Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z4: Quadratische Zahlringe

Stichworte: reeller oder imaginärer quadratischer Zahlkörper, Zahlring davon, halbganze Zahlen, alle normeuklidischen imaginärquadratischen Zahlkörper, Problem der Bestimmung der faktoriellen quadratischen Zahlkörper

---

4.1. **Einleitung:** Die quadratischen ZK vom Grad 2 sind der einfachste Fall eines Zahlkörpers $\neq \mathbb{Z}$. Wir bestimmen deren Zahlring und alle normeuklidischen imaginärquadratischen ZK. Die Bestimmung aller faktoriellen ZK ist schwierig und nur im imaginärquadratischen bekannt; diese werden von uns erst in Z16 vollständig ermittelt.

4.2. **Def:** Ein (reeller bzw. imaginärer) quadratischer Zahlkörper K ist ein Zahlkörper vom Grad 2 ($\subseteq \mathbb{R}$, $\not\subseteq \mathbb{R}$).

4.3. **Bsp:** Jeder quadr. ZK K ist von der Form $K = \mathbb{Q}(\sqrt{m})$ mit $m \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei, d.h. $\forall p$ prim: $p^2 \nmid m$ (d.h. $\mu^2(m) = 1$).

[Nach dem Satz vom primitiven Element [Algebra A20.16] ist $K = \mathbb{Q}(x)$, wo $x^2 + bx + c = 0$ für $b, c \in \mathbb{Q}$, d.h. $(x + \frac{b}{2})^2 + (c - \frac{b^2}{4}) = 0$.
Also ist $K = \mathbb{Q}(x) = \mathbb{Q}(x + \frac{b}{2}) = \mathbb{Q}(\sqrt{-c + b^2/4})$. Schreiben $\frac{b^2}{4} - c = \frac{u}{v} = \frac{uv}{v^2} = \frac{\tilde{u}^2}{v^2} \cdot m$ mit $u, v \in \mathbb{Z}$, $\tilde{u}, m \in \mathbb{Z}$, mit m qu'frei.
Dann ist $K = \mathbb{Q}(\sqrt{\frac{u}{v}}) = \mathbb{Q}(\frac{\tilde{u}}{v}\sqrt{m}) = \mathbb{Q}(\sqrt{m})$. ⌟

Bem: Damit liegt für $m < 0$ ein imaginärer qu. ZK vor, für $m > 1$ ein reeller qu. ZK.
imaginärquadratisch / reellquadratisch

Wir bestimmen nun den Zahlring der quadratischen Zahlkörper:

4.4. **Satz:** Sei $m \in \mathbb{Z} \setminus \{0,1\}$ qu'frei. Der Zahlring von $\mathbb{Q}(\sqrt{m})$ ist
$\begin{cases} \mathbb{Z}[\sqrt{m}], & \text{falls } m \equiv 2,3 \ (4), \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & \text{falls } m \equiv 1 \ (4). \end{cases}$

Bem: Die Elemente von $\mathbb{Z}[\frac{1+\sqrt{m}}{2}] \setminus \mathbb{Z}[\sqrt{m}]$ werden gelegentlich als halbganze Zahlen bezeichnet.

Im Fall $m \equiv 1\ (4)$, wenn auch halbganze Zahlen im Zahlring liegen, leiten wir noch andere Darstellungen der Menge des Zahlrings her:

4.5. **Bem.:** Sei $m \equiv 1\ (4)$. Dann gilt: $\frac{1}{4}((2T-1)^2 - m) = T^2 - T - \frac{m-1}{4} \in \mathbb{Z}[T]$, daraus folgt, dass $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \overset{!}{=} \left\{u + v\,\frac{1+\sqrt{m}}{2};\ u,v \in \mathbb{Z}\right\} \overset{!!}{=} \left\{\frac{u+v\sqrt{m}}{2};\ u,v \in \mathbb{Z},\ u \equiv v\ (2)\right\}$ (**)

Bew.: Es ist $\left(\frac{1+\sqrt{m}}{2}\right)^2 = \frac{1}{4}(1 + 2\sqrt{m} + m) = \frac{1}{2}(\sqrt{m} + c) = \frac{1}{2}(\sqrt{m} + 1) + d$, mit $m + 1 = 2c$, c ungerade wegen $m \equiv 1\ (4)$, etwa $c = 2d + 1$.

Es folgt: $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{u + v\,\frac{1+\sqrt{m}}{2};\ u,v \in \mathbb{Z}\right\}$. Weiter „$\subseteq$" klar.

„$\supseteq$": $\overset{!!}{}$ Für $u,v \in \mathbb{Z}$ gilt: $u \equiv v\ (2) \Leftrightarrow \exists a,b \in \mathbb{Z}: u = 2a + b \wedge v = b$.

D.h.: $\frac{1}{2}(u + v\sqrt{m}) = \frac{1}{2}(2a + b + b\sqrt{m}) = a + b\,\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Also ist $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{1}{2}(u + v\sqrt{m});\ u,v \in \mathbb{Z},\ u \equiv v\ (2)\right\}$. □

4.6. **Bew. von Satz 4.4:** Sei $x = u + v\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ ganz, $u,v \in \mathbb{Q}$. Das Mipo von x über $\mathbb{Q}$ ist $(T-u)^2 - v^2 m = T^2 - 2uT + (u^2 - v^2 m)$. Nun gilt:

x ganz $\Leftrightarrow 2u \in \mathbb{Z} \wedge u^2 - v^2 m \in \mathbb{Z} \Leftrightarrow 2u \in \mathbb{Z} \wedge (2u)^2 - (2v)^2 m \in 4\mathbb{Z}$

$\Leftrightarrow 2u, 2v \in \mathbb{Z} \wedge (2u)^2 - (2v)^2 m \in 4\mathbb{Z}$. (*)

Bew. des letzten „$\Leftrightarrow$": „$\Leftarrow$" klar, fraglich ist nur „$\Rightarrow$": Sei $a := 2u \in \mathbb{Z}$, $z \in \mathbb{Z}$ mit $a^2 - 4v^2 m = 4z$. Setze $v = \frac{p}{q}$ mit $p,q \in \mathbb{Z} \setminus \{0\}$, $ggT(p,q) = 1$.

Haben $a^2 - 4\frac{p^2}{q^2} m = 4z$, also $a^2 q^2 - 4p^2 m = 4q^2 z$. Somit ist $2 \mid a$ oder $2 \mid q$.

- Falls $2 \mid q$, etwa $q = 2x$, gilt $x^2 a^2 - p^2 m = 4x^2 z$, d.h. $x^2(a^2 - 4z) = p^2 m$.
  Da $ggT(p,x) = 1$, folgt $x^2 \mid m$, und damit $x = \pm 1$ da m quadratfrei.
  Somit ist $2v = \pm p \in \mathbb{Z}$.
- Falls $2 \mid a$, etwa $a = 2b$, gilt $b^2 q^2 - p^2 m = z q^2$ bzw. $q^2(b^2 - z) = p^2 m$.
  Da $ggT(p,q) = 1$, folgt $q^2 \mid m$, und damit $q = \pm 1$ da m quadratfrei.
  Dann ist $v = \pm p$ und insbesondere $2v \in \mathbb{Z}$. ⌋

Zu (*): Die Quadrate mod 4 sind 0 und 1 $\rightsquigarrow$ Betrachte (*) mod 4.

- Falls $m \equiv 2, 3\ (4)$: (*) $\Leftrightarrow u,v \in \mathbb{Z}$, d.h. $x \in \mathbb{Z}[\sqrt{m}]$.
- Falls $m \equiv 1\ (4)$: (*) $\Leftrightarrow 2u, 2v \in \mathbb{Z} \wedge 2u \equiv 2v\ (2)$
  $\Leftrightarrow \exists u', v' \in \mathbb{Z}: u = \frac{u'}{2},\ v = \frac{v'}{2},\ u' \equiv v'\ (2)$
  $\Leftrightarrow x = u + v\sqrt{m} \in \left\{\frac{u' + v'\sqrt{m}}{2};\ u', v' \in \mathbb{Z},\ u' \equiv v'\ (2)\right\}$, d.h. (**). □

4.7. **Bsp.:** • Für $m=-1$ ist $K=\mathbb{Q}(i)$. Der Zahlring ist $\mathbb{Z}[i]$, der Gauß'sche Zahlring, denn $m=-1\equiv 3\ (4)$.

• Für $m=5$ ist $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ der Zahlring von $\mathbb{Q}(\sqrt{5})$.

• Für $m=-3$ ist $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, der Eisensteinsche Zahlring, der Zahlring von $\mathbb{Q}(\sqrt{-3})$.

• $\mathbb{Z}[\sqrt{2}]$ ist der Zahlring von $\mathbb{Q}(\sqrt{2})$.

4.8. **Satz:** Genau die folgenden imaginärquadr. ZK $\mathbb{Q}(\sqrt{m})$ mit $m<0$ sind (norm) euklidisch, also faktoriell: [vgl. Algebra A13.6 : eukl. $\Rightarrow$ HIB; A13.17 : HIB $\Rightarrow$ faktoriell]

$m=-1,-2,-3,-7,-11$.

Bew.: Erinnerung an Def.: Ring A euklidisch bzgl. δ $:\Leftrightarrow \forall x,y\in A\setminus\{0\}\ \exists q,r\in A: x=qy+r$ und $(r=0 \vee \delta(r)<\delta(y))$. $\delta: A\to \mathbb{R}_{\geq 0}$

Sei $N: A\to\mathbb{R}$ (vollständig) multiplikativ (d.h. $\forall a,b\in A: N(ab)=N(a)N(b)$).

• Dann: A euklidisch bzgl. $|N| \Leftrightarrow \forall b\in \mathrm{Quot}(A), b\neq 0\ \exists a\in A: |N(b-a)|<1$

„$\Rightarrow$": Sei $b=\frac{x}{y}\in\mathrm{Quot}(A)$, $b\neq 0$. Dann $\exists q,r\in A: x=qy+r \Leftrightarrow \frac{x}{y}=q+\frac{r}{y}$ mit $r=0$ oder $|N(r)|<|N(y)|$, d.h. mit $|N(b-q)|=0$ oder $|N(b-q)|=|N(\frac{r}{y})|=\frac{|N(r)|}{|N(y)|}<1$. (N mult.)

„$\Leftarrow$": Seien $x,y\in A\setminus\{0\}$, und $b:=\frac{x}{y}\in\mathrm{Quot}(A)$, $b\neq 0$. Dann ex. $a\in A$ mit $|N(b-a)|<1$. (N mult.)

Sei $r:=x-ay\in A$, also $x=ay+r$, also $r=0$ oder $|N(r)|=|N(x-ay)|=|N(b-a)|\cdot|N(y)|<|N(y)|$. (N mult., <1)

• Sei nun m eine der genannten Zahlen. Für $m\in\{-1,-2\}$ ist $\mathbb{Z}[\sqrt{m}]$ der Zahlring, ansonsten $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ laut 4.4. Im ersten Fall nimm $N(x+y\sqrt{m}):=x^2-my^2$, ansonsten $N\left(x+y\cdot\frac{1+\sqrt{m}}{2}\right):=\left(x+\frac{y}{2}\right)^2-m\cdot\left(\frac{y}{2}\right)^2$ als Norm. [Multiplikativität nachrechnen oder elegant argumentieren!]

• Sei $b\in\mathbb{Q}(\sqrt{m})$, etwa $b=r+s\sqrt{m}$ mit $r,s\in\mathbb{Q}$, $b\neq 0$.

Im ersten Fall: Seien $x,y\in\mathbb{Z}$ mit $|r-x|\leq\frac{1}{2}$ und $|s-y|\leq\frac{1}{2}$, setze $a:=x+y\sqrt{m}\in\mathbb{Z}[\sqrt{m}]$.

Dann ist $|N(b-a)|=|(r-x)^2-m(s-y)^2|\leq\frac{1}{4}+|m|\cdot\frac{1}{4}<1$, da $|m|\cdot\frac{1}{4}<\frac{3}{4}$.

Im zweiten Fall: Seien $x,y\in\mathbb{Z}$ mit $|r-x-\frac{1}{2}y|\leq\frac{1}{2}$ und $|2s-y|\leq\frac{1}{2}$, sei $a:=x+y\cdot\frac{1+\sqrt{m}}{2}$.

Dann ist $|N(b-a)|=|(r-x-\frac{1}{2}y)^2-m(s-\frac{1}{2}y)^2|\leq\frac{1}{4}+|m|\cdot\frac{1}{16}\leq\frac{1}{4}+\frac{11}{16}=\frac{15}{16}<1$. □

4.9. **Satz:** Genau die folgenden imaginärquadr. ZK $\mathbb{Q}(\sqrt{m})$ mit $m<0$ haben faktoriellen Zahlring: $m=-1,-2,-3,-7,-11,-19,-43,-67,-163$.

[1967 Stark, Baker: „Klassenzahl 1-Problem"] [faktoriell: s. Z16]

4.10. **Bem.:** Im reellquadr. Fall ($m>0$) wird vermutet, dass $\mathbb{Q}(\sqrt{m})$ für unendlich viele m faktoriellen Zahlring hat.