Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 26

Die Endlichkeit der Klassenzahl

Das Ziel dieser Vorlesung ist es, die Endlichkeit der Idealklassengruppe eines Zahlbereichs zu beweisen. Dies geschieht mit den Gittermethoden der beiden letzten Vorlesungen. Diese Methoden erlauben es prinzipiell auch, die Idealklassengruppe algorithmisch zu berechnen und zu entscheiden, ob ein Zahlbereich faktoriell ist oder nicht.

LEMMA 26.1. *Es sei R ein Zahlbereich. Dann gibt es nur endlich viele Ideale $\mathfrak{a}$ in R, deren Norm unterhalb einer gewissen Zahl liegt.*

Beweis. Es genügt zu zeigen, dass es zu einer natürlichen Zahl n nur endlich viele Ideale $\mathfrak{a}$ in R mit $N(\mathfrak{a}) = n$ gibt. Sei also $\mathfrak{a}$ ein solches Ideal. Dann ist $n \in \mathfrak{a}$ nach Lemma 10.5 und damit entspricht $\mathfrak{a}$ einem Ideal aus $R/(n)$. Dieser Ring ist aber nach Satz 9.14 endlich und besitzt somit überhaupt nur endlich viele Ideale. □

LEMMA 26.2. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei $\mathfrak{a} \neq 0$ ein Ideal. Es sei d_τ eine Familie von n positiven reellen Zahlen zu jeder reellen oder komplexen Einbettung, wobei für konjugiert komplexe Einbettungen die gleiche Zahl vorliege. Ferner gelte*

$$\prod_\tau d_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a})$$

Dann gibt es ein $f \in \mathfrak{a}$, $f \neq 0$, mit der Eigenschaft

$$|\tau(f)| < d_\tau$$

für alle τ.

Beweis. Wir nummerieren die Einbettungen mit $1, \ldots, r$ für die reellen und $r+1, r+2, \ldots, r+2s-1, r+2s$ durch, wobei die konjugiert-komplexen Einbettungen nebeneinander stehen. Wir betrachten die Menge

$$\begin{aligned} M &= \big\{(x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+2s}) \in \mathbb{R}^{r+2s} \mid |x_j| < d_j \\ &\quad \text{für } j = 1, \ldots, r,\ x_{r+j}^2 + x_{r+j+1}^2 < d_{r+j}^2 \text{ für } j = 1, 3, \ldots, 2s-1\big\}. \end{aligned}$$

Dies ist eine Produktmenge aus r Intervallen der Länge $2d_j$ und s Kreisscheiben mit den Radien d_j. Diese Menge ist offensichtlich zentralsymmetrisch und konvex ist. Die Menge ist so nicht kompakt. Wir können aber jedes r_j derart verkleinern, dass die Bedingung nach wie vor erfüllt ist und dann in der

entsprechenden Menge $\leq$ statt $<$ schreiben. Da die Menge ein Produkt aus Intervallen und Kreisen ist, ist ihr Volumen gleich

$$2^r \prod_{j=1}^{r} d_j \cdot \pi^s \prod_{j=r+1}^{r+2s} d_j \; = \; 2^r \pi^s \prod_{j=1}^{n} d_j$$

(man beachte, dass der Flächeninhalt des Kreises durch das zweifache Vorkommen der höheren d_j berücksichtigt wird). Nach Voraussetzung und nach Satz 25.9 ist dieses Volumen größer als

$$\begin{aligned} 2^r \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a}) &= 2^{r+s} \sqrt{|\Delta|} N(\mathfrak{a}) \\ &= 2^{r+s} 2^s \operatorname{Vol}(\mathfrak{N}) \\ &= 2^n \operatorname{Vol}(\mathfrak{N}), \end{aligned}$$

wobei $\mathfrak{N}$ die Grundmasche des Gitters zum Ideal $\mathfrak{a}$ unter der reellen Gesamteinbettung bezeichnet. Nach dem Gitterpunktsatz von Minkowski gibt es einen Gitterpunkt $\neq 0$, der in M liegt. D.h. es gibt ein $f \in \mathfrak{a}$ mit $|\tau_j(f)| < d_j$ für alle j. □

Korollar 26.3. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei d_τ eine Familie von positiven reellen Zahlen zu jeder reellen oder komplexen Einbettung, wobei für konjugiert komplexe Einbettungen die gleiche Zahl vorliege. Ferner gelte*

$$\prod_{\tau} d_\tau \; > \; \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|}$$

Dann gibt es ein $f \in R$, $f \neq 0$, mit der Eigenschaft

$$|\tau(f)| \; < \; d_\tau$$

für alle τ.

Beweis. Dies folgt direkt aus Lemma 26.2, angewendet auf das Einheitsideal $\mathfrak{a} = R$. □

Korollar 26.4. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und mit s Paaren von komplexen Einbettungen. Dann enthält jedes Ideal $\mathfrak{a} \neq 0$ ein Element $f \in \mathfrak{a}$, $f \neq 0$, das die Normschranke*

$$|N(f)| \; \leq \; \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a})$$

erfüllt.

Beweis. Für jede Wahl von positiven reellen Zahlen d_τ (wobei τ die komplexen Einbettungen durchläuft, und wobei die Paarbedingung für nichtreelles τ gelte) mit

$$\prod_{\tau} d_\tau \; > \; \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a})$$

gibt es nach Lemma 26.2 ein $f \in \mathfrak{a}$, $f \neq 0$, mit

$$|\tau(f)| < d_\tau$$

für jede komplexe Einbettung τ. Nach Lemma 7.14 ist somit

$$|N(f)| = \prod_\tau |\tau(f)| < \prod_\tau d_\tau.$$

Würde es kein f mit Betragsnorm unterhalb (einschließlich) der angegebenen Grenze geben, könnte man daraus direkt einen Widerspruch produzieren. □

Lemma 26.5. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und mit s Paaren von komplexen Einbettungen. Dann enthält jede Idealklasse aus der Klassengruppe ein Ideal $\mathfrak{a} \subseteq R$, das die Normschranke*

$$N(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt.

Beweis. Es sei $\mathfrak{c}$ die Idealklasse. Die inverse Idealklasse $\mathfrak{c}^{-1}$ sei durch das Ideal $\mathfrak{b} \subseteq R$ repräsentiert, siehe Lemma 13.5. Nach Korollar 26.4 gibt es ein $f \in \mathfrak{b}$ mit

$$N(f) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|} N(\mathfrak{b}).$$

Dann ist $f \cdot \mathfrak{b}^{-1}$ ein Ideal, da ja $\mathfrak{b}^{-1}$ alle Elemente aus $\mathfrak{b}$ nach R multipliziert, und das $\mathfrak{c}$ repräsentiert. Nach Korollar 12.14 ist

$$N(f \cdot \mathfrak{b}^{-1}) = N(f)N(\mathfrak{b})^{-1} \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|} N(\mathfrak{b})N(\mathfrak{b})^{-1} = \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}.$$

□

Satz 26.6. *Es sei R ein Zahlbereich. Dann ist die Divisorenklassengruppe von R eine endliche Gruppe.*

Beweis. Nach Lemma 26.5 wird jede Klasse in der Klassengruppe durch ein Ideal mit einer Norm repräsentiert, die durch die dort angegebene Schranke beschränkt ist. D.h., dass die Ideale mit einer Norm unterhalb dieser Schranke alle Klassen repräsentieren. Nach Lemma 26.1 gibt es aber überhaupt nur endlich viele Ideale mit einer Norm unterhalb einer gegebenen Schranke. □

Das im Beweis verwendete Lemma bietet prinzipiell eine Abschätzung für die Anzahl der Klassengruppe.

Definition 26.7. Es sei R ein Zahlbereich. Dann nennt man die Anzahl der Elemente in der Klassengruppe von R die *Klassenzahl* von R.

Es ist üblich, die Klassenzahl mit h_R (oder h_K, wenn K der Quotientenkörper ist) zu bezeichnen.

KOROLLAR 26.8. *Es sei R ein Zahlbereich und sei $\mathfrak{a}$ ein Ideal in R. Dann gibt es ein $n \geq 1$ derart, dass $\mathfrak{a}^n$ ein Hauptideal ist.*

Beweis. Für das Nullideal ist die Aussage richtig, sei also $\mathfrak{a}$ von 0 verschieden. Die zugehörige Idealklasse $[\mathfrak{a}]$ besitzt aufgrund von Satz 26.6 in der Idealklassengruppe endliche Ordnung, d.h., dass für ein $n \geq 1$

$$[\mathfrak{a}^n] = [\mathfrak{a}]^n = 0$$

ist. Dies bedeutet aber gerade, dass $\mathfrak{a}^n$ ein Hauptideal ist. □

Wir formulieren noch explizit die folgenden Kriterien für Faktorialität.

KOROLLAR 26.9. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei vorausgesetzt, dass jedes Primideal $\mathfrak{p}$ in R, das die Normbedingung*

$$N(\mathfrak{p}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt, ein Hauptideal sei. Dann ist R faktoriell.

Beweis. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ unterhalb der angegebenen Normschranke. Nach Satz 12.2 ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ mit Primidealen $\mathfrak{p}_i$, und wegen Korollar 12.14 sind die Normen dieser Primideale ebenfalls unter der Schranke. Da all diese Primideale nach Voraussetzung Hauptideale sind, ist auch $\mathfrak{a}$ ein Hauptideal. Da nach Lemma 26.5 jede Idealklasse durch ein Ideal unterhalb der Normschranke repräsentiert wird, bedeutet dies, dass jede Idealklasse durch ein Hauptideal repräsentiert wird. Das heißt die Klassengruppe ist trivial und damit ist nach Satz 14.2 der Ring R faktoriell. □

KOROLLAR 26.10. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei vorausgesetzt, dass jede Primzahl p, die die Normbedingung*

$$p \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt, ein Primfaktorzerlegung besitzt. Dann ist R faktoriell.

Beweis. Es sei $\mathfrak{p}$ ein Primideal derart, dass $N(\mathfrak{p})$ unterhalb der angegebenen Schranke liegt, und es sei $\mathbb{Z}p = \mathfrak{p} \cap \mathbb{Z}$ mit einer Primzahl p. Nach Korollar 8.8 ist die Norm von $\mathfrak{p}$ gleich p^i mit $i \leq n$, so dass auch p unterhalb der Schranke ist und somit nach Voraussetzung eine Primfaktorzerlegung für p besteht. Daraus folgt aber, dass $\mathfrak{p}$ ein Hauptideal ist. Aus Korollar 26.9 folgt die Behauptung. □

KOROLLAR 26.11. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei vorausgesetzt,*

dass jede Primzahl p mit

$$p \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D<0\,, \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D>0\,. \end{cases}$$

in A_D eine Primfaktorzerlegung besitzt. Dann ist A_D faktoriell.

Beweis. Für $D<0$ folgt dies direkt aus Korollar 26.10, für $D>0$ erfordert dies eine zusätzliche Überlegung. □

Beispiel 26.12. Es sei $R=\mathbb{Z}[\sqrt{-5}]$, also $D=-5$ und $\triangle=-20$. Jede Idealklasse enthält ein Ideal $\mathfrak{a}$ der Norm

$$N(\mathfrak{a}) \leq \frac{2\sqrt{20}}{\pi},$$

so dass nur Ideale mit Norm 2 zu betrachten sind. Ein Ideal $\mathfrak{a}$ mit $N(\mathfrak{a})=2$ ist ein Primideal $\mathfrak{p}$ mit $\mathfrak{p}\cap\mathbb{Z}=(2)$. Daher ist

$$\mathfrak{p}=(2,1+\sqrt{-5})=(2,1-\sqrt{-5})$$

die einzige Möglichkeit. Nach Beispiel 10.7 ist $\mathfrak{p}$ kein Hauptideal. Daher ist die Idealklassengruppe isomorph zu $\mathbb{Z}/(2)$, wobei das Nullelement durch die Hauptdivisoren (oder Hauptideale) repräsentiert wird und das andere Element durch $\mathfrak{p}$.

Beispiel 26.13. Es sei $R=A_{-19}$ der quadratische Zahlbereich zu $D=-19$, also $A_{-19}=\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ bzw. $A_{-19}\cong\mathbb{Z}[Y]/(Y^2-Y+5)$. Wir wissen aufgrund von Satz Anhang 2.9, dass R nicht euklidisch ist. Dennoch ist R faktoriell und nach Satz . ein Hauptidealbereich und die Klassengruppe ist trivial. Hierfür benutzen wir Korollar 26.11, d.h. wir haben für alle Primzahlen $p\leq\frac{2\sqrt{|\triangle|}}{\pi}$ zu zeigen, dass sie eine Primfaktorzerlegung in R besitzen. Diese Abschätzung wird nur von $p=2$ erfüllt. Für $p=2$ ist der Restklassenring

$$R/(2)\cong\mathbb{Z}/(2)[Y]/(Y^2+Y+1)$$

ein Körper, so dass 2 träge in R ist und insbesondere eine Primfaktorzerlegung besitzt.

Beispiel 26.14. Wir wollen zeigen, dass der fünfte Kreisteilungsring

$$R_5=\mathbb{Z}[X]/\big(X^4+X^3+X^2+X+1\big)$$

faktoriell ist. Es gibt vier komplexe Einbettungen und die Diskriminante ist nach Lemma 17.16 gleich ±125. Wegen

$$\left(\frac{2}{\pi}\right)^2\sqrt{125}<5$$

ist nach Korollar 26.10 nur zu überprüfen, ob die Primzahlen $p=2,3$ in R_5 eine Primfaktorzerlegung besitzen. Da $\mathbb{Z}/(2)[X]/(X^4+X^3+X^2+X+1)$ und $\mathbb{Z}/(3)[X]/(X^4+X^3+X^2+X+1)$ Körper sind (vergleiche Satz 23.2), sind 2 und 3 sogar Primelemente in R_5.

BEMERKUNG 26.15. Für ein vorgegebenes quadratfreies D kann man grundsätzlich effektiv entscheiden, ob der quadratische Zahlbereich A_D faktoriell ist oder nicht. Für $D < 0$ ist dies genau für

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

der Fall. Es war bereits von Gauß vermutet worden, dass dies alle sind, es wurde aber erst 1967 von Heegner und Stark bewiesen. Man weiß auch, für welche von diesen D der Ganzheitsbereich euklidisch ist, nämlich nach Satz Anhang 2.9 für $D = -1, -2, -3, -7, -11$, aber nicht für die anderen vier Werte.

Für $D > 0$ wird vermutet, dass für unendlich viele Werte der Ganzheitsbereich faktoriell ist. Für $D < 100$ liegt ein faktorieller Bereich für die Werte

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$

$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

vor. Dagegen weiß man (Chatland und Davenport 1950), für welche positiven D der Ganzheitsbereich A_D euklidisch ist, nämlich für

$$D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Abbildungsverzeichnis