Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z15: Idealklassengruppe, Klassenzahl

Stichworte: Idealklassengruppe, Klassenzahl, Normschranke mit $\lambda := \prod_i \sum_j |\sigma_i x_j|$, Satz von Dirichlet $h < \infty$, Auffinden der Klassenzahl im Beispiel

---

15.1. **Einleitung:** Die Klassenzahl h eines ZKs K ist die endliche Kardinalität der Klassengruppe $C(K) = I(K)/F(K)$. Es gilt $h=1$ genau wenn K faktoriellen ZR hat.
Die Klassenzahl ist damit eine Art "Maß", wie faktoriell der ZR ist.
Zur Auffindung von h ist nützlich, dass in jedes ganzes Ideal $\mathfrak{a}$ stets ein $x \neq 0$ enthält mit $|N(x)| \leq \lambda N(\mathfrak{a})$, wo λ eine (nur von K abhängige) Konstante ist; jede Idealklasse aus $C(K)$ enthält dann ein ganzes Ideal $\mathfrak{a}$ der Norm $\leq \lambda$. Da $\mathfrak{a}$ in Primideale zerfällt, müssen nur die Klassen der Primideale über $p \leq \lambda$ untersucht werden. Im Bsp. $K = \mathbb{Q}[\sqrt{-5}]$ zeigen wir $h=2$ auf diese Art. Damit rückt die Bedeutung von $\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(x_j)|$ in den Fokus. In Kapitel Z16 werden wir den Wert für λ deutlich verbessern.

15.2. **Erinnerung:** Ist K ein Zahlkörper, so bezeichnet
$I(K)$ die Gruppe der gebrochenen Ideale, und
$F(K)$ die Gruppe der gebrochenen Hauptideale, vgl. 10.14.
Wissen: $F(K) = I(K) \iff A = \mathbb{A} \cap K$ faktoriell, vgl. 10.15.(4) und 11.7.
($F(K)=I(K) \overset{10.15.(4)}{\iff} A$ HIB $\overset{11.7.}{\iff} A$ faktoriell)

15.3. **Def.:** $C(K) := I(K)/F(K)$ heißt Idealklassengruppe von K.
$h := \# C(K)$ heißt Klassenzahl von K.
Weiter sei $cl : I(K) \to C(K)$ die Projektion.

Somit: $h = 1 \iff A = \mathbb{A} \cap K$ faktoriell.
Damit ist die Klassenzahl h eine Kennzahl, "wie faktoriell" ein Zahlring ist.

15.4. **Satz:** Sei K ein Zahlkörper. Dann gibt es ein $\lambda > 0$ so, dass jedes Ideal $\mathfrak{a} \neq 0$ von $A = K \cap \mathbb{A}$ ein Element $x \neq 0$ enthält mit $|N(x)| \leq \lambda N(\mathfrak{a})$.

Bew.: Es ist $N(\mathfrak{a}) = \#A/\mathfrak{a}$, $N((x)) = |N(x)|$. Suchen x mit $(x) \subseteq \mathfrak{a} \subseteq A$.
Sei $x_1, \dots, x_n$ GHB von K, d.h. $A = \bigoplus_{i=1}^{n} \mathbb{Z} x_i$.
Seien $\sigma_1, \dots, \sigma_n$ die Einbettungen von K in $\mathbb{C}$.
Setzen $\lambda := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(x_j)| > 0$, dieses λ (unabh. von $\mathfrak{a}, x$) genügt.

Denn: Sei $m \in \mathbb{N}$ mit $m^n \leq N(\mathfrak{a}) = \#A/\mathfrak{a} < (m+1)^n$.
Betrachte die $(m+1)^n$ Elemente $\sum_{j=1}^{n} m_j x_j \in A$, $0 \leq m_j \leq m$.
Da $\#A/\mathfrak{a} < (m+1)^n$, gibt es also zwei solcher Elemente, die in derselben Restklasse mod $\mathfrak{a}$ liegen. Erhalten so durch Differenzenbildung ein $0 \neq x = \sum_{j=1}^{n} m_j x_j \in \mathfrak{a}$ mit allen $|m_j| \leq m$. Es folgt: $|N(x)| = \left| \prod_{i=1}^{n} \sum_{j=1}^{n} m_j \sigma_i(x_j) \right|$

$\leq m^n \prod_{i=1}^{n} \sum_{j=1}^{m} |\sigma_i(x_j)| = m^n \lambda \leq N(\mathfrak{a}) \cdot \lambda$. ⌟ □

15.5. **Kor.:** Jede Idealklasse enthält ein ganzes Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq \lambda$.

Bew.: Sei C eine Idealklasse, und $\mathfrak{b} \in C^{-1}$ ein ganzes Ideal, $\mathfrak{b} \neq 0$.
Nach 15.4 ex. dann ein $0 \neq x \in \mathfrak{b}$ mit $|N(x)| \leq \lambda N(\mathfrak{b})$.
Setzen nun $\mathfrak{a} := (x) \cdot \mathfrak{b}^{-1} \in C$, ist ganzes Ideal.
Wegen $\mathfrak{a} \cdot \mathfrak{b} = (x)$ ist $N(\mathfrak{a}) \cdot N(\mathfrak{b}) = N((x)) = |N(x)| \leq \lambda N(\mathfrak{b})$,
also $N(\mathfrak{a}) \leq \lambda$. □

15.6. **Satz (von Dirichlet):** Die Idealklassengruppe eines Zahlkörpers ist endlich, d.h. $h < \infty$.

Bew.: Wegen 15.5 gen.z.z.: $\{\mathfrak{a} \subseteq A;\ \mathfrak{a}$ Ideal, $N(\mathfrak{a}) \leq \lambda\}$ ist endlich.
Es ist $N(\mathfrak{a}) = \#A/\mathfrak{a}$, also enthält jedes $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq \lambda$ ein $(0 \neq) q \in \mathbb{N}$ mit $q \leq \lambda^2$ ($q := |N(x)| \leq \lambda N(\mathfrak{a}) \leq \lambda^2$ nach 15.4). Gen.z.z.: Für $q \in \mathbb{N}$ ist $S_q := \{\mathfrak{a} \subseteq A$ Ideal; $q \in \mathfrak{a}\}$ endlich.
Nun: S_q steht in Bijektion mit den Idealen von A/Aq. Da A/Aq endlich, ist also auch S_q endlich. ↳ $\#A/Aq = |N(q)|$ □

15.7. **Bem.:** Sei h die Klassenzahl von K. Dann ist $\mathfrak{a}^h$ Hauptideal für alle Ideale $\mathfrak{a}$ von A.

15.8. **Bsp.:** Sei $K=\mathbb{Q}(\sqrt{-5})$. Dann ist der Zahlring $A=\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell, vgl. 10.2.

In diesem Fall zeigen wir, wie man die Klassenzahl h erhalten kann:

Bestimmung von h: Es ist $\lambda=\prod_{i=1}^{2}\sum_{j=1}^{n}|\sigma_i(x_j)| = (1+\sqrt{5})^2 < 11$.

Jedes Ideal $\mathfrak{a}$ mit $N(\mathfrak{a})\leq 10$ ist Produkt von Primidealen $\mathfrak{p}$ mit $2,3,5$ oder $7\in\mathfrak{p}$.

Nun ist $A\cdot 2 = \mathfrak{p}_2^2 = (\sqrt{-5}+1,2)^2$, $A\cdot 3 = \mathfrak{p}_3\cdot\mathfrak{p}_3' = (\sqrt{-5}+1,3)(\sqrt{-5}+2,3)$,

$A\cdot 5 = \mathfrak{p}_5^2 = (\sqrt{-5})^2$, $A\cdot 7 = \mathfrak{p}_7\cdot\mathfrak{p}_7' = (7,\sqrt{-5}-3)(\sqrt{-5}+3,7)$ laut Zerlegungssatz, s. 13.2.

Für $z=x+y\sqrt{-5}\in\mathbb{Z}[\sqrt{-5}]$ mit $x,y\in\mathbb{Z}$ ist $N(z)=x^2+5y^2\in\{0,1,4,5,6,9,\overset{\geq 10}{\ldots}\}=:\mathcal{N}$.

Dann ist: $N(\mathfrak{p}_2)^2 = N(A\cdot 2) = |N(2)| = 4$, also $N(\mathfrak{p}_2)=2\in\mathcal{N}$, d.h. $\mathfrak{p}_2$ ist nicht Hauptideal, hat Ordnung 2.

- Ebenso: $N(\mathfrak{p}_3)=3\notin\mathcal{N}$, d.h. $\mathfrak{p}_3$ ist kein Hauptideal.

Nun gilt: $z:=1+\sqrt{-5}$ hat Norm 6, also ist $Az=\mathfrak{p}_2\cdot\mathfrak{p}$, wo $\mathfrak{p}\in\{\mathfrak{p}_3,\mathfrak{p}_3'\}$.

Somit ist $cl(\mathfrak{p}) = cl(\mathfrak{p}_2^{-1}) = cl(\mathfrak{p}_2)^{-1} = cl(\mathfrak{p}_2)$.

Wegen $cl(\mathfrak{p})\neq e$ folgt $cl(\mathfrak{p}_3)=cl(\mathfrak{p}_3')=cl(\mathfrak{p}_2)$.

- Ebenso: $\mathfrak{p}_2\cdot\mathfrak{p}_7^{(')} = (7)$ mit $7:=3+\sqrt{-5}$ hat Norm 14, genau: $(7)=\mathfrak{p}_2\cdot\mathfrak{p}$, wo $\mathfrak{p}\in\{\mathfrak{p}_7,\mathfrak{p}_7'\}$, d.h. also $cl(\mathfrak{p}_7)=cl(\mathfrak{p}_2)$.

Resultat: $C(K)$ hat Ordnung 2. Denn: Sei $C\in C(K)$, sei $\mathfrak{a}\in C$ mit $N(\mathfrak{a})\leq\lambda$, und $\mathfrak{a}=\mathfrak{p}\cdot\mathfrak{p}'\cdots\mathfrak{p}^{(n)}$ die PIZ. Dann sind alle $\mathfrak{p},\ldots,\mathfrak{p}^{(n)}\in\{\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_3',\mathfrak{p}_5,\mathfrak{p}_7,\mathfrak{p}_7'\}$.

Also ist $C=cl(\mathfrak{p}_2)$ oder $C=e$. Somit: $h=2$. Insbesondere: A ist nicht faktoriell.

$\hookrightarrow C(K)=\{e, cl(\mathfrak{p}_2)\}$