Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z8: Die additive Struktur von Zahlringen

Stichworte: Ganzheitsbasis, $\operatorname{disc} K$ für Zahlkörper K, disc von quadratischen Zahlkörpern, Beweis von $|N(x)| = \#A/Ax$ mit einer GHB

8.1. **Einleitung:** Die additive Gruppe eines Zahlrings ist frei abelsch vom Rang $n = [K:\mathbb{Q}]$. Deren Basen heißen Ganzheitsbasis des Zahlkörpers. Deren Diskriminante ist unabh. von der Wahl der GHB, also eine Kenngröße des Zahlkörpers, mit der z.B. quadratische ZK unterscheidbar sind. Sei in diesem Kapitel stets K ein ZK mit ZRA.

8.2. **Lemma:** Sei $x_1,\dots,x_n$ eine Basis von $K|\mathbb{Q}$, die $x_1,\dots,x_n$ ganz algebraisch, $d := \operatorname{disc}(x_1,\dots,x_n)$. Dann ist jedes $x \in A$ von der Form $x = m_1\frac{x_1}{d} + \dots + m_n\frac{x_n}{d}$ mit $m_1,\dots,m_n \in \mathbb{Z}$ und $d \mid m_i^2$, $1 \le i \le n$. Diese Darstellung ist immer eindeutig.

Bew.: Schreiben $A \ni x = a_1x_1 + \dots + a_nx_n$, die $a_i \in \mathbb{Q}$. Seien $\sigma_1,\dots,\sigma_n$ die Einbettungen von $K|\mathbb{Q}$ in $\mathbb{C}$. Dann ist $\sigma_i x = \sum_{j=1}^{n} a_j(\sigma_i x_j)$, $1 \le i \le n$.
Dies ist ein lineares Gleichungssystem für $a_1,\dots,a_n$ mit Koeffizientenmatrix $(\sigma_i x_j)_{i,j}$. Sei $\delta = \det((\sigma_i x_j))$. Wegen $\delta^2 = d \neq 0$ ist $(\sigma_i x_j)$ regulär.
Nach der Cramerschen Regel ist dann $a_j = \frac{\det(\dots)}{\delta} =: \frac{e_j}{\delta}$.
Es folgt $\underbrace{da_j}_{\in\mathbb{Q}} = \underbrace{\delta e_j}_{\in A} \in \mathbb{Q} \cap A = \mathbb{Z}$, d.h. es ist $a_j = \frac{m_j}{d}$ für gewisse $m_j \in \mathbb{Z}$.

Also ist $x = m_1\frac{x_1}{d} + \dots + m_n\frac{x_n}{d}$. Nun ist $m_j = \delta e_j$, also $m_j^2 = de_j^2$ und $\frac{m_j^2}{d} = e_j^2 \in \mathbb{Q} \cap A = \mathbb{Z}$, also gilt: $d \mid m_j^2$ für $1 \le j \le n$. $\square$

8.3. **Bsp.:** $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}\setminus\{0,1\}$, $m \equiv 1 \pmod 4$, $A_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ hat 4.4. Autos $\{\mathrm{id}, \sigma\}$ mit $\sigma(\sqrt{m}) = -\sqrt{m}$.
Nimm die $\mathbb{Q}$-Basis $x_1 = 1$, $x_2 = \sqrt{m}$, also $d = \operatorname{disc}(x_1,x_2) = \det^2\begin{pmatrix}1 & \sqrt{m}\\ 1 & -\sqrt{m}\end{pmatrix} = 4m$. Für $x = \frac{u}{2} + \frac{v}{2}\sqrt{m} \in A_K$ also $x = \underbrace{2um}_{\in\mathbb{Z}}\cdot\frac{1}{4m} + \underbrace{2v^2m}_{\in\mathbb{Z}}\cdot\frac{\sqrt{m}}{4m}$ mit $d = 4m \mid (2um)^2, d = 4m \mid (2v^2m)^2$. Wählt man $x_1 = 1$, $x_2 = \frac{1+\sqrt{m}}{2}$, also $d = \operatorname{disc}(x_1,x_2) = \det^2\begin{pmatrix}1 & (1+\sqrt{m})/2\\ 1 & (1-\sqrt{m})/2\end{pmatrix} = \left((1-\sqrt{m})/2 - (1+\sqrt{m})/2\right)^2 = \left(-\sqrt{m}\right)^2 = m$, schreibe $x' = u' + v'\frac{1+\sqrt{m}}{2} \in A_K$, als $x' = \underbrace{um}_{\in\mathbb{Z}}\cdot\frac{1}{m} + \underbrace{vm}_{\in\mathbb{Z}}\cdot\frac{1+\sqrt{m}}{2m}$, wobei $d = m \mid (um)^2$, $d \mid (vm)^2$, ein $x = \underbrace{u+v}_{\text{wo } u \equiv v \pmod 2}\cdot\frac{1+\sqrt{m}}{2} = \underbrace{\frac{2u-2v}{2}}_{\in\mathbb{Z}} + \underbrace{2v}_{\in\mathbb{Z}}\cdot\frac{1+\sqrt{m}}{2}$ $u,v \in \mathbb{Z}$, ebenso.

8.4. **Satz:** Die additive Gruppe des Zahlrings A eines Zahlkörpers K vom Grad n ist frei abelsch vom Rang n.

Bew.: Sei $x_1,\dots,x_n$ eine $\mathbb{Q}$-Basis von K, $\subseteq x_1,\dots,x_n$ ganz.
$\lceil \forall z \in K\ \exists\, m \in \mathbb{Z}\setminus 0 : mz \in A$, da K der Quotientenkörper von A. $\rfloor$
Sei $d := \operatorname{disc}(x_1,\dots,x_n)$. Aus Lemma 8.2 folgt: $\underbrace{\bigoplus_{i=1}^{n} \mathbb{Z} x_i}_{\text{Rang } n} \subseteq A \subseteq \underbrace{\bigoplus_{i=1}^{n} \mathbb{Z} \frac{x_i}{d}}_{\text{Rang } n}$.
Aus Algebra bekannt (Algebra Satz A6.14):
Untergruppen endlich erzeugter frei abelscher Gruppen vom Rang r sind frei abelsch vom Rang $\leq r$, also ist A frei abelsch vom Rang n.
↑ vgl. Algebra A6.8 □

8.5. **Def.:** Basen $x_1,\dots,x_n$ der additiven Gruppe von A heißen Ganzheitsbasen von K. (GHB)
Weiter: $\operatorname{disc} K := \operatorname{disc} A := \operatorname{disc}(x_1,\dots,x_n)$.

8.6. **Bem.:** $\operatorname{disc} K$ hängt nicht von der Wahl von $x_1,\dots,x_n$ ab.

Bew.: Sei $y_1,\dots,y_n$ weitere GHB, $y_i = \sum_j a_{ij} x_j$, die $a_{ij} \in \mathbb{Z}$.
Dann ist $\operatorname{disc}(y_1,\dots,y_n) = (\det((\sigma_\ell y_i)))^2 = (\det(\underbrace{\sum_j a_{ij}(\sigma_\ell x_j)}_{(\sigma_\ell x_j)(a_{ij})^T}))^2$

$$= \operatorname{disc}(x_1,\dots,x_n)\cdot(\det(a_{ij}))^2.$$

Wegen $S=(a_{ij}) \in GL(n,\mathbb{Z})$ ist $\det(a_{ij}) = \pm 1$, da $\det(S\cdot S^{-1}) = \underbrace{\det S}_{\in\mathbb{Z}} \cdot \underbrace{\det S^{-1}}_{\in\mathbb{Z}} = 1$.
Somit folgt $\operatorname{disc}(y_1,\dots,y_n) = \operatorname{disc}(x_1,\dots,x_n)$. □

8.7. **Bem.:** $y_1,\dots,y_n \in A$ GHB $\Leftrightarrow \operatorname{disc}(y_1,\dots,y_n) = \operatorname{disc} K$.

Bew.: „$\Rightarrow$" klar nach 8.6, „$\Leftarrow$": Sei $y_i = \sum_j a_{ij} x_j$, die $a_{ij} \in \mathbb{Z}$. Wegen $\det(a_{ij}) = \pm 1$ ist dann $y_1,\dots,y_n$ Basis von A. □

8.8. **Bsp.:** Sei $K = \mathbb{Q}(\sqrt{m})$, $m \neq 0,1$ quadratfrei. Sei A der ZR von K, nach 4.4 ist dieser

$$A = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{falls } m \equiv 2,3\ (4), \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right], & \text{falls } m \equiv 1\ (4). \end{cases}$$

Für $m \equiv 2,3\ (4)$ ist also $\operatorname{disc} K = \left(\det\begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}\right)^2 = (-2\sqrt{m})^2 = \underline{\underline{4m}}$, und
für $m \equiv 1\ (4)$ ist dann $\operatorname{disc} K = \left(\det\begin{pmatrix} 1 & (1+\sqrt{m})/2 \\ 1 & (1-\sqrt{m})/2 \end{pmatrix}\right)^2 = \underline{\underline{m}}$.

8.9. **Folgerung:** Ist $m_1 \neq m_2$, $m_1, m_2 \in \mathbb{Z} \setminus \{0,1\}$, beide quadratfrei, so folgt $\mathbb{Q}(\sqrt{m_1}) \neq \mathbb{Q}(\sqrt{m_2})$.

8.10. **Korollar:** Sei A der ZR des Zkp K. Dann gilt für $x \in A$: $|N(x)| = \#A/Ax$.

Bew.: Sei $x_1, \dots, x_n$ GHB von K, d.h. $A = \bigoplus_{i=1}^{n} \mathbb{Z} x_i$.
Dann ist $xx_i = \sum_{j=1}^{n} a_{ij} x_j$ mit $a_{ij} \in \mathbb{Z}$.
Es gilt:

$$|N(x)| = |\det \mu_x| = |\det((a_{ij}))| \overset{8.12}{=} \#A/\sum_{i=1}^{n} \mathbb{Z}(xx_i) = \#A/Ax. \qquad \square$$

8.11. **Bsp.:** • Sei $K = \mathbb{Q}(\sqrt{m})$, $m \equiv 2,3 \ (4)$, so dass $x_1 = 1$, $x_2 = \sqrt{m}$ die GHB von K ist.
Dann ist für $y = u + v\sqrt{m} \neq 0$ also $\left\{ \begin{array}{l} y \cdot 1 = u + v\sqrt{m} \\ y\sqrt{m} = vm + u\sqrt{m} \end{array} \right\}$ und $|\det(a_{ij})| = |\det \begin{pmatrix} u & v \\ vm & u \end{pmatrix}| = |u^2 - mv^2| = |N(y)|$.

• Falls A (norm.) euklidisch, gilt für $y \in A, y \neq 0$: $\exists q, r \in A : x = qy + r$, d.h. $x \equiv r \ (Ay)$, wobei $r = 0$ oder $|N(r)| < |N(y)|$ ($|N(r)| \in \mathbb{N}$).
Für $x \in A$ $\exists q, r \in A : x = qy + r$, d.h. $x \equiv r \ (Ay)$, wobei $r = 0$ oder $|N(r)| < |N(y)|$.
Es gibt insg. $\#A/Ay$ viele Restklassen mod Ay, ihre Repräsentanten r sind also so wählbar, dass $0 \leq |N(r)| < |N(y)|$. Wegen 8.10 gilt $\#A/Ay = |N(y)|$, d.h. die verschiedenen r mod Ay haben also alle verschiedenes $|N(r)|$.

8.12. **Satz:** Sei $A = \bigoplus_{i=1}^{n} \mathbb{Z} x_i$ eine freie abelsche Gruppe vom Rang n, sei B eine Untergruppe vom Rang n und $y_1, \dots, y_n$ eine Basis von B, also $B = \bigoplus_{i=1}^{n} \mathbb{Z} y_i$.
Sei $y_i = \sum_{j=1}^{n} a_{ij} x_j$ für $1 \leq i \leq n$ mit $a_{ij} \in \mathbb{Z}$. Dann gilt:
(i) $|\det((a_{ij}))|$ ist unabhängig von der gewählten Basis $y_1, \dots, y_n$.
(ii) Es gibt eine Basis von B, so dass (a_{ij}) obere Dreiecksgestalt hat.
(iii) A/B ist endlich, und $\#A/B = |\det((a_{ij}))|$.

Bew.: (i): Sei $z_1, \dots, z_n$ andere Basis von B, dann $\exists C = (c_{ij}) \in GL(\mathbb{Z}) : y_i = \sum_{j=1}^{n} c_{ij} z_j$, wo C invertierbar in $\mathbb{Z}$ (die z_j können mit einer Matrix $D = (d_{ij}) \in \mathbb{Z}^{n \times n}$ genauso als $\mathbb{Z}$-Linearkombination der y_i geschrieben werden. offenbar: $D = C^{-1}$).
Mit $C \cdot D = I_n$ folgt $\det(C) \cdot \det(D) = 1$ mit $\det(C), \det(D) \in \mathbb{Z}$, also $\det(C) = \pm 1$.
Es folgt $z_i = \sum_j d_{ij} \sum_k a_{jk} x_k = \sum_k \underbrace{\left(\sum_j d_{ij} a_{jk} \right)}_{(D \cdot (a_{ij}))_{ik}} x_k$, also $(b_{ij}) = D \cdot (a_{ij})$ da A frei.
Somit $|\det((b_{ij}))| = \underbrace{|\det(D)|}_{=1} \cdot |\det((a_{ij}))|$. ✓

(ii): Beh.: $\exists z_1,\dots,z_m$ Basis von B : $i>j \Rightarrow b_{ij}=0$.

Zeigen dies mit vollst. Induktion nach n: Für $n=1$ ist die Beh. klar, für $n>1$:

Wähle Basis $z_1,\dots,z_m$ so, dass $0\neq|b_{11}|$ minimal.

Beh.: $\forall i>1 : b_{i1}=0$

Bew.: Sonst sei $b_{i1}=0$ für ein $i>1$. Division mit Rest zeigt:

$\exists q,r\in\mathbb{Z}, |r|<b_{11} : b_{i1}=qb_{11}+r$. Mit $z_i-qz_1\in B$ folgt,

dass $z_1,\dots,z_i-qz_1,\dots,z_m$ Basis von B ist.

⌜ist $a_1z_1+\dots+a_i(z_i-qz_1)+\dots+a_mz_m=0$, folgt $a_1-qa_i=0 \wedge a_j=0$ für $2\leq j\leq m$, insb. $a_1=0$⌟

Nun: $z_2,\dots,z_m\in\bigoplus_{i=2}^{m}\mathbb{Z}x_i$, also: $\bigoplus_{i=2}^{m}\mathbb{Z}z_i$ ist UG von $\bigoplus_{i=2}^{m}\mathbb{Z}x_i$, also ist $\bigoplus_{i=2}^{m}\mathbb{Z}z_i$ freie UG von A vom Rang $m-1$. Laut Induktionsvor. $\exists (b_{ij})_{2\leq i,j\leq m}$ obere Δ-Matrix:

$z_i=\sum_{j=2}^{m}b_{ij}x_j$, somit: $z_i=\sum_{j=1}^{m}b_{ij}x_j$, und ist $i>j$, folgt $b_{ij}=0$. ✓

(iii): Beh.: A/B endlich, nämlich $\#A/B=|\det(a_{ij})|$.

Bew.: Betr. $B=\bigoplus_{i=1}^{m}\mathbb{Z}y_i$, $y_i=\sum_{j\geq i}a_{ij}x_j$ laut (ii).

Sei $A_0:=\bigoplus_{i=2}^{m}\mathbb{Z}x_i$,

dann ist $A_0+B=\sum_{i=2}^{m}\mathbb{Z}x_i+\sum_{i=1}^{m}\mathbb{Z}y_i=\mathbb{Z}a_{11}x_1+A_0$

Also $A/(A_0+B)=\{zx_1+\mathbb{Z}a_{11}x_1+A_0;\ z\in\mathbb{Z}\}$,

so dass $\#A/(A_0+B)=|a_{11}|$ folgt. Ferner ist $A_0\cap B\overset{!}{=}\mathbb{Z}y_2\oplus\dots\oplus\mathbb{Z}y_m$.

⌜"$\supseteq$": $z\in r.S. \Rightarrow z\in B$ ✓ und da (a_{ij}) obere Δ-Matrix, ist auch $z\in A_0$.

"$\subseteq$": $z\in A_0\cap B \Rightarrow z=\sum_{i=2}^{m}b_ix_i$, wäre $z=\beta y_1+s$, $\beta\neq0$, folgte $z\notin A_0$ ↯.

Also ist $z\in r.S.$⌟

Vollst. Induktion auf A_0 (vom Rang $n-1$) und $A_0\cap B<A_0$ angewendet

zeigt: $\#(A_0/A_0\cap B)=|\det\begin{pmatrix}a_{22}&\cdots&a_{2m}\\0&&\vdots\\&&a_{mm}\end{pmatrix}|=|a_{22}|\cdots|a_{mm}|$.

Somit: $\#(A/B)\overset{1.}{=}\#(A_0/B\cap A_0)\cdot\#(A/B+A_0)=|a_{11}|\cdots|a_{m-1}|=|\det(a_{ij})|$. ✓

⌜1. Isom.satz: $A_0/B\cap A_0\cong(A_0+B)/B \Rightarrow \#(A_0/B\cap A_0)\cdot\#(A/B+A_0))=\#(A/(B+A_0))\cdot\#((A_0+B)/B)$

$=\#(A/B)$, denn $(A/B)/(A_0+B)/B\cong A/(A_0+B)$.⌟

□