Лекция №3 Круговое поле

$x^n - 1$ корни $\exp\left(\frac{2\pi i k}{n}\right) \in \mathbb{C}$ ζ-дзета

первообразное: $\zeta^{<n}$ $\exp\left(\frac{2\pi i}{n}\right)$ - корни степени равно n

Упражнение: p-простое, то $\Rightarrow \frac{x^p - 1}{x-1}$ - неприводим над $\mathbb{Q}$

$x^{p-1} + \dots + x + 1$ Сделаем замену $y = x - 1$; $x = y + 1$

Сделаем подстановку и применим критерий Эйзенштейна

$$\frac{(y+1)^p - 1}{y} = y^p + \dots + p$$

$\frac{x^n - 1}{x-1}$; $\frac{x^6 - 1}{x-1} = \frac{(x^3-1)(x^3+1)}{x-1}$

Определение: $\Phi_n(x) := \prod_{\text{первообр. } \zeta} (x - \zeta)$ круговой многочлен

$\deg \Phi_n(x) = \varphi(n)$ - функция Эйлера

Утверждение: $x^n - 1 = \prod_{d \mid n} \Phi_d(x) \Rightarrow$ индукция по n $\Phi_n(x) \in \mathbb{Z}[x]$

Теорема: $\Phi_n(x)$ неприводим в $\mathbb{Z}[x] \Leftrightarrow$ в $\mathbb{Q}[x]$

Д-во: $\Phi_n(x) = \prod(x - \zeta) = f(x) \cdot F(x)$ пусть ζ-корень $f(x)$.
от противного

Взяли простое $p \nmid n \Rightarrow \zeta^p$ - тоже первообразный корень

Предположим, что ζ^p не корень f, а корень g (неприводимый)
↓ множитель F

$$\Phi_n(x) = f(x) g(x) \cdot h(x) \quad \text{т.к. } f(x) g(x) = 1$$
$$F(x)$$

Теперь приведем по модулю p

$\overline{\Phi}_n(x) = \overline{f}(x) \overline{g}(x) \overline{h}(x)$

$g(x^p)$ корень ζ $g(x^p) : f(x)$

$\overline{g}(x^p) = (\overline{g}(x))^p$

$(\overline{g}(x))^p : \overline{f}(x) \Rightarrow \forall$ неприводимый делитель $\overline{f}(x)$ встречается в $\overline{g}(x)$

$\Rightarrow \overline{\Phi}_n(x)$: квадрат этого неприводимого делителя $\overline{f}(x)$

$\Rightarrow (\overline{\Phi}_n, \overline{\Phi}_n') \neq 1$ есть кратные корни

$\overline{\Phi}_n \mid x^n - 1$ $(x^n - 1)' = n x^{n-1}$

$p \nmid n \Rightarrow$ единств. корень $(x^n-1)'$ этот 0

$(x^n-1;\ (x^n-1)') = 1$

Итак, если $f(x)$ неприводим. делитель $\Phi_n(x)$, а ζ-корень f, то $\forall p \nmid n$ ζ^p-тоже корень f

$\Phi(n) = p_1 \cdots p_k$, $p_i \nmid n$
$\varphi(n)$

□

Следствие $\mathbb{Q}[\sqrt[n]{1}] = \mathbb{Q}(\zeta) = \mathbb{Q}[x]/\Phi_n(x)$

$\deg \Phi_n(x) = \varphi(n)$

$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q} = \varphi(n)$

$[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = \varphi(n)$

Следствие: $\mathrm{Aut}\, \mathbb{Q}(\sqrt[n]{1}) = (\mathbb{Z}/n\mathbb{Z})^*$
ψ
a

$a(\zeta) = \zeta^a$

Следствие: $n = p$ -простое $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/(p-1)\mathbb{Z}$

Тогда $\mathrm{Aut}\, \mathbb{Q}(\sqrt[p]{1}) = \langle 1, \sigma, \sigma^2, \dots, \sigma^{p-2} \rangle$ цикл. группа с обр. σ

Перенумеруем перообразные корни $\zeta = \zeta_0, \zeta_1 := \sigma(\zeta), \zeta_2 = \sigma^2(\zeta) \cdots \zeta_{p-2} = \sigma^{p-2}(\zeta)$

Пример: $p = 17$

$(\mathbb{Z}/17\mathbb{Z})^* = \mathbb{F}_{17}^* = \mathbb{Z}/16\mathbb{Z}$

можно взять $\sigma = 3 \to 9 \to 10 \to 13 \to 5 \to 15 \to 11 \to 16 \to 14 \to 8 \to 7 \to 4 \to 12 \to 2 \to 6 \to 1$

$\zeta_0, \zeta_1 = e^{\frac{6\pi i}{17}}$, $\zeta_2 = \zeta^\sigma = e^{\frac{18\pi i}{17}}$ $\sigma \frac{2\pi i}{k}$
$= e^{2\cdot\frac{2\pi i}{17}}$

$\mathrm{Aut} = \langle \sigma \rangle \supset \langle \sigma^2 \rangle \supset \langle \sigma^4 \rangle \supset \langle \sigma^8 \rangle \supset \{e\}$

$\mathbb{Q}(\sqrt[n]{1}) := \{\alpha;\ \sigma(\alpha) = \alpha\} = \mathbb{Q} = K_1$, $\deg = 1$

$\mathbb{Q}(\sqrt[n]{1})^{\sigma^2} := \{\alpha : \sigma^2(\alpha) = \alpha\} = K_2$ $\deg = 2$

$\mathbb{Q}(\sqrt[n]{1})^{\sigma^4} := = K_3$ $\deg = 4$

$\mathbb{Q}(\sqrt[n]{1})^{\sigma^8} := = K_4$ $\deg = 8$

$\mathbb{Q}(\sqrt[n]{1})^{\sigma^{16}} := = K_5 = \mathbb{Q}[\sqrt[n]{1}]$ $\deg = 16$

Элементы K_2

Базис $\mathbb{Q}(\sqrt[17]{1})$: $\mathbb{Q}$ - это

$(\zeta_0, \zeta_1, \zeta_2, \dots \zeta_{15})$

↓ Это $\zeta_0 = \zeta_0 + \zeta_1 + \zeta_4 + \dots + \zeta_{14}$ > базис K_2

$\zeta_1 = \zeta_1 + \zeta_3 + \dots + \zeta_{15}$

$\zeta_0 + \zeta_1 = \zeta_0 + \zeta_1 + \dots + \zeta_{15} = \left(\sum \sqrt[17]{1}\right) - 1 = -1$

$\zeta_0 \cdot \zeta_1 = 64$ слагаемых $= 4 \sum_{j+1} \zeta = -4$

$\zeta^{3^a} \cdot \zeta^{3^b} = \zeta^{(3^a + 3^b)}$

$\zeta_0 \zeta_1 = -4$; $\zeta_0 + \zeta_1 = -1$.

$x^2 + x - 4$

$\zeta_0, \zeta_1 = \frac{-1 \pm \sqrt{17}}{2}$

Замечание: $\mathbb{Q}(\sqrt{17}) \subset \mathbb{Q}(\sqrt[17]{1})$

Вообще $\mathbb{Q}(\sqrt{N}) \subset \mathbb{Q}(\sqrt[4N]{1})$ - это очень трудный факт

$\mathbb{Q}(\sqrt[3]{1})$, $\mathbb{Q}(\sqrt{3}) \not\subset \mathbb{Q}\left(\frac{1 \pm \sqrt{3}}{2}\right)$, $x^2 + x + 1 = 0$

Очень близко к квадратичному закону взаимности

Построение циркулем и линейкой

Мы доказали, что правильный N-угольник можно построить циркулем и линейкой

Базис

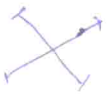
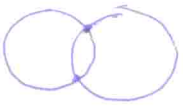
Определение поле $K \supset \mathbb{Q}$ поликвадратично, если оно получается последовательным присоединением корней

$\mathbb{Q} \subset K_2 \subset K_3 \subset \dots \subset K$

Утверждение: пусть есть какое-то построение у $\mathcal{L}$ и мы добавили к $\mathbb{Q}$ координаты всех точек, полученных в построении и получили $K \supset \mathbb{Q}$

Тогда K поликвадратично

Д-во: элементарное построение - это

а)  б)  в) 

а) Взятие линейного уравнения $k_i \rightsquigarrow k_i$

б) Взятие квадратного уравнения $k_i \rightsquigarrow k_i(\sqrt{?})$

в) Инвариант. жевл. б)

Лемма: башня расширений $K \subset L \subset M$

$\deg M : L = n$

$\dim_L M$

$\deg L : K = l$

$\deg M : K = ml$ $\Rightarrow \alpha_i \beta_j$ - базис M над K

Д-во: $\alpha_1, \dots, \alpha_l$ - базис L над K

$\beta_1, \dots, \beta_m$ базис M над K

Все произведения $\mu = \sum_i b_i \beta_i = \sum c_i^j \alpha_j \beta_i$

$b_i = \sum_j c_i^j \alpha_j$

Нет соотношений:

$\sum c_i^j \alpha_j \beta_i = 0 \Rightarrow \sum_i \left(\sum_j c_i^j \alpha_j\right) \beta_i = 0$.

Следствие: а) $\deg$ неприводимого поля равна 2^k

б) неприв. поле не может содержать корней степени не 2^k

Пример: $\mathbb{Q}(\sqrt[7]{1})$ $\deg = 6 \neq 2^k \Rightarrow$ нельзя построить 7-угольник циркулем и линейкой.