Algorithmische Zahlentheorie

13.01.2026

$K = \mathbb{Q}(\theta)$ $\quad \theta$ ganz, $m(K) \in \mathbb{Z}[x]$ sei das Mipo

$|\ n < \infty$

$\mathbb{Q}$

$\mathcal{O} \subseteq K$ sei eine Ordnung, z.B. $\mathcal{O} = \mathbb{Z}[\theta]$

Def.: • $\mathcal{O}$ <u>p-maximal</u> $\Leftrightarrow p \nmid [\mathcal{O}_K : \mathcal{O}]$

• $I_p := \sqrt{p\mathcal{O}} = \{ x \in \mathcal{O} \mid \exists m \in \mathbb{N} : x^m \in p\mathcal{O} \}$

<u>Satz von PZ:</u> Sei

$$\mathcal{O}' := \{ x \in K \mid x I_p \subseteq I_p \} \supseteq \mathcal{O}$$

Dann gilt: Entweder

(i) $\mathcal{O}' = \mathcal{O}$ und $\mathcal{O}$ ist p-maximal

oder

(ii) $\mathcal{O}' \supsetneq \mathcal{O}$ und $p \mid [\mathcal{O}' : \mathcal{O}] \mid p^n$

Betrachte p mit $p^2 \mid d(\theta)$ und iteriere mit PZ.

Dedekindkriterium

Sei

$$\overline{m}(x) = \prod_{i=1}^{k} \overline{m}_i(x)^{e_i} \quad \text{in } \mathbb{F}_p[x]$$

$\uparrow$ irred., paarweise verschieden

Setze: $g(x) := \prod_{i=1}^{k} m_i(x)$ in $\mathbb{Z}[x]$

$\uparrow$ normierte Lifts

Dann gilt:

(1) $I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta]$

$\uparrow$ bez. $\mathcal{O} = \mathbb{Z}[\theta]$.

(2) Sei $\overline{h}(x) = \frac{\overline{m}(x)}{\overline{g}(x)} \in \mathbb{F}_p[x]$. Dann gilt:

$$f(x) := \frac{1}{p}\left(g(x)h(x) - m(x)\right) \in \mathbb{Z}[x]$$

und

$\mathcal{O} = \mathbb{Z}[\theta]$ p-max. $\Leftrightarrow (\overline{f}, \overline{g}, \overline{h}) = 1$ in $\mathbb{F}_p[x]$

(3) Sei $\overline{u} = \frac{\overline{m}}{(\overline{f}, \overline{g}, \overline{h})}$ in $\mathbb{F}_p[x]$.

Dann gilt:

(i) $\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{p}u(\theta)\mathbb{Z}[\theta]$

(ii) Falls $d := \deg(\overline{f}, \overline{g}, \overline{h})$, so gilt:

$$[\mathcal{O}' : \mathbb{Z}[\theta]] = p^d, \quad d(\mathcal{O}') = d(\theta) / p^{2d}.$$

Beweis:

(1) klar, $p \in I_p$

$$\bar{m} \mid \bar{g}^n \Rightarrow g(\theta)^n \equiv 0 \pmod{p\mathbb{Z}[\theta]}$$

$$\Rightarrow g(\theta) \in I_p$$

$$\Rightarrow p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta] \subseteq I_p$$

Sei umgekehrt $x \in I_p \subseteq \mathbb{Z}[\theta] = \mathcal{O}$.

$\parallel$

$A(\theta)$ mit $A \in \mathbb{Z}[X]$

Sei $x^m \in p\mathbb{Z}[\theta]$ für geeignetes $m \in \mathbb{N}$.

Also gilt:

$$\bar{A}^m(\bar{\theta}) = 0 \quad \text{in} \quad \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \quad (*)$$

$V := \mathbb{Z}[\theta]/p\mathbb{Z}[\theta]$ ist ein $\mathbb{F}_p$-VR der Dim. n

mit $\mathbb{F}_p$-Basis $\bar{1}, \bar{\theta}, \dots, \bar{\theta}^{n-1}$.

Multiplikation mit $\bar{\theta}$ ist ein Endomorphismus von V mit Minimalpolynom $\bar{m}(X)$.

klar: $\bar{m}(X) \mid$ Mipo von Mult. mit $\bar{\theta}$

Weil $\bar{1}, \bar{\theta}, \dots, \bar{\theta}^{n-1}$ l.u. / $\mathbb{F}_p$

gilt Gleichheit.

Nun folgt:

$$(*) \Rightarrow \bar{m}(x) \mid \bar{A}^m(x)$$

$$\Rightarrow \bar{m}_i(x) \mid \bar{A}^m(x), \quad \forall i$$

$$\Rightarrow \bar{m}_i(x) \mid \bar{A}(x), \quad \forall i$$

$$\Rightarrow \bar{g}(x) \mid \bar{A}(x)$$

$$\Rightarrow A(x) \equiv g(x)\, v(x) \pmod{p\mathbb{Z}[x]}$$

$$\Rightarrow A(\theta) \in g(\theta)\mathbb{Z}[\theta] + p\mathbb{Z}[\theta]$$

(2) folgt aus (3) (ii).

Zu (3) aus (1) folgt:

$$x \in \mathcal{O}' = \{x \in K \mid x I_p \subseteq I_p\} \Leftrightarrow xp,\ xg(\theta) \in I_p$$

$$x \in I_p \subseteq \mathcal{O} = \mathbb{Z}[\theta] \Rightarrow x = \frac{A_1(\theta)}{p} \text{ mit } A_1 \in \mathbb{Z}[x].$$

Lemma: (1) $xp \in I_p \Leftrightarrow \bar{g} \mid \bar{A}_1$ in $\mathbb{F}_p[x]$

(2) Sei $\bar{k} := \bar{f}/(\bar{f}, \bar{g})$. Dann gilt:

$$xg(\theta) \in I_p \Leftrightarrow \bar{h}\bar{k} \mid \bar{A}_1$$

Beweis des Lemmas am Ende.

Weiter im Beweis des Dedekindschen Lemmas.

$$x = \frac{A_1(\theta)}{p} \in I_p \iff \bar{g} \mid \bar{A}_1 \text{ und } \bar{h}\bar{k} \mid \bar{A}_1$$

$$\iff \operatorname{kgV}(\bar{g}, \bar{h}\bar{k}) \mid \bar{A}_1$$

Nutze die Formeln

$$\operatorname{kgV}(g_1, g_2) = \frac{g_1 g_2}{\operatorname{ggT}(g_1, g_2)}, \quad \operatorname{kgV}(hg_1, hg_2) = h \operatorname{kgV}(g_1, g_2)$$

$$\Rightarrow \operatorname{kgV}(\bar{g}, \bar{h}, \bar{k}) = \bar{u}$$

Insgesamt folgt:

$$x \in I_p \iff \bar{u} \mid \bar{A}_1 \iff A_1(\theta) \in p\mathbb{Z}[\theta] + u(\theta)\mathbb{Z}[\theta]$$

$$\iff x \in \mathbb{Z}[\theta] + \frac{1}{p} u(\theta)\mathbb{Z}[\theta].$$

Zu (3)(ii): Ein Vertretersystem von $\mathcal{O}'/\mathbb{Z}[\theta]$ ist gegeben durch

$$\frac{1}{p} u(\theta) A(\theta)$$

mit $\bar{A}(x) \in \mathbb{F}_p[x]$, so daß

$$\deg(\bar{A}) < \deg(\bar{m}) - \deg(\bar{r}_1) \quad \text{(Übung)}$$

Beweis von Lemma (*), Teil (i):

$$x_p \in \mathcal{I}_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta]$$

$$\Leftrightarrow A_1(\theta) \in p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta]$$

$$\Leftrightarrow \bar{g} \mid \bar{A}_1$$

Teil (ii) siehe Buch von Cohen. ∎

Der Round 2 - Algorithmus

Starte $\mathcal{O} = \mathbb{Z}[\theta]$.

Faktorisiere $d(\theta)$ und für jedes p mit $p^2 \mid d(\theta)$ gehe folgendermaßen vor:

Wende das Dedekindkriterium an

$\Rightarrow$ entweder $\mathcal{O}$ ist p-maximal
oder $\mathcal{O} \longleftarrow \mathcal{O}'$

Falls $p^2 \mid d(\mathcal{O})$, berechne $\mathcal{O}'$ nach PZ, solange bis $\mathcal{O}' = \mathcal{O}$. Dann ist $\mathcal{O}'$ p-maximal.

Gehe über zur nächsten Primzahl q mit $q^2 \mid d(\mathcal{O})$

ZIEL: Berechne die HNF von I_p und $\mathcal{O}'$, ausgehend von der HNF von $\mathcal{O}$ (alle HNF's werden bzgl. der $\mathbb{Z}$-Basis $1, \theta, \dots, \theta^{n-1}$).

Lemma: Sei $j \geq 1$ mit $p^j \geq n = [K:\mathbb{Q}]$.
Dann gilt für $R = \mathcal{O}/p\mathcal{O}$:

$$\mathrm{rad}(R) = \ker(x \mapsto x^{p^j})$$

↑ wegen $\mathrm{char}(R) = p$ ist dies eine $\mathbb{F}_p$-lineare Abb., denn:

$$(x+y)^p = x^p + y^p.$$
$$(ax)^p = a x^p \text{ für } a \in \mathbb{F}_p,\ x, y \in R.$$

Zur Erinnerung:

$$\mathrm{rad}(R) = \{ f \in R \mid \exists m \in \mathbb{N} : f^m = 0 \} = \sqrt{(0)}.$$

Beweis:

„$\supseteq$" $x \in \ker(x \mapsto x^{p^j}) \Rightarrow x^{p^j} = 0$

„$\subseteq$" Sei $x \in \mathrm{rad}(R)$

$\Rightarrow m_x : R \to R,\ r \mapsto xr$, ist nilpotent

↑ Mult. mit x

$\Rightarrow$ m_x ist ein $\mathbb{F}_p$-Endom. von R, dessen Eigenwerte gleich 0 sind

$\Rightarrow$ $\chi(x) = x^n$ in $\mathbb{F}_p[X]$

$\uparrow$ char. Polynom

$\Rightarrow$ $x^n = 0$ nach Cayley-Hamilton

$\Rightarrow$ $x^{p^f} = 0$ ∎

Beobachtg: Sei $R = \mathcal{O}/p\mathcal{O}$. Dann gilt:

$$I_p = \mathrm{Lift}(\mathrm{rad}(R)) + p\mathcal{O}$$

Bew: Übung

Sei $\omega_1, \dots, \omega_n$ die die NNF von $\mathcal{O}$.

$\Rightarrow$ $\overline{\omega_1}, \dots, \overline{\omega_n}$ ist $\mathbb{F}_p$-Basis von $R = \mathcal{O}/p\mathcal{O}$

Berechne $\overline{a_{i,k}} \in \mathbb{F}_p$, so daß gilt:

$$\overline{\omega_k}^{p^f} = \sum_{i=1}^{n} \overline{a_{i,k}}\ \overline{\omega_i}$$

Sei $\overline{A} = \left(\overline{a_{i,k}}\right)_{i,k} \in \mathbb{F}_p^{n \times n}$. Dies ist die darstellende Matrix von $x \mapsto x^{p^f}$.

Dann gilt:

$$\mathrm{rad}(R) = \ker(\bar{A})$$

$\ker(\bar{A})$ ist leicht zu berechnen

$\rightsquigarrow$ liefert geliftete Elemente in K

Berechne nun die HNF von diesen Elementen und $p w_1, \dots, p w_n$. Dies liefert die HNF von I_p.

Noch zu tun: Berechne

$$\mathcal{O}' = \{ x \in K \mid x I_p \subseteq I_p \}$$

mittels linearer Algebra über $\mathbb{F}_p$.

<u>Lemma:</u> Sei $\mathcal{U}$ der Kern der $\mathbb{F}_p$-linearen Abb.

$$\begin{aligned} \mathcal{O} &\longrightarrow \mathrm{End}(I_p / pI_p) \\ \alpha &\longmapsto (\bar{\beta} \mapsto \bar{\alpha}\bar{\beta}) \end{aligned}$$

Dann gilt:

$$\mathcal{O}' = \frac{1}{p}\mathcal{U}.$$

<u>Beweis:</u>

„$\subseteq$" Sei $\alpha \in \mathcal{O}' \Rightarrow \alpha p \in I_p \subseteq \mathcal{O}$

$\Rightarrow \alpha = \alpha_1 / p$ mit einem $\alpha_1 \in \mathcal{O}$

z.z. $\alpha_1 \in \mathcal{U}$

Dies ist äquivalent zu: $\alpha_1 \beta \in p I_p$, $\forall \beta \in I_p$

Dazu:

$$\alpha_1 \beta = p \underbrace{\alpha \beta}_{\in I_p, \text{ da } \alpha \in \mathcal{O}'} \in p I_p$$

„$\supseteq$" Sei $\overline{\alpha}\overline{\beta} = 0$ in $I_p / p I_p$ für alle $\beta \in I_p$

$\Rightarrow \alpha\beta \in p I_p$, $\forall \beta \in I_p$

$\Rightarrow \frac{\alpha}{p} \cdot \beta \in I_p$, $\forall \beta \in I_p$

$\Rightarrow \frac{\alpha}{p} \in \mathcal{O}'$ ∎

Anwendung zur expliziten Berechnung von $\mathcal{O}'$:

Aus der Berechnung von I_p haben wir eine $\mathbb{Z}$-Basis $g_1, \dots, g_n$ von I_p. Eine $\mathbb{F}_p$-Basis von $I_p / p I_p$ ist also gegeben durch

$$\overline{g_1}, \dots, \overline{g_n}$$

Eine $\mathbb{F}_p$-Basis von $\mathrm{End}(I_p / p I_p) \simeq \mathrm{Mat}(n, \mathbb{F}_p)$ ist gegeben durch die $\mathbb{F}_p$-linearen Abbildungen

$$f_{ij} : \begin{cases} \overline{g_i} \longmapsto \overline{g_j} \\ \overline{g_s} \longmapsto 0 \ , \quad s \neq i \end{cases}$$

Via obigem Isomorphismus entspricht dies der Matrix, die genau an der Stelle (j,i) ein 1 hat und sonst 0.

Zur Berechnung der darstellenden Matrix von

$$\mathcal{O}/p\mathcal{O} \longrightarrow \mathrm{End}\left(I_p/pI_p\right)$$

$$\overline{\alpha} \longmapsto \left(\overline{\beta} \mapsto \overline{\alpha}\overline{\beta}\right)$$

bez. der $\mathbb{F}_p$-Basen $\overline{\omega}_1, \dots, \overline{\omega}_n$ und f_{ij}, $1 \le i,j \le n$ berechne man $a_{k,i,j} \in \mathbb{F}_p$, so daß gilt

$$\overline{\omega}_k \overline{\varphi}_i = \sum_{j=1}^{n} \overline{a}_{k,i,j} \overline{\varphi}_j$$

Dann gilt: $\overline{\omega}_k \overline{\varphi}_i = \left(\sum_{j=1}^{n} \overline{a}_{k,i,j} f_{ij}\right)\left(\overline{\varphi}_i\right)$,

d.h. die Multiplikation mit $\overline{\omega}_k$ auf I_p/pI_p ist gleich

$$\sum_{j=1}^{n} \overline{a}_{k,i,j} f_{ij},$$

oder mit anderen Worten: die Matrix

$$B = \left(\overline{a}_{k,i,j}\right)_{\substack{(i,j)\ \text{Zeilenindex} \\ k\ \text{Spaltenindex}}} \in \mathbb{F}_p^{n^2 \times n}$$

ist die darstellende Matrix. Berechne nun den Kern von B.

Dies liefert $\overline{v}_1, \dots, \overline{v}_s \in \mathcal{O}/p\mathcal{O}$. Lifte zu $v_1, \dots, v_s \in \mathcal{O}$ und berechne die HNF zu

$$v_1, \dots, v_s, p\omega_1, \dots, p\omega_n$$

Dies liefert $\mathcal{U}$ und damit $\mathcal{O}' = \frac{1}{p}\mathcal{U}$.

Ein Beispiel: $K = \mathbb{Q}(\sqrt{2})$ $\quad d_K = 8$

$\Theta = 15\sqrt{2}$

$m(K) = x^2 - 450$

$d(\Theta) = 4 \cdot 450 = 3^2 \cdot 5^2 \cdot 2^3$

Natürlich wissen wir: $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$.
Wir wollen trotzdem Round 2 von $p=3$ und $p=5$ durchführen.

$p=3$ Eigentlich könnten (und sollten) wir zunächst das Dedekindkriterium anwenden. Zur Übung wenden wir jedoch direkt P2 an.

Berechne von I_3: $\quad \omega_1 = 1, \ \omega_2 = 15\sqrt{2} = \Theta$

$j = 1$ genügt

$$\omega_1^3 = 1, \quad \omega_2^3 = 15^3 \cdot 2 \cdot \sqrt{2} = 2 \cdot 15^2 \cdot \omega_2$$

$$\Rightarrow \overline{A} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow \ker(\bar{A}) = \mathbb{F}_p \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Also ist die HNF von $\begin{pmatrix} p & 0 & 0 \\ 0 & p & 1 \end{pmatrix}$ zu berechnen

$$\rightsquigarrow \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow I_p = \mathbb{Z}_p + \mathbb{Z}\Theta \qquad (\text{für } p=3)$$

<u>Berechne nun Θ'</u> : $\quad g_1 = p \,,\; g_2 = \Theta$

$$\omega_1 g_1 = g_1 \,,\quad \omega_1 g_2 = g_2$$

$$\omega_2 g_1 = 15\sqrt{2} \cdot 3 \equiv 0 \pmod{p\Theta}$$
$$\omega_2 g_2 = \left(15\sqrt{2}\right)^2 = 2 \cdot 15^2 \equiv 0 \pmod{p\Theta}$$

$$\Rightarrow$$

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\Rightarrow U = \ker(B) = \mathbb{F}_p \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Also ist die HNF von

$$\begin{pmatrix} 0 & p & 0 \\ 1 & 0 & p \end{pmatrix}$$

zu berechnen $\rightsquigarrow \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$

$$\Rightarrow \mathcal{O}' = \frac{1}{p}\left(\mathbb{Z}p + \mathbb{Z}\theta\right)$$

$$= \mathbb{Z} + \mathbb{Z}\cdot 5\sqrt{2}$$

Wegen $d(\mathcal{O}') = 5^2 \cdot 2^3$ ist $\mathcal{O}'$ 3-maximal.

$p = 5$ Zur Übung wenden wir das Dedekindkriterium an für $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\cdot 5\sqrt{2} = \mathbb{Z}[5\sqrt{2}]$, $\theta = 5$

Es gilt

$$m(X) = X^2 - 50 \equiv X^2 \pmod{p}$$

$$g(X) = X, \quad h(X) = X, \quad f(X) = 0$$

$$\Rightarrow \operatorname{ggT}(\bar{f}, \bar{g}, \bar{h}) = X$$

$\Rightarrow \mathcal{O}$ ist <u>nicht</u> 5-maximal.

Wir erhalten $u(X) = X$ und

$$\mathcal{O}' = \mathbb{Z}[\theta] + \left(\frac{1}{5}\cdot 5\sqrt{2}\right)\mathbb{Z}[\theta]$$

$$= \mathbb{Z}[\theta] + \sqrt{2}\,\mathbb{Z}[\theta]$$

$$= \langle 1, 5\sqrt{2}, \sqrt{2}, \sqrt{2}\cdot 5\sqrt{2} \rangle_{\mathbb{Z}}$$

$$= \langle 1, \sqrt{2}, 20 \rangle_{\mathbb{Z}} = \langle 1, \sqrt{2} \rangle_{\mathbb{Z}} = \mathcal{O}_K.$$