vdots \operatorname{ord} x_i$
   $$x_i^{b_i} - 1, \qquad j \neq i$$
   $x_j^{b_i} = 1$ при $i \neq j$
   $$\varepsilon^{b_i} = \underbrace{x_1^{b_i}}_{1} \dots \underbrace{x_i^{b_i}}_{\neq 1} \dots \underbrace{x_k^{b_i}}_{1} \neq 1$$
   $$h \vdots \operatorname{ord}\varepsilon, \qquad b_i \not\vdots \varepsilon \quad \forall i \qquad \implies \operatorname{ord}\varepsilon = h$$
3. ε — примитивный
   $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{h-1}$ различны $\implies 1, \varepsilon, \dots, \varepsilon^{h-1}$ — все элементы U $(\varepsilon^i = \varepsilon^j \implies \varepsilon^{i-j} = 1)$

$\square$

Лемма 1 (количество примитивных корней). K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители
Тогда в K есть $\varphi(h)$ примитивных корней из единицы.

Доказательство. ε — примитивный корень
Все корни: $\varepsilon^0 = 1, \quad \varepsilon^1 = \varepsilon, \quad \varepsilon^2, \quad \dots, \quad \varepsilon^{n-1}$

Докажем, что ε^s примитивный $\iff$ НОД$(s, h) = 1$:

- Пусть НОД$(s, h) = 1$, $\quad (\varepsilon^s)^k = 1 \implies \varepsilon^{sk} = 1 \implies sk \,\vdots\, h \implies k \,\vdots\, h$

$$\operatorname{ord} \varepsilon^s = h$$

- Пусть НОД$(s, h) = d \neq 1$

$$(\varepsilon^s)^{\frac{h}{d}} = \varepsilon^{\frac{sh}{d}} = (\underbrace{\varepsilon^h}_{=1})^{\frac{s}{d}} = 1 \implies \operatorname{ord} \varepsilon^s = \frac{h}{d} \implies \varepsilon^s \text{ не примитивный}$$

$\square$

Определение 2. K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители
$\varepsilon_1, \dots, \varepsilon_{\varphi(h)}$ — все примитивные корни степени h

Многочлен деления круга (круговой многочлен) — это

$$\Phi_h(x) = (x - \varepsilon_1)(x - \varepsilon_2) \dots (x - \varepsilon_{\varphi(h)})$$