Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

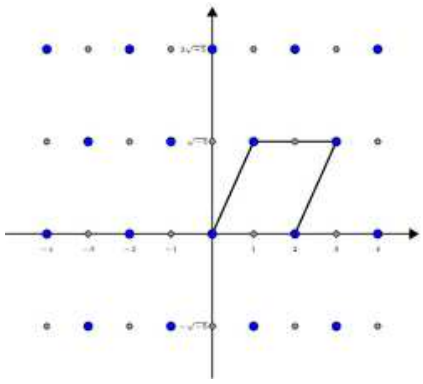
Vorlesung 27

Die Endlichkeit der Klassenzahl für quadratische Zahlkörper

Wir beweisen nun die Endlichkeit der Klassenzahl für die Ganzheitsringe in quadratischen Zahlkörpern. Es sei bemerkt, dass diese Aussage für alle Zahlbereiche gilt, nicht nur für die quadratischen, wir beschränken uns aber auf diese.

LEMMA 27.1. *Sei R ein quadratischer 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 Korollar 21.5 und damit entspricht $\mathfrak{a}$ einem Ideal aus $R/(n)$. Dieser Ring ist aber nach Satz 18.14 endlich und besitzt somit überhaupt nur endlich viele Ideale. □



Das Gitter zum Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ und zum Ideal $(2, 1+\sqrt{-5})$ (blau, mit einer Grundmasche).

BEMERKUNG 27.2. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Wir wollen ein von 0 verschiedenes Ideal $\mathfrak{a}$ aus A_D als ein (vollständiges) Gitter $\Gamma_{\mathfrak{a}}$ in $\mathbb{R}^2$ auffassen. Bei $D < 0$, also im imaginär-quadratischen Fall, verwenden wir die natürliche Einbettung

$$\mathfrak{a} \subseteq A_D \subset L = \mathbb{Q}[\sqrt{D}] \subset \mathbb{C} \cong \mathbb{R}^2.$$

Wir identifizieren also das Ideal mit seinem Bild unter diesen Inklusionen. Dem Element $q_1 + q_2\sqrt{D}$ entspricht in der reellen Ebene das Element

$$(q_1, q_2\sqrt{-D}) \, = \, (q_1, q_2\sqrt{|D|}).$$

Bei $D > 0$, also im reell-quadratischen Fall, verwenden wir stattdessen die Einbettung

$$L = \mathbb{Q}[\sqrt{D}] \longrightarrow \mathbb{R}^2, \, q_1 + q_2\sqrt{D} \longmapsto (q_1, q_2\sqrt{D}).$$

Man beachte, dass in der zweiten Komponente die Wurzel $\sqrt{D}$ mitgeschleppt wird, und dass diese Abbildung lediglich eine $\mathbb{Q}$-lineare Abbildung ist, während im imaginär-quadratischen Fall ein Ringhomomorphismus nach $\mathbb{C}$ vorliegt.

Das Ideal $\mathfrak{a}$ sei nun (bei positivem oder negativem D) durch die $\mathbb{Z}$-Basis (a, b) erzeugt, mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und mit $b = \alpha + \beta u$ wie in Satz 21.1 beschrieben. Hierbei sei $1, u$ die übliche $\mathbb{Z}$-Basis von A_D, also $u = \sqrt{D}$ bzw. $u = \frac{1+\sqrt{D}}{2}$. Das Basiselement u wird auf $(0, \sqrt{|D|})$ bzw. auf $\left(\frac{1}{2}, \frac{\sqrt{|D|}}{2}\right)$ geschickt. Daher wird das zum Ideal gehörige Gitter $\Gamma_{\mathfrak{a}}$ (in $\mathbb{R}^2$) durch

$$(a, 0) \text{ und } \left(\alpha, \beta\sqrt{|D|}\right) \text{ bei } D = 2, 3 \mod 4$$

und

$$(a, 0) \text{ und } \left(\alpha + \frac{\beta}{2}, \beta\frac{\sqrt{|D|}}{2}\right) \text{ bei } D = 1 \mod 4$$

aufgespannt.

Wir setzen zunächst die Norm des Ideals mit dem Flächeninhalt des Gitters in Verbindung.

LEMMA 27.3. *Sei $D \neq 0, 1$ eine quadratfreie Zahl, sei A_D der zugehörige quadratische Zahlbereich und sei $\varphi\colon A_D \to \mathbb{R}^2$ die in Bemerkung 27.2 beschriebene Einbettung. Es sei $\mathfrak{a} \neq 0$ ein Ideal und $\Gamma_{\mathfrak{a}} \subset \mathbb{R}^2$ das zugehörige Gitter. Dann ist der Flächeninhalt der Grundmasche des Gitters gleich*

$$\mu(\Gamma_{\mathfrak{a}}) \, = \, \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a}).$$

Beweis. Das Ideal $\mathfrak{a}$ sei durch die $\mathbb{Z}$-Basis (a, b) mit $(a) = \mathbb{Z} \cap \mathfrak{a}$ und $b = \alpha + \beta u$ erzeugt, wie in Satz 21.1 beschrieben. In Bemerkung 27.2 wurde die zugehörige Gitterbasis ausgerechnet. Der Flächeninhalt eines Gitters wird gegeben durch den Betrag der Determinante von zwei Basiselementen des Gitters. Daher ist bei $D = 2, 3 \mod 4$

$$\mu(\Gamma_{\mathfrak{a}}) \, = \, \left|\det \begin{pmatrix} a & \alpha \\ 0 & \beta\sqrt{|D|} \end{pmatrix}\right| \, = \, a\beta\sqrt{|D|} \, = \, a\beta\frac{\sqrt{|\triangle|}}{2} \, = \, \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|},$$

wobei wir Korollar 21.5 und die Diskriminantengleichung $\triangle = 4D$ benutzt haben.

Bei $D = 1 \mod 4$ ist

$$\mu(\Gamma_{\mathfrak{a}}) = \left|\det \begin{pmatrix} a & \alpha + \frac{\beta}{2} \\ 0 & \frac{\beta\sqrt{|D|}}{2} \end{pmatrix}\right| = a\beta\sqrt{|D|} = \frac{1}{2}N(\mathfrak{a})\sqrt{|\triangle|}$$

aus den gleichen Gründen. □

LEMMA 27.4. *Sei $D \neq 0, 1$ eine quadratfreie Zahl, sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei $\mathfrak{a} \neq 0$ ein Ideal. Dann gibt es ein $f \in \mathfrak{a}$, $f \neq 0$, mit der Eigenschaft*

$$|N(f)| \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a}) & \text{bei } D < 0, \\ \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a}) & \text{bei } D > 0\,. \end{cases}$$

Beweis. Wir wollen den Gitterpunktsatz von Minkowski auf das Gitter $\Gamma = \Gamma_{\mathfrak{a}}$ anwenden, das in Fakt konstruiert wurde. Nach Lemma 27.3 hat die Grundmasche des Gitters den Flächeninhalt $\frac{\sqrt{|\triangle|}N(\mathfrak{a})}{2}$.

Sei $D < 0$. Als Menge T betrachten wir den Kreis um den Nullpunkt mit Radius $\sqrt{\frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a})}$. Der Kreis ist kompakt, zentralsymmetrisch und konvex, und sein Flächeninhalt ist bekanntlich $2\sqrt{|\triangle|}N(\mathfrak{a})$. Dies ist so groß wie das Vierfache des Flächeninhalts der Grundmasche des Gitters, der in Lemma 27.3 berechnet wurde. Also gibt es einen vom Nullpunkt verschiedenen Gitterpunkt $x \in \Gamma \cap T$, und $x = \varphi(f)$ mit $f \in \mathfrak{a}$. Die Norm von f (also das Quadrat des komplexen Betrags) ist dann $N(f) \leq \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{a})$, wie behauptet.

Sei nun $D > 0$. Für einen Punkt $x = (x_1, x_2) = (y_1, y_2\sqrt{D})$ (mit $y_1, y_2 \in \mathbb{Q}$) besitzt das Element $y = \varphi^{-1}(x)$ (aus $Q(A_D)$) die Norm

$$N(y) = y_1^2 - y_2^2 D = (x_1 - x_2)(x_1 + x_2).$$

Die Bedingung

$$|N(y)| = |(x_1 - x_2)(x_1 + x_2)| = c$$

beschreibt somit vier gedrehte Hyperbeln, die jeweils eine Achse senkrecht schneiden. Diese Hyperbeln schließen das (konvexe, kompakte, zentralsymmetrische) Quadrat mit den Eckpunkten $(\pm\sqrt{c}, \pm\sqrt{c})$ ein. Wir setzen $c := \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a})$. Dann hat das Quadrat T mit diesen Eckpunkten den Flächeninhalt $2\sqrt{|\triangle|}N(\mathfrak{a})$ und enthält nach dem Gitterpunktsatz von Minkowski einen vom Nullpunkt verschiedenen Gitterpunkt $x \in \Gamma_{\mathfrak{a}} \cap T$. Dieser entspricht einem Element $f \in \mathfrak{a}$, $f \neq 0$, und

$$|N(f)| = \left|x_1^2 - x_2^2\right| \leq x_1^2 \leq c = \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{a}).$$

□

LEMMA 27.5. *Sei $D \neq 0, 1$ eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Dann enthält jede Idealklasse aus der Klassengruppe ein Ideal $\mathfrak{a} \subseteq A_D$, das die Normschranke*

$$N(\mathfrak{a}) \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0\,, \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

$$\leq$$

erfüllt.

Beweis. Sei c eine Idealklasse. Die inverse Klasse c^{-1} wird durch ein Ideal $\mathfrak{b} \subseteq R$ repräsentiert. Nach Lemma 27.4 enthält $\mathfrak{b}$ ein Element f, $f \neq 0$, mit

$$|N(f)| \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|}N(\mathfrak{b}) & \text{bei } D < 0\,, \\ \frac{1}{2}\sqrt{|\triangle|}N(\mathfrak{b}) & \text{bei } D > 0\,. \end{cases}$$

Wir setzen $\mathfrak{a} := (f)\mathfrak{b}^{-1}$, was nach dem Satz von Dedekind zu $\mathfrak{a}\mathfrak{b} = (f)$ äquivalent ist. Dieses $\mathfrak{a}$ ist ein Ideal, da ja $\mathfrak{b}^{-1}$ nach Bemerkung 24.7 alle Elemente aus $\mathfrak{b}$ nach R multipliziert. Nach Kollorar 21.11 und nach Satz 21.7 ist

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) = N((f)) = |N(f)|\,.$$

Daher ist

$$N(\mathfrak{a}) = \frac{|N(f)|}{N(\mathfrak{b})} \leq \begin{cases} \frac{2}{\pi}\sqrt{|\triangle|} & \text{bei } D < 0\,, \\ \frac{1}{2}\sqrt{|\triangle|} & \text{bei } D > 0\,. \end{cases}$$

□

SATZ 27.6. *Sei $R = A_D$ ein quadratischer Zahlbereich. Dann ist die Divisorenklassengruppe von R eine endliche Gruppe.*

Beweis. Nach Lemma 27.5 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 27.1 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 27.7. Sei A_D ein quadratischer Zahlbereich. Dann nennt man die Anzahl der Elemente in der Klassengruppe von A_D die *Klassenzahl* von A_D.

KOROLLAR 27.8. *Sei $R = A_D$ ein quadratischer 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 27.6 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 beiden folgenden Kriterien für Faktorialität.

KOROLLAR 27.9. *Sei $D \neq 0,1$ eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei vorausgesetzt, dass jedes Primideal $\mathfrak{p}$ in A_D, das die Normbedingung*

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

erfüllt, ein Hauptideal sei. Dann ist A_D faktoriell.

Beweis. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ unterhalb der angegebenen Normschranke. Nach Satz 23.14 ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ mit Primidealen $\mathfrak{p}_i$, und wegen Kollorar 21.11 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 27.5 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 25.2 der Ring A_D faktoriell. □

KOROLLAR 27.10. *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. 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 Satz 20.13 gibt es in A_D die drei Möglichkeiten

$$(p) = \mathfrak{p} \text{ oder } (p) = \mathfrak{p}^2 \text{ oder } (p) = \mathfrak{p}\overline{\mathfrak{p}}\,.$$

Die Norm von $\mathfrak{p}$ ist p oder p^2, 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 27.9 folgt die Behauptung. □

Beispiel 27.11. 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. Beispiel 21.8 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 27.12. 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 25.5, dass R nicht euklidisch ist. Dennoch ist R faktoriell und nach Satz 25.2 ein Hauptidealbereich und die Klassengruppe ist trivial. Hierfür benutzen wir Korollar 27.10, 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.

Abbildungsverzeichnis