

Zahlentheorie

Vorlesung 20

Quadratische Zahlbereiche

DEFINITION 20.1. Ein *quadratischer Zahlbereich* ist der Ring der ganzen Zahlen in einem Erweiterungskörper von \mathbb{Q} vom Grad 2.

Quadratische Zahlbereiche sind zwar die einfachsten Zahlbereiche, sind aber keineswegs einfach, sondern zeigen bereits die Reichhaltigkeit der algebraischen Zahlentheorie.

DEFINITION 20.2. Eine ganze Zahl heißt *quadratfrei*, wenn jeder Primfaktor von ihr nur mit einem einfachen Exponenten vorkommt.

NOTATION 20.3. 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 12.1) kann man q durch eine quadratfreie ganze Zahl ersetzen. Die quadratische Körpererweiterung kann man als $\mathbb{Q} = \mathbb{Q}[\sqrt{D}]$ 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 20.4. Sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *reell-quadratisch*, wenn D positiv ist, und *imaginär-quadratisch*, wenn D negativ ist.

DEFINITION 20.5. 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)

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

als *Konjugation* bezeichnet.

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

BEMERKUNG 20.6. Im imaginär-quadratischen Fall, wenn also $D < 0$ ist, so ist $\sqrt{D} = i\sqrt{-D}$ mit $\sqrt{-D}$ reell. Die Konjugation schickt dies dann auf $-\sqrt{D} = -i\sqrt{-D}$, 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 20.7. Bei einer endlichen Körpererweiterung $K \subseteq L$ werden Norm und Spur eines Elementes $z \in L$ über die Determinante und die Spur der Multiplikationsabbildung $f: L \rightarrow L$ 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

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

und

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

LEMMA 20.8. 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 18.6, aus Satz 15.15, und aus der Gestalt des Minimalpolynoms (nämlich gleich $f^2 + S(f)f + N(f)$, falls $f \notin \mathbb{Q}$) im quadratischen Fall. \square

Wir kommen zur expliziten Beschreibung eines quadratischen Zahlbereiches.

SATZ 20.9. Sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gilt

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

und

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

Beweis. Sei $x \in A_D$ gegeben, $x = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$. Aus Lemma 20.8 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 $D = 2, 3 \pmod{4}$ keine weitere Lösung existiert. Für $D = 1 \pmod{4}$ hingegen gibt es auch noch die Lösung $n = 1 \pmod{2}$ und $r = 1 \pmod{2}$, 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 $D = 1 \pmod{4}$. 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. \square

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

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

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

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

Wie 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 20.10. *Sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich Dann ist die Diskriminante von A_D gleich*

$$\Delta = 4D, \text{ wenn } D = 2, 3 \pmod{4}$$

und

$$\Delta = D, \text{ wenn } D = 1 \pmod{4}.$$

Beweis. Im Fall $D = 2, 3 \pmod{4}$ ist $A_D = \mathbb{Z}[X]/(X^2 - D)$ 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 $D \equiv 1 \pmod{4}$ 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

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

□

Primideale in quadratischen Zahlbereichen

BEMERKUNG 20.11. Das Verhalten von Primzahlen in einer quadratischen Erweiterung lässt sich aus der oben erzielten Beschreibung mit Gleichungen erhalten.

Generell wird bei $R = \mathbb{Z}[X]/(F)$ das Verhalten von p in R durch $(\mathbb{Z}/(p))[X]/(\bar{F})$ beschrieben, wobei \bar{F} bedeutet, dass die ganzzahligen Koeffizienten durch ihre Restklasse modulo p ersetzt werden. Wir nennen den Ring

$$R/(p) = \mathbb{Z}/(p)[X]/(\bar{F}) = \mathbb{Z}[X]/(p, F)$$

den *Faserring* über p .

Bei $D \equiv 2, 3 \pmod{4}$ hat man einfach

$$R/(p) = \mathbb{Z}/(p)[X]/(X^2 - D),$$

wobei man D durch $D \pmod{p}$ ersetzen kann. Die prinzipiellen Möglichkeiten werden in Lemma 19.9 beschrieben. Ob über p ein oder zwei Primideale liegen hängt davon ab, ob D ein Quadratrest modulo p ist und ob p ungerade ist, und p ist prim genau dann, wenn D kein Quadratrest modulo p ist.

Bei $D \equiv 1 \pmod{4}$ hat man

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

Ist p ungerade, so ist 2 eine Einheit in $\mathbb{Z}/(p)$ und man kann quadratisch ergänzen. Dann ist

$$\omega^2 - \omega - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{1}{4} - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{D}{4}.$$

Der Faserring hat daher die Form $\mathbb{Z}/(p)[Y]/(Y^2 - \frac{D}{4})$ und nach Multiplikation der Gleichung mit der Einheit 4 kann man dies als $\mathbb{Z}/(p)[Z]/(Z^2 - D)$ schreiben, so dass es wieder darum geht, ob D ein Quadratrest modulo p ist.

Ist hingegen $p = 2$, so schreibt sich die Gleichung als $\omega^2 + \omega + c$, wobei $c = 1$ ist, wenn $D = 5 \pmod{8}$ ist, und $c = 0$, wenn $D = 1 \pmod{8}$. Im ersten Fall ist die Gleichung irreduzibel über $\mathbb{Z}/(2)$ und 2 ist prim in R , im zweiten Fall ist die Gleichung reduzibel und 2 zerfällt in zwei Primideale.

Damit können wir entscheiden, wie viele Primideale in A_D über einer Primzahl p liegen. Wir wollen darüber hinaus genau beschreiben, wie das Zerlegungsverhalten einer Primzahl in einer quadratischen Erweiterung aussieht, und beginnen mit der Situation, wo p die Diskriminante teilt.

LEMMA 20.12. *Sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Die Primzahl p sei ein Teiler der Diskriminante Δ von A_D . Dann gibt es oberhalb von p genau ein Primideal \mathfrak{p} und es ist $\mathfrak{p}^2 = (p)A_D$.*

Beweis. Sei zunächst $D = 2, 3 \pmod{4}$, so dass $\Delta = 4D$ nach Lemma 20.10 ist und als Primteiler p der Diskriminante 2 und die Teiler von D in Frage kommen. Es ist

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

Bei $p|D$ steht hier $(\mathbb{Z}/(p))[X]/(X^2)$ und dieser Ring hat das einzige Primideal (X) mit $X^2 = 0$. Diesem Primideal entspricht in A_D das Primideal $\mathfrak{p} = (p, X)$. Es ist $\mathfrak{p}^2 = (p)$. Einerseits gilt für $f \in \mathfrak{p}^2$ im Faserring modulo p die Beziehung $f \in (X^2) = 0$, woraus $f \in (p)$ folgt. Andererseits ist $X^2 = D = up$ (in A_D) mit $u \in \mathbb{Z}$. Da D quadratfrei ist, ist u teilerfremd zu p und daher kann man mit $1 = ru + sp$ schreiben

$$p = p(ru + sp) = rup + sp^2 = rX^2 + sp^2 \in \mathfrak{p}^2.$$

Bei $p = 2$ gilt in $\mathbb{Z}/(2)[X]$ die Beziehung $(X - D)^2 = X^2 - D^2 = X^2 - D$, so dass eine analoge Situation vorliegt.

Sei jetzt $D = 1 \pmod{4}$ und sei p ein Primteiler von $\Delta = D$. Es ist

$$\begin{aligned} A_D/(p) &= \left(\mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right) \right) / (p) \\ &= (\mathbb{Z}/(p))[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right). \end{aligned}$$

Da D ungerade ist, ist 2 eine Einheit in $\mathbb{Z}/(p)$, so dass man die Gleichung modulo p als

$$\left(\omega - \frac{1}{2}\right)^2 - \frac{1}{4} - \frac{D-1}{4} = \left(\omega - \frac{1}{2}\right)^2 - \frac{D}{4} = \left(\omega - \frac{1}{2}\right)^2$$

schreiben kann, so dass wieder eine analoge Situation vorliegt. \square

Zu einem Ideal \mathfrak{a} bezeichnet $\bar{\mathfrak{a}}$ das *konjugierte Ideal*, das aus allen konjugierten Elementen aus \mathfrak{a} besteht.

SATZ 20.13. *Sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gibt es für eine Primzahl p die folgenden drei Möglichkeiten:*

- (1) p ist prim in A_D .
- (2) Es gibt ein Primideal \mathfrak{p} in A_D derart, dass $(p) = \mathfrak{p}^2$ ist.
- (3) Es gibt ein Primideal \mathfrak{p} in A_D derart, dass $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ ist mit $\mathfrak{p} \neq \bar{\mathfrak{p}}$.

Beweis. Sei $R = A_D$. Wir betrachten den Restklassenring $L = R/(p)$, der eine quadratische Erweiterung des Körpers $\mathbb{Z}/(p)$ ist. Damit gibt es nach Lemma 19.9 die drei Möglichkeiten:

- (1) L ist ein Körper.
- (2) L ist von der Form $L = \mathbb{Z}/(p)[\epsilon]/\epsilon^2$.
- (3) L ist der Produktring $L \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$.

Im ersten Fall ist p ein Primelement in R . Im zweiten Fall besitzt L genau einen Restklassenkörper als einzigen nicht-trivialen Restklassenring, nämlich $\mathbb{Z}/(p)$. Nach der in Aufgabe 9.15 bewiesenen Korrespondenz gibt es also genau ein Primideal \mathfrak{p} mit $(p) \subseteq \mathfrak{p}$ (das dem Ideal (ϵ) im Restklassenring entspricht). Dann ist $\mathfrak{p} = (p, \epsilon)$ (wobei hier ϵ ein Repräsentant in R sei) und $\mathfrak{p}^2 = (p)$.

Im dritten Fall besitzt L zwei Restklassenkörper und damit zwei maximale Ideale, deren Durchschnitt, das zugleich deren Produkt ist, das Nullideal ist. Zurückübersetzt nach R heißt das, dass es zwei verschiedene Primideale \mathfrak{p} und \mathfrak{q} gibt mit $(p) \subseteq \mathfrak{p}, \mathfrak{q}$ und mit $(p) = \mathfrak{p} \cap \mathfrak{q}$. Nach Aufgabe 18.11 ist $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}$. Mit $(p) \subseteq \mathfrak{p}$ ist auch $(p) \subseteq \bar{\mathfrak{p}}$. Wir zeigen, dass $\bar{\mathfrak{p}} = \mathfrak{q}$ ist, d.h., dass die beiden Primideale über p konjugiert vorliegen. Da nach Lemma 20.12 bei $p|\Delta$ der zweite Fall vorliegt, wissen wir, dass p die Diskriminate nicht teilt.

Bei $D = 2, 3 \pmod{4}$ ist p ungerade und D ist ein Quadratrest modulo p . Seien a und $-a$ die beiden verschiedenen (!) Quadratwurzeln modulo p . Dann werden die beiden Primideale durch $(p, a \pm \sqrt{D})$ beschrieben, und diese sind konjugiert.

Bei $D = 1 \pmod{4}$ und p ungerade ist nach der Bemerkung 20.11 über die explizite Beschreibung der Faserringe D wieder ein Quadratrest modulo p .

Seien a und $-a$ die beiden verschiedenen (!) Quadratwurzeln von D modulo p . Dann ist $\omega - \frac{1}{2} = \pm \frac{a}{2}$ und daher sind die beiden Primideale gleich $(p, \omega \pm a - \frac{1}{2}) = (p, \frac{a \pm \sqrt{D}}{2})$, so dass wieder ein konjugiertes Paar vorliegt.

Bei $D = 1 \pmod{4}$ und $p = 2$ ist nach der Fakt $D = 1 \pmod{8}$. Die Nullstellen des beschreibenden Polynoms sind dann 0 und 1. Daher sind die Primideale darüber gegeben durch $(2, \omega)$ und $(2, \omega - 1)$. Es ist $(2, \omega) = (2, \frac{\sqrt{D+1}}{2})$ und $(2, \omega - 1) = (2, \frac{\sqrt{D+1}}{2} - 1) = (2, \frac{\sqrt{D-1}}{2})$, so dass wieder ein konjugiertes Paar vorliegt. \square