

⑥ Круговые поля и Теорема Ферма для регулярных простых показателей

1. Круговые поля и их СВ-ВА

Определение (из Теор. Галуа): Круговое расширение

L поля $\mathbb{Q}$ раз. чисел — это поле разложения $x^n - 1$ над $\mathbb{Q}$,
сделанное $x^n - 1$. Говорят, что L — **круговое поле**.

Если ζ — неприводим. корень ст. n над $\mathbb{Q}$, т.е. $\zeta^n = 1$, но
 $\zeta^d \neq 1 \quad \forall d=1, \dots, n-1$, то $L = \mathbb{Q}[\zeta]$.

Факт: ζ^m — тоже неприводим. $\Leftrightarrow (m, n) = 1$.

Факт: $[L : \mathbb{Q}] = \varphi(n)$ и $G = \text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}_n^*$.

Опр 1 Мин. поли-н $\Phi_n(t) \in \mathbb{Q}[t]$ непрвод. корня
ср. и из 1 наз-ся **Круговым делителем**.

Лемма 1 (СВ-ВА круговых делител-ов) **известно**

1) $\Phi_n(t) = \prod_{\substack{(m,n)=1 \\ 1 \leq m \leq n}} (t - \zeta^m)$, в частности, $\Phi_n(t)$ не зависит
от выбора ζ .

$$2) t^n - 1 = \prod_{d|n} \Phi_d(t) \quad (*)$$

3) p -член $\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \dots + t + 1$ и $\varphi(p) = p - 1$

4) $\Phi_{p^k}(t) = \frac{t^{p^k} - 1}{t^{p^{k-1}} - 1} = \Phi_p(t^{p^{k-1}})$, и $\varphi(p^k) = p^k - p^{k-1}$.

5) $\Phi_n(t) = \prod_{d|n} (t^d - 1)^{\mu(n/d)}$, μ -ф-ция обращения Мёбиуса.
В частности, $\deg \Phi_n(t) = \varphi(n)$, т.е. Φ_n непрвод.

Пример: $\mu: \mathbb{N} \rightarrow \{-1, 0, 1\}$ — ф-ция т.ч. $\mu(st) = \mu(s)\mu(t)$
 если $(s, t) = 1$, $\mu(p) = -1$ и $\mu(p^2) = 0$ при $\lambda > 1 \forall$ простого p .

2. Кольцо целых Кривого не является евклидовым.

Вспомогательное простое число.

Лемма 1 Пусть $u = p^k$, ξ — первостепенный корень n -ой ст. из 1
 $L = \mathbb{Q}[\xi]$, $P = (1 - \xi) \trianglelefteq \mathcal{O}_L$. Тогда P — простое,
 $p \mathcal{O}_L = P^e$, где $e = |L : \mathbb{Q}| = \varphi(n)$, $N_{L/\mathbb{Q}}(\xi) = (-1)^e$ и $N_{L/\mathbb{Q}}(1 - \xi) = p$.

Δ -во: Пусть ξ^1 — еще один, непер. корень из 1 ст. n . Тогда
 $\xi^1 = \xi^s$ и $\xi = (\xi^1)^t$, где $(s, p) = (t, p) = 1$. Поэтому

$$\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta'] \text{ и } \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']. \text{ Кроме того,}$$

$$\frac{1-\zeta'}{1-\zeta} = \frac{1-\zeta^s}{1-\zeta} = 1 + \zeta + \dots + \zeta^{s-1} \in \mathbb{Z}[\zeta] \text{ и } \frac{1-\zeta}{1-\zeta'} = 1 + \zeta' + \dots + (\zeta')^{t-1} \in \mathbb{Z}[\zeta']$$

$$\Rightarrow \frac{1-\zeta'}{1-\zeta} \text{ и } \frac{1-\zeta}{1-\zeta'} \in \mathbb{Z}[\zeta]^* \subseteq \mathcal{O}_L^*. \text{ Умножим}$$

$$p = \Phi_p(t^{p^{kn}}) \Big|_{t=1} = \Phi_p(1) = \prod_{1-\zeta'^t = p^k} (1-\zeta') = \prod_{1-\zeta'^t = p^k} \left(\frac{1-\zeta'}{1-\zeta} (1-\zeta) \right) = u(1-\zeta)^e,$$

$$\text{где } e = \varphi(u) \text{ и } u \in \mathcal{O}_L^* \Rightarrow p \mathcal{O}_L^* = (1-\zeta)^e = \mathfrak{p}^e.$$

По теореме 2.4.1 о фунд. соотв., существует, что $L/\mathbb{Q}$ — р-ад. Гал. и, следовательно, $p \mathcal{O}_L^* = (\mathbb{Q}_1 - \mathbb{Q}_2)^{e'}$ и $e = |L:\mathbb{Q}| = e'fg \Rightarrow e = e', f = g = 1$ и $\mathfrak{p} = \mathbb{Q}_1 \Rightarrow \mathfrak{p}$ — непр. идеал.

$$\text{В силу леммы 1.3.3 (A172)} \quad N(1-\zeta) = \prod_{\sigma \in G} \sigma(1-\zeta) = \prod_{(\sigma, p)=1} (1-\zeta^s) = \Phi_p(1) = \mathfrak{p}.$$

Лемма 2 Пусть $n = p^k > 2$, ζ - первообр. с. n , $L = \mathbb{Q}[\zeta]$.

Тогда $D(1, \zeta, \dots, \zeta^{e-1}) = (-1)^{e/2} p^m$, где $e = |L: \mathbb{Q}| = \varphi(n)$,
 $m = p^{k-1}(pk - k - 1)$. В частности, $p \nmid \text{disc } L$.

Д-во: (см. Голарель стр. 36) Мы покажем, что

верен следующий частный случай леммы 2 для $n = p$.

Мы г-м (см гол. 3.10 и к лемме 4), что

$$D(1, \zeta, \dots, \zeta^{p-1}) = \text{Dis}(t^{p-1} + t + 1) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$$

и $e = p-1 = \varphi(p)$. В частности, так как $p \nmid \text{disc}(O_L/\mathbb{Z})$

$\Rightarrow$ так как $p \nmid O_L$ разветв. в L по т. 2.4.3 из ANT 4

Т. 1 (о корнях унитар в круговом поле) Пусть

$n > 2$, ζ - n -корень ε -и $n \in \mathbb{I}$, $L = \mathbb{Q}[\zeta]$. Тогда

$O_L = \mathbb{Z}[\zeta]$, в частности, $1, \zeta, \dots, \zeta^{q(n)-1}$ - унитар базис L над $\mathbb{Q}$.

Для $n \geq 3$ и ζ - n -корня ε -и $n \in \mathbb{I}$ можно

$\mathbb{Q}[\zeta]^+ = \mathbb{Q}[\zeta + 1/\zeta] \subseteq \mathbb{R}$. Имеем $[\mathbb{Q}(\zeta) : \mathbb{Q}[\zeta]^+] = 2$,

т.к. $\text{Mot}_{\mathbb{I}}^{\zeta}(t) = t^2 - (\zeta + 1/\zeta)t + 1$. Поэтому $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta]^+ + \zeta \mathbb{Q}[\zeta]^+$.

Т. 2 (о единицах круговых полей) Пусть $p > 2$, $n = p^k$,

ζ - n -корень ε -и n , $L = \mathbb{Q}[\zeta]$. Тогда $\forall u \in O_L^*$

имеем $u = \zeta^m v$ где некое $m \in \mathbb{I}$ и $v \in O_{\mathbb{Q}[\zeta]^+}^*$.

1-30 т. 2 (сказано $n=p>2$) : Укажем $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_L$

$d = \prod (\zeta - \zeta^{p^{-1}}) = \pm p^{p-1}$ по лемме 2. В чужой системе.

1.4.1 (см. NT3) $p^{p-1} \mathcal{O}_L = d \mathcal{O}_L \subseteq \mathbb{Z}[\zeta]$. По

лемме 1 $p \mathcal{O}_L = \mathfrak{P}$, где $\mathfrak{P} = (1-\zeta) \mathcal{O}_L$ и $e = \varphi(p) = p-1$
 $\Rightarrow p^{(p-1)^2} \mathcal{O}_L \subseteq \mathbb{Z}[\zeta]$.

В гомоморфизме лемма 1 не нужна, но $f(\mathbb{P}/p\mathbb{Z}) = 1$,

т.е. $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/\mathfrak{P}) = 1 \Rightarrow \mathcal{O}_L/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$

$\Rightarrow \forall x \in \mathcal{O}_L \exists d \in \mathbb{Z} : x \in d + \mathfrak{P} \Rightarrow \mathcal{O}_L = \mathbb{Z} + \mathfrak{P}$

$\Rightarrow \mathcal{O}_L = \mathbb{Z}[\zeta] + \mathfrak{P}$, т.е. $\mathbb{Z} \subseteq \mathbb{Z}[\zeta]$. Укажем

$$(*) \quad O_L = \mathbb{Z}[\frac{1}{p}] + (1 - \frac{1}{p}) O_L$$

Подставим в O_L из определения, ее определение из левого:

$$O_L = \mathbb{Z}[\frac{1}{p}] + (1 - \frac{1}{p}) (\mathbb{Z}[\frac{1}{p}] + (1 - \frac{1}{p}) O_L) = \mathbb{Z}[\frac{1}{p}] + (1 - \frac{1}{p})^2 O_L.$$

Продолжая этот процесс, видим, что $\forall k \geq 1$

$$O_L = \mathbb{Z}[\frac{1}{p}] + (1 - \frac{1}{p})^k O_L.$$

Подставляя $k = (p-1)^2$ и учитывая, что $(1 - \frac{1}{p})^{(p-1)^2} O_L \subseteq \mathbb{Z}[\frac{1}{p}]$,

имеем $O_L = \mathbb{Z}[\frac{1}{p}]$, что и требовалось $\square$

Зам. Случай $n = p^2$ доказывался аналогично, если лемма 2 доказана в полной области.

Лемма 1.2 : $n = p^k$ ξ — н.в. н-ой с. из $\mathbb{L}$, $p \geq 2$.

Лемма $\mu(L) = \ker \varrho = \{\pm \xi^a, a = 0, \dots, n-1\}$ —
линейно в ссх корней 2n-ой с. из $\mathbb{L}$.

Лемма В ссх сгруппы $\mathbb{L}$ элемент 5.3 (см. АНТ 11)
 $\mu(L)$ состоит из всех корней из $\mathbb{L}$, лежащих в $\mathbb{L} = \mathbb{Q}[\xi]$.

Предп., что N — наим. н.в. числа, т.ч. ξ — н.в. с. N из $\mathbb{L}$
лежит в L . Тогда $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(N) \Rightarrow |\mathbb{Q}(\xi) : \mathbb{Q}| \text{ делит } |\mathbb{Q}(N) : \mathbb{Q}|$, т.е. $\varphi(N)$ делит $\varphi(n) = p^{k-1}(p-1) \Rightarrow N = 2n$,
 $p \geq 2$ □

Вернемся к формулировке: Для $u \in \mathbb{Q}_L$ имеем
 $u = \sum_{i=0}^{\varphi(n)-1} a_i \xi^i, a_i \in \mathbb{Z}$ в ссх 1.

$\bar{u} = \sum a_i \zeta^{-i} \in O_L$ ($\text{так } \bar{\zeta} = \zeta^{-1}$). В случае если,
если $u \in O_L^* \Rightarrow \bar{u} \in O_L^* \Rightarrow \alpha = \frac{u}{\bar{u}} \in O_L^*$.

Мы показали, что $\alpha \in \ker \ell = \mu(L)$. Аналогично
покажем, что $\forall \sigma \in \text{Hom}(L, \mathbb{C}) \quad |\sigma(\alpha)| = 1$.
(см. определение $\ell: O_L^* \rightarrow \mathbb{R}^{\Gamma \backslash S}$).

Если $\sigma \in \text{Hom}(L, \mathbb{C})$, то $\sigma(\zeta) = \zeta^k$.

Раскладывая $u = x + \zeta y$ над $L^+ = \mathbb{Q}[\zeta]^+ = \mathbb{Q}[\zeta + \zeta^{-1}]$,
где $x, y \in L^+ \subseteq \mathbb{R}$ имеем $\bar{u} = x + y \zeta^{-1}$. Кроме,

$\sigma(\bar{u}) = \sigma(x) + \zeta^{-k} \sigma(y) = \overline{\sigma(u)}$, т.к. $\sigma(\zeta + \zeta^{-1}) = \zeta^k + \zeta^{-k} \in \mathbb{R}$

и значит $\overline{\sigma(x)} = \sigma(x)$, $\overline{\sigma(y)} = \sigma(y)$. Таким образом,

$|\sigma(\alpha)| = \left| \frac{\sigma(u)}{\sigma(\bar{u})} \right| = \frac{|\sigma(u)|}{|\overline{\sigma(u)}|} = 1$, так как u уст. нсб.

В аналогичном $\alpha = \pm \zeta^a$. Если $\alpha = -\zeta^a$, то
 $u = -\zeta^a \bar{u}$. Тогда $-u \equiv u \pmod{(1-\zeta)}$, т.е. $\zeta^a - 1 \equiv 0 \pmod{(1-\zeta)}$.

С другой стороны, очевидно, что $u \equiv \bar{u} \pmod{(1-\zeta)}$,
 т.е. $u = \sum a_i \zeta^i \equiv \sum a_i \equiv \sum a_i \zeta^{-i} = \bar{u} \pmod{(1-\zeta)}$.

Но тогда $2u \in (1-\zeta)\mathcal{O}_L = \mathfrak{P} \Rightarrow 2 \in \mathfrak{P}$, но это
 невозможно, т.е. $(1-\zeta)\mathcal{O}_L \cap \mathbb{Z} = p\mathbb{Z}$. Поэтому $\alpha = \zeta^a$.

Т.е. u инвариантно, т.е. $\exists m : 2u \equiv u \pmod{n}$. А значит
 $u = \alpha \bar{u} = \zeta^{2m} \bar{u} = \zeta^m \underbrace{(\zeta^m \bar{u})} \Rightarrow u = \zeta^m v$ и $v = \zeta^{-m} u$.

$v = \zeta^m \bar{u} = \zeta^{-m} u \Rightarrow v = \bar{v} \in L^+$ ~~эквивалентно~~ 