

Z13: Explizite Primidealzerlegungen

Stichworte:

Explizite PIZ im quadratischen ZK und im Kreisteilungskörper,

verzweigte PZ = Primteiler von $disc K$ und Ausartung der bilinearen Spurform von A/A_p

13.1. Einleitung: Die explizite PIZ laut Z12 wird in bestimmten Beispielen durchgeführt: im quadratischen ZK und im Kreisteilungskörper. Wir stellen fest, dass die in einem ZK verzweigten Primzahlen genau die Primteiler von $disc K$ sind, so dass der Verzweigungsfall überhaupt nur endlich oft eintreten kann. Dies tritt genau dann ein, wenn die bilineare Spurform von A/A_p nichtausgeartet ist.

13.2. Bsp.: Quadratische Zahlkörper

Sei $L = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, und $A = \mathbb{Q}(\sqrt{m}) \cap \mathbb{A}$, $p \in \mathbb{N}$ prim.

Wegen $n = \sum_{i=1}^r e_i f_i = 2$ gibt es höchstens drei Zerlegungstypen von p :

$$A_p = \begin{cases} p_1 \cdot p_2, & \text{mit } p_1 \neq p_2, & \begin{cases} \lceil 1 \cdot 1 + 1 \cdot 1 \rceil & \text{(voll zerlegter Fall)} \\ \lceil 2 \cdot 1 \rceil & \\ \lceil 1 \cdot 2 \rceil & \end{cases} \\ p^2 & \text{(verzweigter Fall)} \\ \text{prim} & \text{(träge Fall)} \end{cases}$$

1. Fall: $p \neq 2$. Wegen $\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ (Index 2) sei $\mathcal{O} = \mathbb{Z}[\sqrt{m}]$.

Es ist $T^2 - m \in \mathbb{Z}[T]$, sowie $T^2 - \bar{m} \in \mathbb{F}_p[T]$.

(a) Sei \bar{m} Quadrat mod p : Etwa $\bar{m} = \bar{j}^2$. (D.h. $\left(\frac{m}{p}\right) = 1$)

Dann ist $T^2 - \bar{m} = (T - \bar{j})(T + \bar{j})$. (zerlegt)

• Falls $p | m$: $\bar{j} = 0$, d.h. $T^2 - \bar{m} = T^2$, also: $A_p = (\sqrt{m}, p)^2$. (verzweigt)

• Falls $p \nmid m$: $\bar{j} \neq 0$, d.h. $T^2 - \bar{m} = (T - \bar{j})(T + \bar{j})$, also: $A_p = (\sqrt{m} - \bar{j}, p)(\sqrt{m} + \bar{j}, p)$.

(b) Sei \bar{m} kein Quadrat mod p : Dann ist $T^2 - \bar{m}$ irred., also A_p prim. (D.h. $\left(\frac{m}{p}\right) = -1$) (träge)

2. Fall: $p = 2$.

(a) Sei $m \equiv 2, 3 \pmod{4}$: Dann ist $A = \mathbb{Z}[\sqrt{m}]$ und $\mathbb{F}_2[T] \ni T^2 - \bar{m} = (T - \bar{m})^2$, also ist $A \cdot 2 = (\sqrt{m} - m, 2)^2$. (verzweigt)

2. Fall: $p=2$.

(b) Sei $m \equiv 1 \pmod{4}$: Mit $x := \frac{1+\sqrt{m}}{2}$ ist dann $A = \mathbb{Z}[x]$

und $f := T^2 - T - \frac{m-1}{4} \in \mathbb{Z}[T]$ ist das Mipo von x .

• Falls $m \equiv 1 \pmod{8}$: Haben $\bar{f} = T^2 - T = T(T-1)$.

Also ist $A \cdot 2 = \left(\frac{1+\sqrt{m}}{2}, 2\right) \cdot \left(\frac{-1+\sqrt{m}}{2}, 2\right)$. (zerlegt)

• Falls $m \equiv 5 \pmod{8}$: Haben $\bar{f} = T^2 + T + 1$, ist irred. über F_2 .

Also ist $A \cdot 2$ prim. (träge)

13.3. Bem: Also ist p verzweigt genau wenn

$disc = 4m \leftarrow (m \equiv 2,3 \pmod{4} \text{ und } (p|m \text{ oder } p=2)) \text{ oder } (m \equiv 1 \pmod{4} \text{ und } (p|m \text{ und } p \neq 2)),$
d.h. wenn $p | disc \mathbb{Q}(\sqrt{m})$. $disc = m$ (vgl. 8.8)

13.4. Bsp.: Kräfteilungskörper

Sei $K = \mathbb{Q}(\omega)$ mit $\omega = e^{2\pi i/m}$. Der Zahlring ist $\mathbb{Z}[\omega]$ nach Satz 9.2.

Das Mipo Φ_m von $\omega | \mathbb{Q}$ hat Grad $\varphi(m)$. Sei p prim die zu zerlegende PZ.

1. Fall: $p \nmid m$

Betrachte $\mathbb{Z} \rightarrow \mathbb{Z}/(p) = \mathbb{F}_p$. Haben: $\Phi_m \in \mathbb{Z}[T]$ zerfällt in $\mathbb{F}_p[T]$

in ein Produkt $\bar{\Phi}_m = \bar{f}_1 \cdots \bar{f}_r$, die \bar{f}_i p.w.v., wobei $f := \deg f_i$

$\hat{=}$ multiplikative Ordnung von $p \pmod{m}$, also $r = \frac{\varphi(m)}{f}$ [s. Lemma 13.8 unten].

Erhalten $\mathbb{Z}[\omega]_p = \mathfrak{a}_1 \cdots \mathfrak{a}_r$, mit $f(\mathfrak{a}_i | p) = \deg f_i = f$. alle $e_i = 1$

(zerlegt)

2. Fall: $m = p^k$

Es gilt $T^m - 1 = \Phi_m(T) \cdot \Psi(T)$ in $\mathbb{Z}[T]$.

In $\mathbb{F}_p[T]$ gilt nun: $T^{p^k} - 1 = (T-1)^{p^k}$, also ist $\bar{\Phi} = (T-1)^{\varphi(p^k)}$,

und somit $\mathbb{Z}[\omega]_p = \mathfrak{a}_1^{\varphi(p^k)}$, wobei $\mathfrak{a}_1 = (\omega-1, p)$ ist.

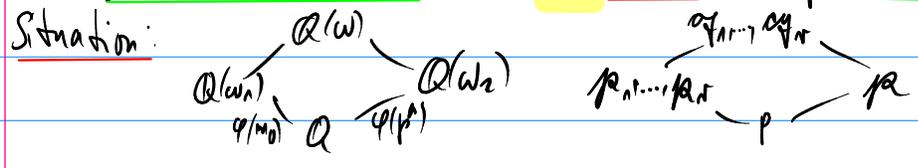
Es gilt $\prod_{i=1}^{p-1} (\omega^i - 1) = N(\omega-1) = p$, vgl. auch 6.22(1),

jedes $\omega^i - 1$ ist Vielf. von $\omega - 1$
 $\Rightarrow p \in \mathbb{Z}[\omega] \cdot (\omega - 1)^j$ für ein j

Also ist $\mathfrak{a}_1 = (\omega-1) = \mathbb{Z}[\omega] \cdot (\omega-1)$ ein Hauptideal.

(verzweigt)

Allgemeiner Fall: Sei $m = p^k m_0$ mit $p \nmid m_0$. Dann ist $\omega_1 := \omega^{p^k}$ eine primitive m_0 -te EW und $\omega_2 := \omega^{m_0}$ eine primitive p^k -te EW.



Für $1 \leq i \leq r$ sei \mathfrak{a}_i Primideal von $\mathbb{Z}[w]$ über p_i .

Diese \mathfrak{a}_i liegen alle über p , und es gilt:

$$e(\mathfrak{a}_i | (p)) \geq e(p_i | (p)) \stackrel{2. \text{ Fall}}{=} \varphi(p^k), \quad f(\mathfrak{a}_i | (p)) \geq f(p_i | (p)) \stackrel{1. \text{ Fall}}{=} \frac{\varphi(m_0)}{r}$$

Somit: $\sum_{i=1}^r e(\mathfrak{a}_i | (p)) f(\mathfrak{a}_i | (p)) \geq \sum_{i=1}^r \varphi(p^k) \frac{\varphi(m_0)}{r} = \varphi(p^k) \varphi(m_0) = \varphi(m) = [\mathbb{Q}(w) : \mathbb{Q}]$

Also sind $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ alle über (p) liegenden Ideale, und $e(\mathfrak{a}_i | (p)) = \varphi(p^k)$, $f(\mathfrak{a}_i | (p)) = \frac{\varphi(m_0)}{r}$. Vergleiche: $\text{disc } \mathbb{Q}(w) \mid m^{\varphi(m)}$ nach 6.22 (2). \square
 \hookrightarrow Die Primteiler von $\text{disc } \mathbb{Q}(w)$ sind verzweigt.

13.5. Satz: Die in einem Zahlkörper verzweigten Primzahlen sind genau die Primteiler seiner Diskriminante.

Bew.: Sei $[K : \mathbb{Q}] = n$, $A = K \cap \mathbb{A}$, $d := \text{disc}(K)$. Sei $B: x_1, \dots, x_n$ GHB von K , d.h. $A = \bigoplus_{i=1}^n \mathbb{Z} x_i$. Sei p prim, und $A \rightarrow A/pA =: \bar{A}$, $x \mapsto \bar{x}$, die Projektion.

Es ist \bar{A} eine kommutative \mathbb{F}_p -Algebra, und $\bar{B}: \bar{x}_1, \dots, \bar{x}_n$ ist \mathbb{F}_p -Basis von \bar{A} .

Für $\bar{z} \in \bar{A}$ sei $M_{\bar{B}} \bar{z}$ die Multiplikation mit \bar{z} in \bar{A} .

Ist $M_B(\mu_z) = (a_{ij})$, so sind die $a_{ij} \in \mathbb{Z}$ und $M_{\bar{B}}(\mu_{\bar{z}}) = (\bar{a}_{ij})$.

Sei $\bar{\tau}$ die Spur auf der \mathbb{F}_p -Algebra \bar{A} . Dann ist

$$\bar{d} = \det(\tau_{\bar{B}}^K(x_i, x_j)) = \det(\tau_{\bar{B}}^K(x_i, x_j)) = \det(\text{Spur}(\mu_{x_i} \mu_{x_j})) = \det(\text{Spur} \mu_{x_i x_j}) = \det(\bar{\tau}(\bar{x}_i \bar{x}_j))$$

Somit gilt: $p \mid d \Leftrightarrow \bar{d} = 0 \Leftrightarrow$ die bilineare Spurform $\bar{\Phi}$ von \bar{A} ist ausgeartet.

Bleibt zu zeigen: Beh.: p unverzweigt in $K \Leftrightarrow \bar{\Phi}$ nicht ausgeartet.

Demnach sind die Primteiler p von d genau die verzweigten Primzahlen.

Zum Bew. des Beh. sei $pA = \mathfrak{a}_1^{e_1} \dots \mathfrak{a}_r^{e_r}$ die PIZ.

Zu (2): Sei $x \in A \setminus \{0\}$ mit $x^n = 0$. Gen.z.z.: $\text{Spur}(\mu_x) = 0$.

x nilpotent $\Rightarrow \forall a \in A: xa$ nilpotent (da A kommutativ) $\Rightarrow \forall a \in A: \Phi(xa) = \text{Spur}(\mu_{xa}) = 0$.

Gen.z.z.: Ex. K -Basis von A mit $M(\mu_x)$ obere Dreiecksmatrix.

$M(\mu_x) = (a_{ij})$ obere Δ -Matrix $\Rightarrow 0 = (a_{ij})^n \Rightarrow \forall 1 \leq i \leq m: a_{ii}^n = 0 \Rightarrow a_{ii} = 0 \Rightarrow \text{Spur}(\mu_x) = 0$.

Nun vollst. Ind. nach $m := \dim_K A$: $m = 1: V, m > 1$:

im μ_x ist echter Unterraum von A , da μ_x nicht injektiv.

Sei y_1, \dots, y_r Basis von $\text{im } \mu_x$ mit $\mu_x(y_i) = xy_i \in L(\{y_1, \dots, y_{i-1}\})$, $1 \leq i \leq r$, nach Ind. Vor.

Ergänze zu Basis y_1, \dots, y_m von A . Dann $\mu_x(y_i) = xy_i \in L(\{y_1, \dots, y_{i-1}\})$ für $1 \leq i \leq m$.

□

Alternativ: $A = (K[X]/K) \oplus W \rightsquigarrow y \in A, y = y_1 + y_2 \Rightarrow x^{m-1}y = x^{m-1}y_1 + 0 \cdot y_2$
 $\Rightarrow x^{m-1}y = x^{m-1}(a_1x + \dots + a_sx^s) = \underbrace{x^m}_{=0} \cdot (a_1 + \dots + a_sx^{s-1}) = 0 \Rightarrow \Phi(x^{m-1}, y) = 0$.

Zuletzt das Lemma zur Zerlegung eines KT Polynoms mod p , das in Bsp. 13.4 benutzt wurde:

13.8. Lemma: Sei $\Phi_m \in \mathbb{Z}[T]$ das m -te Kreisteilungspolynom, $p \nmid m$, sei $e := \text{ord}_m(p)$, und $\bar{\Phi}_m \in \mathbb{F}_p[T]$ das mod p reduzierte Polynom. Gilt weiter $\bar{\Phi}_m = \bar{f}_1 \cdot \bar{f}_2 \cdot \dots$, die $\bar{f}_i \in \mathbb{F}_p[T]$ p.w.v. und irreduzibel, dann ist $r = \frac{\varphi(m)}{e}$, und alle $\deg \bar{f}_i = e$.

Bew.: Sei $x \in \mathbb{C}$, Nst. von Φ_m und etwa Nst. von \bar{f}_1 , sei $E_m | \mathbb{F}_p$ endl. Erweiterung mit primitiven El. x , d.h. $E_m = \mathbb{F}_p(x)$. Dann ist $d := \deg(x) = [E_m : \mathbb{F}_p]$, also $\#E_m = p^d$.

z.z.: $d = e$. Daraus betr. $m = \text{ord}(x)$ in E_m^x , also ist $m | \#E_m^x = p^d - 1$.

• In \mathbb{Z}_m^x gilt $p^d \equiv 1$, so dass $e | d$ folgt. Mit $d \geq 1$ erhalten wir $d \geq e$.

• Laut Def. von e gilt $p^e \equiv 1 \pmod{m}$, d.h. $m | p^e - 1$. Da x eine m -te EW ist, folgt $x^{p^e - 1} = 1$, also $x^{p^e} = x$.

Nun ist x primitives El. von $E_m | \mathbb{F}_p$, und die Abb. $y \mapsto y^p$ ein \mathbb{F}_p -Auto von E_m , so dass für alle $y \in E_m^x$ folgt, dass $y^p = y$ bzw. $y^{p^e - 1} = 1$ gelten muss.

Dabei ist E_m^x eine zyklische Gruppe der Ordnung $p^d - 1$, also folgt $p^d - 1 | p^e - 1$, d.h. $d \leq e$.

□