# Kreisteilungskörper

$n\geq 1$

$\zeta$: primitive n-te Einheitswurzel

$\zeta^n = 1$, $\zeta^k \neq 1$, $1\leq k<n$

äqv $\zeta = e^{\frac{2\pi i k}{n}}$ $1\leq k\leq n$, $(k,n)=1$

n-ter Kreisteilungskörper $\mathbb{Q}(\zeta)|\mathbb{Q}$ galoissch vom Grad $\varphi(n)$

Minimalpoly von $\zeta$ $\Phi_n(X) := \prod_{\substack{1\leq k\leq n\\ (k,n)=1}} (X-\zeta^k)$

$= \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times} (X-\zeta^k)$ $\Rightarrow \deg \Phi_n(X) = \varphi(n) = d$

falls $n = q^\nu$ Primzahlpotenz

$$\Phi_n(X) = \frac{X^{q^\nu}-1}{X^{q^{\nu-1}}-1} = X^{q^{\nu-1}(q-1)} + \dots + X^{q^{\nu-1}} + 1$$

**Satz** $1,\zeta,\dots,\zeta^{d-1}$ mit $d=\varphi(n)$ ist eine Ganzheitsbasis vom Ring $\mathcal{O}$ ganzen Zahlen von $\mathbb{Q}(\zeta)$ d.h.

$$\mathcal{O} = \mathbb{Z} + \zeta\mathbb{Z} + \dots + \zeta^{d-1}\mathbb{Z} = \mathbb{Z}[\zeta]$$

**Lem** $n = q^\nu$ Primzahlpotenz, $\lambda = 1-\zeta$

$\Rightarrow (\lambda)$ ist Primideal vom Grad 1 und

$q\mathcal{O} = (\lambda)^d$

Ferner hat die Basis $1,\zeta,\dots,\zeta^{d-1}$ von $\mathbb{Q}(\zeta)|\mathbb{Q}$ Diskriminante

$$d(1,\zeta,\dots,\zeta^{d-1}) = \pm q^s,\ s = q^{\nu-1}(\nu q - \nu - 1)$$

---

**Bew** $\zeta\in\mathcal{O}$, $\varepsilon_k := 1+\zeta+\dots+\zeta^{k-1} = \frac{1-\zeta^k}{1-\zeta} \in \mathcal{O}$

$X=1$

$q = \prod_{k\in\mathbb{Z}_n^\times} (1-\zeta^k) = \prod_{k\in\mathbb{Z}_n^\times} \varepsilon_k(1-\zeta)$

$k\in\mathbb{Z}_n^\times$ invertierbar $\Rightarrow \exists k'\in\mathbb{Z}: k'k\equiv 1 \mod n$

$\Rightarrow \frac{1-\zeta}{1-\zeta^k} = \frac{1-\zeta^{k'k}}{1-\zeta^k} = \frac{1-(\zeta^k)^{k'}}{1-\zeta^k} =$

$1+\zeta^k+\dots+(\zeta^k)^{k'-1} \in \mathcal{O}$

$\Rightarrow \varepsilon_k$ Einheit, $\varepsilon := \prod_k \varepsilon_k$ Einheit

$\Rightarrow q = \varepsilon(1-\zeta)^d \Rightarrow q\mathcal{O} = (\lambda)^d$

$\Rightarrow (\lambda)$ Primideal vom Grad

$\sum_i e_i f_i = d$

$\pm d(1,\zeta,\dots,\zeta^{d-1}) = \prod_{i\neq j}(\zeta_i - \zeta_j) = \prod_{i=1}^{d} \Phi_n'(\zeta_i)$

$\zeta_i$ die Konjugierten von $\zeta$ unter der Wirkung der Galois Gruppe

$L|K$ separabel $\overset{(*)}{\Rightarrow} N_{L|K}(x) = \prod_\sigma \sigma x$

$\sigma: L\to\bar{K}$ K-Einbettungen

$\prod_i \Phi_n'(\zeta_i) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi_n'(\zeta))$

$(X^{q^{\nu-1}}-1)\Phi_n(X) = X^{q^\nu}-1$ $(n=q^\nu)$

ableiten nach $X$, auswerten $X=\zeta$

$\Rightarrow (\zeta^{q^{\nu-1}}-1)\Phi_n'(\zeta) = q^\nu\zeta^{-1}$

---

$\xi := \zeta^{q^{\nu-1}}$ $q$-te primitive Einheitswurzel

$$\boxed{(\xi-1)\Phi_n'(\zeta) = q^\nu\zeta^{-1}}$$

$N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1) \overset{(*)}{=} \prod_{1\leq k<q}(\xi^k-1) = \pm\Phi_q(1) = \pm q$

$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi-1) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)^{q^{\nu-1}} = \pm q^{q^{\nu-1}}$

$N(\zeta^{-1}) = 1$, $N(q^\nu) = N(n) = n^{\varphi(n)}$

$\Rightarrow N_{\mathbb{Q}(\zeta)|\mathbb{Q}}\Phi_n'(\zeta) = \pm q^s$

$\pm d(1,\zeta,\dots,\zeta^{d-1})$ □

**Satz** $\mathcal{O} = \mathbb{Z}[\zeta]$

**Bew** Ang. $n = q^\nu$ Primzahlpotenz

$q^s\mathcal{O} \subseteq \mathbb{Z}+\zeta\mathbb{Z}+\dots+\zeta^{d-1}\mathbb{Z} = \mathbb{Z}[\zeta] \subseteq \mathcal{O}$ $(\zeta\in\mathcal{O})$

$\lambda = 1-\zeta$, Primideal vom Grad 1 mit

$q\mathcal{O} = (\lambda)^d \Rightarrow \mathcal{O}/\lambda\mathcal{O} \cong \mathbb{Z}/q\mathbb{Z}$

$\Rightarrow \mathcal{O} = \mathbb{Z}/q\mathbb{Z} + \lambda\mathcal{O}$ $\mathbb{Z}_q \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}$

$\Rightarrow \mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O}$

$\lambda\mathcal{O} = \underbrace{\lambda\mathbb{Z}[\zeta] + \lambda^2\mathcal{O}}$ $\quad \lambda\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\zeta]$

$\rightsquigarrow \mathcal{O} = \mathbb{Z}[\zeta] +$

$= \mathbb{Z}[\zeta] + \lambda^2\mathcal{O}$

$\Rightarrow \mathcal{O} = \mathbb{Z}[\zeta] + \lambda^t\mathcal{O} \quad \forall t \geq 1$

$\Rightarrow \underline{\mathcal{O}} = \mathbb{Z}[\zeta] + \lambda^{ds}\mathcal{O} = \mathbb{Z}[\zeta] + (q\mathcal{O})^s\mathcal{O}$

$= \mathbb{Z}[\zeta] + \underbrace{q^s\mathcal{O}}_{\subseteq \mathbb{Z}[\zeta]} = \underline{\mathbb{Z}[\zeta]}$

$n = q_1^{\nu_1}\cdots q_r^{\nu_r}$ Primfaktorzerlegung

$\mathbb{Q}(\zeta) = \underline{\mathbb{Q}(\zeta_1)}\cdots\mathbb{Q}(\zeta_r)$

$\zeta_i := \zeta^{m_i} \quad m_i = \frac{n}{q_i^{\nu_i}}$

$(\ldots)$

$\{ \underline{\zeta_1^{j_1}\cdots\zeta_r^{j_r}} \mid 0 \leq j_i < d_i \}$

$\zeta^d = 1 \rightsquigarrow 1, \zeta, \ldots, \zeta^{d-1}$

---

<u>Satz</u> $n = \prod_p p^{\nu_p}$ Primfaktorzerlegung

$\zeta$: n-te Primitive Einheitswurzel

$f_p \in \mathbb{Z}_{>0}$ minimal s.d. $p^{f_p} \equiv 1 \mod \frac{n}{p^{\nu_p}}$

$\Rightarrow (p) = (\pi_1\cdots\pi_r)^{\varphi(p^{\nu_p})}$

$\pi_i$ verschiedene Primideale vom $f_p$

---

$x^p + y^p$ faktorisieren in $\mathbb{Q}(\zeta)$

$$t^p - 1 = \prod_{0\leq k<p}(t - \zeta^k)$$

$$\left(-\frac{x}{y}\right)^p - 1 = \prod_{0\leq k<p}\left(-\frac{x}{y} - \zeta^k\right)$$

$$x^p + y^p = \prod_{0\leq k<p}(x + y\zeta^k)$$

---

$\pi \supseteq (z)^p \overset{\pi \text{ prim}}{\Longrightarrow} \pi \supseteq (z)$

$\pi \supseteq (z) + (yp) \ni 1$, $z, y, p$ paarweise teilerfremd

↯ $\pi$ primideal

---

$(x+y\zeta) = \underline{I}^p$ Ideal $I$

$(x+y)\underline{(x+y\zeta)}\cdots(x+y\zeta^{p-1}) = (z)^p$

<u>Def</u> $p$ ist <u>regulär</u> falls $p$ die Kardinalität der Klassengruppe von $\mathbb{Q}(\zeta)$ nicht teilt. ($\zeta$: prim. $p$-te Einheitswurzel)

$C_0$ Klasse Hauptideale

## Grosser Fermatscher Satz

$x^n + y^n = z^n \quad n > 2$ hat keine positiven ganzzahligen Lösungen $(x,y,z) \in \mathbb{Z}^3_{>0}$

<u>Ang.</u> $n = p \geq 5$ prim, $(x,y,z) \in \mathbb{Z}^3_{>0}$ Lsg $\quad$ oBdA, $x,y,z$ paarweise teilerfremd

$p \nmid xyz$

$(x+y)(x+y\zeta)\cdots(x+y\underline{\zeta^{p-1}}) = (z)^p$

<u>Beh</u> $(x+y\zeta)$ hat keine gemeinsamen Primideal faktoren mit den anderen Hauptidealen auf der linken Seite

<u>Ang</u> $\pi \supseteq (x+y\zeta)$

$\pi \supseteq (x+y\zeta^k) \quad k \not\equiv 1 \mod p$

$\Rightarrow \pi \supseteq (x+y\zeta^k) - (x+y\zeta)$

$\pi \supseteq (y\zeta(\zeta^{k-1}-1)) = \underline{(y(\zeta^{k-1}-1))}$

$p = \prod_{k\in\mathbb{Z}_n^\times}(1-\zeta^k) \quad n = p \quad \mathbb{Z}_n^\times = \mathbb{F}_p\setminus\{0\}$

$\Rightarrow (p) = (1-\zeta)\cdots(1-\zeta^{p-1})$

$\Rightarrow \pi \supseteq (yp)$

Sei $p$ regulär $\Rightarrow \nexists$ Elemente der Ordnung $p$ in der Klassengruppe

$I \in C \Rightarrow I^p \in C^p = C_0 \Rightarrow \operatorname{ord}(C) \mid p$

$I^p = (x+y\zeta)$ Hauptideal

$p$ prim $\Rightarrow \operatorname{ord}(C) = 1 \Leftrightarrow C = C_0$

$\Rightarrow I$ Hauptideal $\Rightarrow x + y\zeta = u\alpha^p$

$u$: Einheit

$\alpha \in \underline{\mathbb{Z}[\zeta]}$

$$\alpha^p = \left(\sum_{i=0}^{p-1} a_i \zeta^i\right)^p \equiv \sum_{i=0}^{p-1} a_i^p \underbrace{\zeta^{ip}}_{=1} \bmod p \quad \underbrace{\phantom{xx}}_{\in \mathbb{Z}}$$

$(\beta+\gamma)^p \equiv_p \beta^p + \gamma^p \quad \forall \beta,\gamma \in \mathbb{Z}[\zeta]$

$\forall u \in \mathbb{Z}[\zeta]: \frac{u}{\bar{u}} = \zeta^k \quad \exists k \geq 0$

$\Rightarrow x + y\zeta = u\alpha^p \equiv \frac{u}{\bar{u}} \overline{u\alpha^p}$

$= \underline{\zeta^k (x + y\zeta^{-1})}$

Beh $k \equiv 1 \bmod p$

~~Ang $k \not\equiv 1 \bmod p$~~

$p \mid \zeta^k(x + y\zeta^{-1}) - (x + y\zeta)$

$p \mid \underline{-x} - y\zeta + \underline{x\zeta^k} + y\zeta^{k-1}$

$p \mid a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1} \quad (a_i \in \mathbb{Z})$

$\Rightarrow p \mid a_i \quad \forall i$

$\left[x \cdot 1 + x\underbrace{\zeta^k}_{\neq 1}\right]$

$p \nmid x \Rightarrow k \equiv_p 0$

$\Rightarrow p \mid -y\zeta + y\zeta^{-1} \qquad p > 2$

$\Rightarrow p \mid y \;\lightning\; p \nmid xyz$

---

$x + y\zeta \equiv x\zeta + y \bmod p$

$\Rightarrow x \equiv y \bmod p$

$x^p + (-z)^p = (-y)^p \qquad (p$ ungerade$)$

$\Rightarrow x \equiv -z \bmod p$

$2x^p \equiv x^p + y^p = z^p \equiv -x^p \bmod p$

$\Rightarrow p \mid 3x^p \qquad p \geq 5$

$\Rightarrow p \mid x^p$

$\Rightarrow p \mid x \;\lightning\; p \nmid xyz$

$x, y, z \qquad x^p + y^p = z^p$

$p \geq 5$ prim, regulär

$p \nmid xyz$

---

**Satz** Für $p$ ungerade, prim

$p^* := (-1)^{\frac{p-1}{2}} p \qquad \zeta$: primitive $p$-te Einheitswurzel

$\Rightarrow \mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta)$

Bew $p^* = \left(\frac{-1}{p}\right) p \qquad$ (Eulersches krit.)

Sei $\tau := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a \qquad p^* = (-1)^{\frac{1}{2}} 2 = 2i \qquad \zeta^p = 1$

Beh $p^* = \tau^2$

$$\left(\frac{-1}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)\left(\sum_a \left(\frac{a}{p}\right)\zeta^a\right)\left(\sum_b \left(\frac{b}{p}\right)\zeta^b\right)$$

$$= \sum_{a,b} \left(\frac{-ab}{p}\right) \zeta^{a+b}$$

$$= \sum_{a,b} \left(\frac{ab}{p}\right) \zeta^{a-b} \qquad \left(\frac{b^{-1}}{p}\right) = \left(\frac{b}{p}\right)$$

$$= \sum_{a,b} \left(\frac{ab^{-1}}{p}\right) \zeta^{a-b} \qquad c := ab^{-1}$$

$$= \sum_{b,c} \left(\frac{c}{p}\right) \zeta^{b(c-1)}$$

$$= \sum_{c \neq 1} \left(\frac{c}{p}\right) \sum_b \zeta^{b(c-1)} + \underbrace{\left(\frac{1}{p}\right)}_{1} \sum_b \underbrace{\zeta^0}_{1}$$

$$= \sum_{c \neq 1} \left(\frac{c}{p}\right) \sum_b \xi^b + (p-1)$$

$\xi := \zeta^{c-1} \qquad \sum_c \left(\frac{c}{p}\right) \overset{!}{=} 0$

$-\underline{\sum_c \left(\frac{c}{p}\right)} = \left(\frac{x}{p}\right) \sum_c \left(\frac{c}{p}\right) = \sum_c \left(\frac{xc}{p}\right) = \underline{\sum_{c'} \left(\frac{c'}{p}\right)}$

$$\left(\frac{-1}{p}\right)\tau^2 = -\left(\frac{1}{p}\right)\underbrace{\sum_b \zeta^b}_{-1} + p-1$$

$$= -1\,(-1) + p-1 = p$$

$$\Rightarrow \tau^2 = \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)p = p^* \quad \square$$

für ein $x$ mit $\left(\frac{x}{p}\right) = -1$

1) Was sind ganzen Zahlen von $\mathbb{Q}(\zeta)$?

2) Wie zerfallen Primzahlen in Primideale über $\mathbb{Q}(\zeta)$?

3) Wie hilft uns die Primidealfaktor. von $\mathbb{Z}[\zeta]$ einen Teil des grossen Fermatschen Satzes zu zeigen?