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

Algebraische Zahlentheorie

Vorlesung 9

Quadratische Zahlbereiche

Wir beschreiben nun die bisher entwickelten Konzepte im Fall von quadratischen Zahlbereichen genauer. In diesen lassen sich sehr häufig viele Sachen mit einem vertretbaren Aufwand ausrechnen, zugleich zeigen sich aber auch schon viele typische Phänomene der allgemeinen Theorie.

DEFINITION 9.1. Ein *quadratischer Zahlbereich* ist der Ring der ganzen Zahlen in einem Erweiterungskörper von $\mathbb{Q}$ vom Grad 2.

NOTATION 9.2. Zu einer quadratfreien Zahl $D \neq 0,1$ bezeichnet man den zugehörigen quadratischen Zahlbereich, also den Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$, mit

$$A_D\,.$$

Eine quadratische Körpererweiterung der rationalen Zahlen wird durch ein normiertes irreduzibles Polynom beschrieben, das man durch quadratisches Ergänzen auf die Form X^2-q bringen kann. Durch Multiplikation mit einem Quadrat (siehe Aufgabe 9.1) kann man q durch eine quadratfreie ganze Zahl ersetzen. Die quadratische Körpererweiterung kann man also als $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{D}]$ mit einer quadratfreien Zahl $D \neq 0,1$ ansetzen. Ein großer Unterschied besteht je nachdem, ob D positiv oder negativ ist. Im positiven Fall ist $\sqrt{D}$ eine reelle irrationale Zahl, im negativen Fall handelt es sich um eine imaginäre Zahl. Man definiert:

DEFINITION 9.3. Es sei $D \neq 0,1$ quadratfrei und sei A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *reell-quadratisch*, wenn D positiv ist, und *imaginär-quadratisch*, wenn D negativ ist.

DEFINITION 9.4. Es sei $D \neq 0,1$ eine quadratfreie Zahl und sei $\mathbb{Q}[\sqrt{D}]$ die zugehörige quadratische Körpererweiterung und A_D der zugehörige quadratische Zahlbereich. Dann wird der Automorphismus (auf $\mathbb{Q}[\sqrt{D}]$, auf $\mathbb{Z}[\sqrt{D}]$ und auf A_D)

$$a+b\sqrt{D} \longmapsto a-b\sqrt{D}$$

als *Konjugation* bezeichnet.

Wir bezeichnen die Konjugation von z mit $\bar{z}$.

BEMERKUNG 9.5. Im imaginär-quadratischen Fall, wenn also $D < 0$ ist, so ist $\sqrt{D} = \mathrm{i}\sqrt{-D}$ mit $\sqrt{-D}$ reell. Die Konjugation schickt dies dann auf $-\sqrt{D} = -\mathrm{i}\sqrt{-D}$, so dass diese Konjugation mit der komplexen Konjugation übereinstimmt. Im reell-quadratischen Fall allerdings hat die Konjugation $\sqrt{D} \mapsto -\sqrt{D}$ nichts mit der komplexen Konjugation zu tun.

BEMERKUNG 9.6. Bei einer endlichen Körpererweiterung $K \subseteq L$ werden Norm und Spur eines Elementes $x \in L$ über die Determinante und die Spur der Multiplikationsabbildung $f\colon L \to L$ definiert. Im Fall einer quadratischen Erweiterung

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{D}]$$

sind diese beiden Invarianten einfach zu berechnen: Da 1 und $\sqrt{D}$ eine $\mathbb{Q}$-Basis bilden, ist $z = a+b\sqrt{D}$ und damit ist die Multiplikationsmatrix durch

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$

gegeben. Somit ist

$$N(z) = a^2 - b^2 D = (a + b\sqrt{D})(a - b\sqrt{D}) = z\overline{z}$$

und

$$S(z) = 2a = (a + b\sqrt{D}) + (a - b\sqrt{D}) = z + \overline{z}.$$

LEMMA 9.7. *Es sei $\mathbb{Q} \subset L$ eine quadratische Körpererweiterung und $f \in L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn sowohl die Norm als auch die Spur von f zu $\mathbb{Z}$ gehören.*

Beweis. Dies folgt aus Satz 7.5, aus Satz 8.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)), und aus der Gestalt des Minimalpolynoms (nämlich gleich $f^2 - S(f)f + N(f)$, falls $f \notin \mathbb{Q}$) im quadratischen Fall. □

Wir kommen zur expliziten Beschreibung eines quadratischen Zahlbereiches.

SATZ 9.8. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gilt*

$$A_D = \mathbb{Z}[\sqrt{D}], \text{ wenn } D = 2, 3 \mod 4$$

und

$$A_D = \mathbb{Z}[\frac{1+\sqrt{D}}{2}], \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Sei $x \in A_D$ gegeben, $x = a+b\sqrt{D}$, $a, b \in \mathbb{Q}$. Aus Lemma 9.7 folgt

$$N(x) = a^2 - Db^2 \in \mathbb{Z} \text{ und } S(x) = 2a \in \mathbb{Z}\,.$$

Aus der zweiten Gleichung folgt, dass $a = \frac{n}{2}$ mit $n \in \mathbb{Z}$ ist. Sei $b = \frac{r}{s}$ mit r, s teilerfremd, $s \geq 1$. Die erste Gleichung wird dann zu $\left(\frac{n}{2}\right)^2 - D\left(\frac{r}{s}\right)^2 = k \in \mathbb{Z}$ bzw. $n^2 - 4D\left(\frac{r}{s}\right)^2 = 4k$. Dies bedeutet, da r und s teilerfremd sind, dass $4D$ von s^2 geteilt wird. Da ferner D quadratfrei ist, folgt, dass $s = 1$ oder

$s = 2$ ist. Im ersten Fall ist n ein Vielfaches von 2 (da n^2 ein Vielfaches von 4 ist), so dass $x \in \mathbb{Z}[\sqrt{D}]$ ist.

Sei also $s = 2$, was zur Bedingung

$$n^2 - Dr^2 = 4k$$

führt. Wir betrachten diese Gleichung modulo 4. Bei n und r gerade ist $x \in \mathbb{Z}[\sqrt{D}]$. Die einzigen Quadrate in $\mathbb{Z}/(4)$ sind 0 und 1, so dass für $D = 2, 3 \mod 4$ keine weitere Lösung existiert. Für $D = 1 \mod 4$ hingegen gibt es auch noch die Lösung $n = 1 \mod 2$ und $r = 1 \mod 2$, also n und r beide ungerade. Diese Lösungen gehören alle zu $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

Die umgekehrte Inklusion $\mathbb{Z}[\sqrt{D}] \subseteq A_D$ ist klar, sei also $D = 1 \mod 4$. Dann ist aber

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 - \frac{1+\sqrt{D}}{2} = \frac{1+D+2\sqrt{D}-2-2\sqrt{D}}{4} = \frac{D-1}{4} \in \mathbb{Z},$$

und dabei ist $\frac{D-1}{4}$ eine ganze Zahl, so dass dies sofort eine Ganzheitsgleichung über $\mathbb{Z}$ ergibt. □

In den im vorstehenden Satz beschriebenen Fällen kann man jeweils den Ring der ganzen Zahlen durch eine Variable und eine Gleichung beschreiben. Für $D = 2, 3 \mod 4$ ist

$$A_D \cong \mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[X]/(X^2 - D).$$

Für $D = 1 \mod 4$ setzt man häufig $\omega = \frac{1+\sqrt{D}}{2}$ für den Algebra-Erzeuger. Dieser Erzeuger erfüllt die Gleichung $\omega^2 - \omega - \frac{D-1}{4} = 0$. Wir haben also

$$A_D \cong \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right).$$

Wir werden häufiger in beiden Fällen diese Ganzheitsbasis $1, \omega$ nennen, mit $\omega = \sqrt{D}$ im ersten Fall und

$$\omega = \frac{1+\sqrt{D}}{2}$$

im zweiten Fall.

LEMMA 9.9. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann ist die Diskriminante von A_D gleich*

$$\triangle = 4D, \text{ wenn } D = 2, 3 \mod 4$$

und

$$\triangle = D, \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Im Fall $D = 2,3 \mod 4$ ist nach Satz 9.8 $A_D = \mathbb{Z}[X]/(X^2 - D)$ und daher bilden 1 und X eine Ganzheitsbasis. Die möglichen Produkte zu dieser Basis sind in Matrixschreibweise

$$\begin{pmatrix} 1 & X \\ X & D \end{pmatrix}.$$

Wendet man darauf komponentenweise die Spur an so erhält man

$$\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix}$$

und die Determinante davon ist $4D$.

Im Fall $D = 1 \mod 4$ ist hingegen

$$A_D = \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right)$$

und eine Ganzheitsbasis ist 1 und ω. Die Matrix der Basisprodukte ist dann

$$\begin{pmatrix} 1 & \omega \\ \omega & \omega + \frac{D-1}{4} \end{pmatrix}.$$

Wendet man darauf die Spur an (die Spur von ω ist 1), so erhält man

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 + \frac{D-1}{2} \end{pmatrix}$$

und die Determinante davon ist

$$2\left(1 + \frac{D-1}{2}\right) - 1 = 2 + D - 1 - 1 = D.$$

□

Die Summe von Quadraten

Wir haben nun die Mittel an der Hand, um die Zahlen, die die Summe von zwei Quadratzahlen sind, mit Hilfe des Ringes der Gaußschen Zahlen zu charakterisieren.

Satz 9.10. *Es sei p ein ungerade Primzahl. Dann sind folgende Aussagen äquivalent.*

(1) *p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.*
(2) *p ist die Norm eines Elementes aus $\mathbb{Z}$[i].*
(3) *p ist zerlegbar (nicht prim) in $\mathbb{Z}$[i].*
(4) *-1 ist ein Quadrat in $\mathbb{Z}/(p)$.*
(5) *Es ist $p = 1 \mod 4$.*

Beweis. Siehe Aufgabe 9.22. □

Satz 9.11. *Es sei n eine positive natürliche Zahl. Wir schreiben $n = r^2 m$, wobei jeder Primfaktor von m nur einfach vorkomme. Dann ist n die Summe von zwei Quadraten genau dann, wenn in der Primfaktorzerlegung von m nur 2 und Primzahlen vorkommen, die modulo 4 den Rest 1 haben.*

Beweis. Siehe Aufgabe 9.23. □

Noethersche Ringe und Dedekindbereiche

Emmy Noether (1882-1935)

Definition 9.12. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

Korollar 9.13. *Jeder Zahlbereich ist ein noetherscher Ring.*

Beweis. Nach Korollar 8.5 ist jedes von 0 verschiedene Ideal als additive Gruppe isomorph zu $\mathbb{Z}^n$, also ist insbesondere jedes Ideal als abelsche Gruppe endlich erzeugt. Insbesondere sind die Ideale dann als Ideale (also als R-Moduln) endlich erzeugt. □

Satz 9.14. *Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R ist der Restklassenring $R/\mathfrak{a}$ endlich.*

Beweis. Nach Lemma 7.6 gibt es ein $m \in \mathbb{Z} \cap \mathfrak{a}$, $m \neq 0$. Damit ist $mR \subseteq \mathfrak{a}$ und damit hat man eine surjektive Abbildung

$$R/(m) \longrightarrow R/\mathfrak{a}.$$

Der Ring links ist nach Korollar 8.8 endlich (mit m^n Elementen), also besitzt der Ring rechts auch nur endlich viele Elemente. □

Wir geben noch einen zweiten Beweis der vorstehenden Aussage.

Als kommutative Gruppe ist $R = \mathbb{Z}^n$. Sei $a \in \mathfrak{a}$, $a \neq 0$. Dann ist das von a erzeugte Hauptideal eine Untergruppe

$$aR \cong \mathbb{Z}^n \subseteq R \cong \mathbb{Z}^n.$$

Deshalb ist die Restklassengruppe $\mathbb{Z}^n/aR$ endlich und wegen der natürlichen Surjektion $\mathbb{Z}^n/aR \to R/\mathfrak{a}$ ist auch der Restklassenring endlich.

Satz 9.15. *Sei R ein Zahlbereich. Dann ist jedes von 0 verschiedene Primideal von R bereits ein maximales Ideal.*

Beweis. Sei $\mathfrak{p}$ ein Primideal $\neq 0$ in R. Dann ist der Restklassenring $R/\mathfrak{p}$ nach Lemma 3.3 ein Integritätsbereich und nach Satz 9.14 endlich. Ein endlicher Integritätsbereich ist aber nach Aufgabe 5.36 bereits ein Körper, so dass nach Lemma 3.5 ein maximales Ideal vorliegt. □

Richard Dedekind (1831-1916)

Die bisher etablierten Eigenschaften von Zahlbereichen lassen sich im folgenden Begriff zusammenfassen.

Definition 9.16. Einen Integritätsbereich R nennt man einen *Dedekindbereich*, wenn er noethersch und normal ist und wenn jedes von 0 verschiedene Primideal darin maximal ist.

Die Eigenschaft, dass jedes von 0 verschiedene Primideal maximal ist, bedeutet, dass die maximalen Ketten von Primidealen die Form $0 \subset \mathfrak{m}$ besitzen

(wenn ein Körper vorliegt, so gibt es nur das einzige Primideal 0). Man sagt auch, dass die *Krulldimension* des Ringes gleich 1 ist.

KOROLLAR 9.17. *Jeder Zahlbereich ist ein Dedekindbereich.*

Beweis. Dies folgt aus Satz 7.2, aus Korollar 9.13 und aus Satz 9.15. □

SATZ 9.18. *Hauptidealbereiche sind Dedekindbereiche.*

Beweis. Die Normalität folgt aus Satz 2.19 und Satz 6.12. Die Eigenschaft noethersch folgt, da in einem Hauptidealbereich jedes Ideal sogar von einem Element erzeugt wird. Die Maximalität der von 0 verschiedenen Primideale folgt aus Lemma 3.7. □

Abbildungsverzeichnis