23/09/20

$$\begin{array}{ccc} \mathcal{O}_K = \mathbb{Z}[\zeta_n] & \subset & \mathbb{Q}(\zeta_n) = K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Kummer-Dedekind:

$$p\mathbb{Z}[\zeta_n] = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

$$\Updownarrow$$

$$\Phi_n(x) = \bar{g}_1^{e_1} \cdots \bar{g}_s^{e_s} \quad \text{en } \mathbb{F}_p[x].$$

Lema $n = \prod_p p^{v_p}$. Sea $p \in \mathbb{Z}$ primo racional.

$f = \operatorname{ord}(p) \bmod n/p^{v_p} \iff f = \min$ t.q. $p^f \equiv 1 \pmod{n/p^{v_p}}$

$$\bar{\Phi}_n = (\bar{g}_1 \cdots \bar{g}_s)^{\varphi(p^{v_p})}, \text{ donde } \deg g_i = f.$$

Dem Caso 1 $p \nmid n$, $v_p = 0$. $h = X^n - 1$ es separable en $\mathbb{F}_p[x]$

$(\operatorname{mcd}(h, h') = 1) \Rightarrow \Phi_n$ es tb. separable.

$f = \operatorname{ord}_n p \pmod n \Rightarrow f$ es el más pequeño tq.

$\mathbb{F}_{p^f}^\times$ contiene raíces n-ésimas primitivas

$\iff \mathbb{F}_{p^f}$ es el campo de descomposición de $\bar{\Phi}_n \in \mathbb{F}_p[x]$.

$$\bar{\Phi}_n = \bar{g}_1 \cdots \bar{g}_s \quad \text{en } \mathbb{F}_p[x].$$

$$\deg \bar{g}_i = [\mathbb{F}_{p^f} : \mathbb{F}_p] = f.$$

Caso 2 $p \mid n$, $n = m \cdot p^e$, $e = v_p$, $p \nmid m$.

Esto se reduce al caso anterior.

$$\Phi_n(x) \equiv \Phi_m(x)^{\varphi(p^e)} \pmod p \qquad \square$$

Teorema Sea $K = \mathbb{Q}(\zeta_n)$. $n = \prod_p p^{v_p}$

$$p\mathcal{O}_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_s^e, \quad \text{donde } \cdot) \ e = \varphi(p^{v_p})$$

$\cdot) \ \mathcal{O}_K/\mathfrak{p}_i \simeq \mathbb{F}_{p^{f_i}}$ donde $f = \operatorname{ord}(p) \bmod (n/p^{v_p})$.

Ejemplo $K = \mathbb{Q}(\zeta_{75})$ $\varphi(15) = 8$.

$p\mathcal{O}_K$ depende de $p \bmod 3$ y 5.

$p(3)$ \ $p(5)$	1	2	3	4
1	$\mathfrak{p}_1 \cdots \mathfrak{p}_8$	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 \cdots \mathfrak{p}_4$
2	$\mathfrak{p}_1 \cdots \mathfrak{p}_4$	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 \cdots \mathfrak{p}_4$

$3\mathbb{Z}[i\sqrt{15}] = \mathfrak{p}^2$ $\quad$ $5\mathbb{Z}[\sqrt{15}] = \mathfrak{q}^4$

Ejemplo (Kummer) $K = \mathbb{Q}(\zeta_{23})$ $\quad$ $\varphi(23) = 22$.

el primero p. t.q. $p \equiv 1 \ (23)$ es 47

$47\,\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_{22}$ $\quad$ $N(\mathfrak{p}_i) = 47$.

Afirmación (Kummer): Los $\mathfrak{p}_i$ no son principales.

Si $\mathfrak{p}_i = \alpha \mathcal{O}_K \Rightarrow N_{K/\mathbb{Q}}(\alpha) = \pm 47$

$N(\alpha) = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\alpha) = (\alpha\,\sigma^2(\alpha)\,\sigma^4(\alpha) \cdots \sigma^{20}(\alpha)) \times (\sigma(\alpha)\,\sigma^3(\alpha) \cdots \sigma^{21}(\alpha))$

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

σ - un generador de $Gal(K/\mathbb{Q})$

$\bar{\alpha} = \sigma^{11}(\alpha)$

$\mathbb{Q}(\sqrt{-23}) \subset \mathbb{Q}(\zeta_{23})$

↑ el subcampo dijo por (σ^2)

$N_{K/\mathbb{Q}}(\alpha) = \beta \cdot \bar{\beta}$, donde $\beta, \bar{\beta} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-23})}$

$\beta = \frac{a}{2} + \frac{b}{2}\sqrt{-23}$, $a, b \in \mathbb{Z}$ $\quad$ $a \equiv b \ (2)$

$N_{K/\mathbb{Q}}(\alpha) = \frac{a^2 + 23b^2}{4} = 47$

$a^2 + 23b^2 \neq 4 \cdot 47$

Conclusión: $\mathfrak{p}_i$ no son principales

$\Rightarrow \mathbb{Z}[\zeta_{23}]$ no es un DFU.