(5) Круговые поля и теорема Ферма для регулярных простых показателей

1. Круговые пп-ия и их св-ва

Напоминание (из теории Галуа): Круговое расширение L поля $\mathbb{Q}$ рац. чисел — это поле разложения пад $\mathbb{Q}$ пп-ия $x^n - 1$. Говорят, что L — **круговое поле**.

Если ξ — первообр. корень ст. n из 1, т.е $\xi^n = 1$, но $\xi^d \neq 1 \ \forall d = 1, n-1$, то $L = \mathbb{Q}[\xi]$.

Факт: ξ^m — тоже первообр. $\iff (m, n) = 1$.

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

Опр 1 Мин. мн-н $\Phi_n(t) \in \mathbb{Q}[t]$ первообр. корня ст. n из 1 наз-ся круговым многочленом.

Лемма 1 (св-ва круговых мн-нов) Известно

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

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

3) p - простое $\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + \dots + t + 1$ 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) $\Phi_n(t) = \prod_{d \mid n} (t^d - 1)^{\mu(n/d)}$, μ - ф. для обращения Мёбиуса.

В частности, $\deg \Phi_n(t) = \varphi(n)$, т.к. Φ_n неприводим.

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

2. Кольцо целых кругового поля и его единицы.

Всюду далее p — простое число.

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

Д-во: Пусть ξ' — еще один прим. пер. корень из 1 ст. n. Тогда $\xi' = \xi^s$ и $\xi = (\xi')^t$, где $(s,p) = (t,p) = 1$. Поэтому

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

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

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

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

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

По т. 2.4.1 (ANT8) о фунд. тожд., учитывая, что $L/\mathbb{Q}$ – расш. Галуа, имеем $p\mathcal{O}_L = (\mathfrak{Q}_1 \cdots \mathfrak{Q}_g)^{e'}$ и $e = |L:\mathbb{Q}| = e'fg \Rightarrow e = e'$, $f = g = 1$ и $\mathfrak{P} = \mathfrak{Q}_1$. $\Rightarrow \mathfrak{P}$ – простой идеал.

В силу предл. 1.5.3 (ANT3) $N(1-\zeta) = \prod_{\sigma \in G} \sigma(1-\zeta) = \prod_{(s,p)=1} (1-\zeta^s) = \Phi_{p^k}(1) = p$. ∎

Лемма 2 Пусть $n = p^k > 2$, ζ – первообр. ч. n, $L = \mathbb{Q}[\zeta]$.
Тогда $D(1, \zeta, \dots \zeta^{e-1}) = (-1)^{\frac{e}{2}} p^m$, где $e = |L:\mathbb{Q}| = \varphi(n)$,
$m = p^{k-1}(pk - k - 1)$. В частности, в L разветв. только $p\mathcal{O}_L$.

Д-во: (См. Гэтвуд стр. 36) Мы показали, что верен следующий частный случай леммы 2 для $n = p$.
Мы д-ли (см. доп. задачи к семинару 4), что
$D(1, \zeta, \dots \zeta^{p-2}) = \mathrm{Dis}(\zeta^{p-2} + \dots + \zeta + 1) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$
и $e = p - 1 = \varphi(p)$. В частности, только $p \mid \mathrm{disc}(\mathcal{O}_L/\mathbb{Z})$
$\Rightarrow$ только $p\mathcal{O}_L$ разветв. в L по т. 2.4.3 из ANT ∎
Упр 1. Д-ть лемму 2 в полном объеме.

Т. 1 (о конечных группах в круговом поле) Пусть $n > 2$, ξ – n-й корень степени из 1, $L = \mathbb{Q}[\xi]$. Тогда $O_L = \mathbb{Z}[\xi]$, в частности, $1, \xi, \dots \xi^{\varphi(n)-1}$ – целый базис L над $\mathbb{Q}$.

Для $n > 2$ и ξ – n-й корень n-ой степени из 1 положим $\mathbb{Q}[\xi]^+ = \mathbb{Q}[\xi + \frac{1}{\xi}] \subseteq \mathbb{R}$. Имеем $[\mathbb{Q}(\xi) : \mathbb{Q}[\xi]^+] = 2$, т.к. $\mu_{\xi, \mathbb{Q}[\xi]^+}(t) = t^2 - (\xi + \frac{1}{\xi})t + 1$. Поэтому $\mathbb{Q}[\xi] = \mathbb{Q}[\xi]^+ + \xi\mathbb{Q}[\xi]^+$.

Т. 2 (о единицах круговых полей) Пусть $p > 2$, $n = p^k$, ξ – n-й корень из 1 ст. n, $L = \mathbb{Q}[\xi]$. Тогда $\forall u \in O_L^*$ имеем $u = \xi^m v$ для некот. $m \in \mathbb{Z}$ и $v \in O^*_{\mathbb{Q}[\xi]^+}$.

Д-во т. 1 (случай $n=p>2$): имеем $\mathbb{Z}[\xi] \subseteq \mathcal{O}_L$

$d = D(1, \xi .. \xi^{p-1}) = \pm p^{p-2}$ по лемме 2. В силу предл. 1.6.1 (см. ВИТ 4) $p^{p-2}\mathcal{O}_L = d\,\mathcal{O}_L \subseteq \mathbb{Z}[\xi]$. По лемме 1 $p\mathcal{O}_L = \mathfrak{P}^e$, где $\mathfrak{P} = (1-\xi)\mathcal{O}_L$ и $e = \varphi(p) = p-1$

$\Rightarrow$ $p^k \cdot \mathcal{O}_L \subseteq \mathbb{Z}[\xi]$, где $k = (p-2)(p-1)$.

В док-ве леммы 1 мы видели, что $f\left(\mathfrak{P}/p\mathbb{Z}\right) = 1$, т.е $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(\mathcal{O}_L/\mathfrak{P}\right) = 1 \Rightarrow \mathcal{O}_L/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$

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

$\Rightarrow \mathcal{O}_L = \mathbb{Z}[\xi] + \mathfrak{P}$, т.к $\mathbb{Z} \subseteq \mathbb{Z}[\xi]$. Имеем

(*) $\mathcal{O}_L = \mathbb{Z}[\xi] + (1-\xi)\mathcal{O}_L$

Подставим в $\mathcal{O}_L$ из предыдущего, её выражение из левой:

$$\mathcal{O}_L = \mathbb{Z}[\xi] + (1-\xi)\left(\mathbb{Z}[\xi] + (1-\xi)\cdot\mathcal{O}_L\right) = \mathbb{Z}[\xi] + P^2\cdot\mathcal{O}_L.$$

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

$$\mathcal{O}_L = \mathbb{Z}[\xi] + P^k\cdot\mathcal{O}_L.$$

Подставляя $k = (p-2)(p-1)$ и учитывая, что $P^k\cdot\mathcal{O}_L \subseteq \mathbb{Z}[\xi]$, имеем $\mathcal{O}_L = \mathbb{Z}[\xi]$, что и требовалось ▤

Зам. Случай $n = p^2$ доказывается аналогично, если лемма 2 доказана в полном объёме.

Д-во т. 2 : $n = p^k$ ξ - п. к. n-ой ст. из 1, $p > 2$.

Лемма $\mu(L) = \ker \ell = \{1, \xi^a, a = 0, \dots, n-1\}$ - мн-во всех корней $2n$-ой ст. из 1.

Д-во: В силу следствия 2 леммы 4.3 (см. ANT 11) $\mu(L)$ состоит из всех корней из 1, лежащих в $L = \mathbb{Q}(\xi)$.

Пусть, что N - наим. нат. число, т. ч. ξ - п. к. ст. N из 1 лежит в L. Тогда $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\xi) \Rightarrow |\mathbb{Q}(\xi) : \mathbb{Q}|$ делит $|\mathbb{Q}(\xi) : \mathbb{Q}|$, т. е $\varphi(N)$ делит $\varphi(n) = p^{n-1}(p-1) \Rightarrow N = 2n$, $p > 2$ ■

Вернемся к док-ву теоремы: Для $u \in \mathcal{O}_L$ имеем $u = \sum_{i=0}^{\varphi(n)-1} a_i \xi^i$, $a_i \in \mathbb{Z}$ в силу Т. 1. Теорему

$\bar{u} = \sum a_i \xi^{-i} \in O_L$ (где $\bar{\xi} = \xi^{-1}$). Далее,

$u \in O_L^* \Rightarrow \bar{u} \in O_L^* \Rightarrow \alpha = \frac{u}{\bar{u}} \in O_L^*$.

Мы доказали, что $\alpha \in \ker l = \mu(L)$. Для этого достат. показать, что $\forall \sigma \in \mathrm{Hom}(L, \mathbb{C})$ $|\sigma(\alpha)| = 1$. (см. опр-е отображения $l : O_L^+ \to \mathbb{R}^{r+s}$).

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

Раскладывая $u = x + \xi y$ над $L^+ = \mathbb{Q}[\xi]^+ = \mathbb{Q}[\xi + \xi^{-1}]$, где $x, y \in L^+ \subseteq \mathbb{R}$ имеем $\bar{u} = x + y\xi^{-1}$. Следовательно, $\sigma(\bar{u}) = \sigma(x) + \xi^{-k}\sigma(y) = \overline{\sigma(u)}$, т.к. $\sigma(\xi + \xi^{-1}) = \xi^k + \xi^{-k} \in \mathbb{R}$ и значит $\overline{\sigma(x)} = \sigma(x)$, $\overline{\sigma(y)} = \sigma(y)$. Таким образом,

$|\sigma(\alpha)| = \left|\sigma(u)/\sigma(\bar{u})\right| = \frac{|\sigma(u)|}{|\overline{\sigma(u)}|} = 1$, что и треб. было.

В силу леммы $\alpha = \pm \xi^a$. Если $\alpha = -\xi^a$, то $u = -\xi^a \cdot \bar{u}$. Тогда $-u \equiv \bar{u} \pmod{(1-\xi)}$, т.к. $\xi^a - 1 \equiv 0 \,(1-\xi)$.

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

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

Т.к. n нечетно, то $\exists m \in \mathbb{Z}_{>0}: 2m \equiv a \pmod{n}$. Имеем $u = \alpha \bar{u} = \xi^{2m} \bar{u} = \xi^m (\xi^m \cdot \bar{u}) \Rightarrow u = \xi^m v$, где $v = \xi^{-m} u$.

$\bar{v} = \xi^m \bar{u} = \xi^{-m}(\xi^{2m} \bar{u}) = \xi^{-m} u = v \Rightarrow v = \bar{v} \in L^+$, ч.т.д.