Quadratische Zahlkörper

Alexander Jakubowski

28-06-2017

Contents

1 Quadratische Zahlkörper

In den vorangegangenen Vorträgen haben wir uns mit allgemeinen Zahlkörpern befasst. In diesem Kapitel soll der Fall einer quadratischen Körpererweiterung F, das heisst

$$[F : \mathbb{Q}] = 2 \ ,$$

genauer beleuchtet werden.

1.1 Integritätsbasis von D

Erinnerung D bezeichnet den Ring der ganzalgebraischen Zahlen in F, das heisst

$$\begin{aligned} D &= \{z \in F \mid \exists\ f \in \mathbb{Z}[T] \text{ mit führendem Koeffizienten 1, sd.} f(z) = 0\} \\ &= F \cap \Omega \ . \end{aligned}$$

Ziel dieses Abschnittes ist es, eine Integritätsbasis $\{\alpha_1, \alpha_2\}$ von D zu finden, das heisst

$$\begin{aligned} D &= \mathbb{Z} \cdot \alpha_1 + \mathbb{Z} \cdot \alpha_2 \text{ und} \\ F &= \mathbb{Q} \cdot \alpha_1 + \mathbb{Q} \cdot \alpha_2 \end{aligned}$$

Satz 1 $F = \mathbb{Q}(\sqrt{d})$ für ein quadratfreies $d \in \mathbb{Z}$.

Beweis Sei $F = \mathbb{Q}(\alpha)$. Da F quadratisch ist, ist α Nullstelle eines Polynoms von Grad zwei. Etwa:

$$a\alpha^2 + b\alpha + c = 0 \ \text{ mit } a, b, c \ \in \mathbb{Z}$$

Und somit:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Bezeichne $A := b^2 - 4ac$.
Da $b,\ 2a \in \mathbb{Z}$, gilt:

$$F = \mathbb{Q}(\sqrt{A})$$

Angenommen, A sei nicht quadratfrei. Also $A = A_1^2 \cdot A_2$ mit $A_1, A_2 \in \mathbb{Z}$ und A_2 quadratfrei. Dann gilt:

$$F = \mathbb{Q}(\sqrt{A}) = \mathbb{Q}(\sqrt{A_1^2 \cdot A_2}) = \mathbb{Q}(\sqrt{A_2})$$

□

Sei σ eine Einbettung von $F/\mathbb{Q}$ nach $\mathbb{C}$. Da σ Elemente aus $\mathbb{Q}$ fixiert, gilt:

$$d = \sigma(d) = \sigma(\sqrt{d}^{\,2}) = \sigma(\sqrt{d})^2 \Rightarrow \sigma(\sqrt{d}) = \pm\sqrt{d}$$

Also

$$Gal(F/\mathbb{Q}) = \{id, \sigma\} \ \cong \mathbb{F}_2$$

Wobei für $\alpha := r + s \cdot\sqrt{d}$ mit $r, s \in \mathbb{Q}$ gilt:

$$\sigma(\alpha) = r - s \cdot\sqrt{d}$$

Jetzt berechnet man leicht Norm und Spur von α:

$$\begin{aligned} N(\alpha) &= id(\alpha) \cdot \sigma(\alpha) = r^2 - ds^2 \\ t(\alpha) &= id(\alpha) + \sigma(\alpha) = 2r \end{aligned}$$

Satz 2 $\alpha \in D \Leftrightarrow t(\alpha), N(\alpha) \in \mathbb{Z}$

Beweis "$\Rightarrow$" Wurde in Kapitel 12 gezeigt.
"$\Leftarrow$" Seien $t(\alpha), N(\alpha) \in \mathbb{Z}$
Setze $\alpha = r + s \cdot\sqrt{d}$. Also gilt $2r, r^2 - ds^2 \in \mathbb{Z}$

Betrachte:

$$\begin{aligned} (x - \alpha)(x - \sigma(\alpha)\ ) &= x^2 - (\alpha + \sigma(\alpha)\ ) \cdot x + \alpha \cdot \sigma(\alpha) \\ &= x^2 - t(\alpha) \cdot x + N(\alpha) \ \in \ \mathbb{Z}[x] \end{aligned}$$

□

Satz 3

$$\begin{aligned} d \equiv 2, 3 \mod 4 &\Rightarrow D = \mathbb{Z} + \mathbb{Z} \cdot\sqrt{d} \\ d \equiv 1 \mod 4 &\Rightarrow D = \mathbb{Z} + \mathbb{Z} \cdot \frac{-1 + \sqrt{d}}{2} \end{aligned}$$

Beweis Sei $\alpha = r + s \cdot\sqrt{d}$. Sei weiterhin $\alpha \in D$, das heisst $2r, r^2 - ds^2 \ \in \mathbb{Z}$. Bezeichne $2r =: m$. Es folgt:

$$\frac{m^2}{4} - ds^2 \ \in \mathbb{Z}$$

Erweitern mit 4 liefert:

$$m^2 - 4ds^2 \in \mathbb{Z}$$

Und da $m \in \mathbb{Z}$, folgt:

$$4ds^2 \in \mathbb{Z}$$

Da d quadratfrei, folgt weiter $2s \in \mathbb{Z}$. Bezeichne $2s =: n$

$$\begin{aligned} \frac{m^2}{4} - \frac{n^2 d}{4} = r^2 - s^2 d \in \mathbb{Z} \\ \Rightarrow \; m^2 - n^2 d \equiv 0(4) \end{aligned}$$

Fall 1 $d \equiv 2, 3(4)$

$$\begin{aligned} m^2 - n^2 d \equiv 0(4) \\ \Rightarrow m^2 + 2n^2 \equiv 0(4) \text{ bzw.} \\ \Rightarrow m^2 + n^2 \equiv 0(4) \end{aligned}$$

Quadrate mod 4 sind 0 und 1. Somit können obige Kongruenzen nur erfüllt sein, wenn $m^2, n^2 \equiv 0(2)$ gilt. Es folgt:

$$m, n \equiv 0(2) \Rightarrow r, s \in \mathrm{Z}$$

Das heisst $\alpha = r + s \cdot \sqrt{d} \in \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$. Also gilt $D \subset \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$.
Die umgekehrte Inklusion folgt leicht, da offenbar gilt:

$$\alpha \in \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d} \Rightarrow t(\alpha), N(\alpha) \in \mathbb{Z}$$

Fall 2 $d \equiv 1(4)$

$$\begin{aligned} m^2 - n^2 d \equiv 0(4) \\ \Rightarrow m^2 - n^2 \equiv 0(4) \end{aligned}$$

Also gilt

$$m \equiv n(2)$$

Das heisst m, n sind beide gerade bzw. ungerade.
Es gilt:

$$\begin{aligned} \alpha &= r + s \cdot \sqrt{d} \\ &= \frac{m + n \cdot \sqrt{d}}{2} \\ &= \frac{m+n}{2} + n \cdot \left(\frac{-1 + \sqrt{d}}{2} \right) \\ &\in \; \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{-1 + \sqrt{d}}{2} \right) \end{aligned}$$

Das heisst $\alpha \in \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{-1+\sqrt{d}}{2}\right)$. Also gilt $D \subset \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$.
Die umgekehrte Inklusion gilt, da für $\alpha := a + b \cdot \frac{-1+\sqrt{d}}{2}$ gilt:

$$\begin{aligned} \alpha &= a - \frac{b}{2} + \frac{b}{2}\sqrt{d} \text{ somit} \\ t(\alpha) &= 2a - b \in \mathbb{Z} \\ N(\alpha) &= a^2 - ab + \frac{b^2}{4} - \frac{b^2}{4}d \\ &= a^2 - ab + \frac{b^2}{4} \cdot (1-d) \in \mathbb{Z} \end{aligned}$$

□

1.2 Diskriminante von F

Mit dem Wissen über die Integritätsbasis von F kann nun die Diskriminante bestimmt werden.

Satz 4 Für $F = \mathbb{Q}(\sqrt{d})$ und dessen Diskriminante δ_F gilt:

$$\begin{aligned} d \equiv 2,3(4) &\Rightarrow \delta_F = 4d \\ d \equiv 1(4) &\Rightarrow \delta_F = d \end{aligned}$$

Beweis

Fall 1 Sei $d \equiv 2,3(4)$. Also $D = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$

$$\begin{aligned} \delta_F &= \Delta(D) \\ &= \Delta(1,\sqrt{d}) \\ &= \det \begin{pmatrix} t(1 \cdot 1) & t(1 \cdot \sqrt{d}) \\ t(\sqrt{d} \cdot 1) & t(\sqrt{d} \cdot \sqrt{d}) \end{pmatrix} \\ &= \det \begin{pmatrix} t(1) & t(\sqrt{d}) \\ t(\sqrt{d}) & t(d) \end{pmatrix} \end{aligned}$$

$$\begin{aligned} t(1) &= id(1) + \sigma(1) \\ &= 1 + 1 \\ &= 2 \end{aligned}$$

$$\begin{aligned} t(\sqrt{d}) &= id(\sqrt{d}) + \sigma(\sqrt{d}) \\ &= \sqrt{d} - \sqrt{d} \\ &= 0 \end{aligned}$$

$$\begin{aligned} t(d) &= id(d) + \sigma(d) \\ &= d + d \\ &= 2d \end{aligned}$$

Insgesamt also:

$$\begin{aligned} \delta_F &= \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} \\ &= 4d \end{aligned}$$

Fall 2 Sei $d \equiv 1(4)$. Also $D = \mathbb{Z} + \mathbb{Z} \cdot \frac{-1+\sqrt{d}}{2}$

$$\begin{aligned} \delta_F &= \Delta(D) \\ &= \Delta(1, \frac{-1+\sqrt{d}}{2}) \\ &= \det \begin{pmatrix} t(1) & t(\frac{-1+\sqrt{d}}{2}) \\ t(\frac{-1+\sqrt{d}}{2}) & t((\frac{-1+\sqrt{d}}{2})^2) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & -1 \\ -1 & \frac{d+1}{2} \end{pmatrix} \\ &= d \end{aligned}$$

□

1.3 Primideale über F

Wiederholung Theorem 3 Kap. 12 §3
Sei $F/\mathbb{Q}$ galoische Körpererweiterung von Grad n und $p \in \mathbb{Z}$ rational prim. Schreibe

$$(p) = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g},$$

wobei die $\mathfrak{p}_i$ Primideale in D sind. Bezeichne mit f_i den Trägheitsgrad von $\mathfrak{p}_i$. Also $|D/\mathfrak{p}_i| = p^{f_i}$ Dann ist:

$$\begin{aligned} e_1 = e_2 = \cdots = e_g =: e \\ f_1 = f_2 = \cdots = f_g =: f \end{aligned}$$

Und es gilt: $efg = n$

Im Fall eines quadratsichen Zahlkörpers gilt also $efg = 2$. Dies ist genau dann erfüllt, wenn einer der Faktoren 2 und die anderen 1 sind. Dies entspricht:

Korollar 5 Für jede rationale Primzahl $p \in \mathbb{Z}$ gilt genau eine der folgenden Aussagen:

1. p zerfällt:
   $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_1$
2. p bleibt prim:
   $(p) = \mathfrak{p}$
3. p verzweigt:
   $(p) = \mathfrak{p}^2$

Satz 6 a Sei p ungerade rationale Primzahl

1. $p \nmid \delta_F$ und $x^2 \equiv d(p)$ ist in $\mathbb{Z}$ lösbar.
   Dann zerfällt p.
2. $p \nmid \delta_F$ und $x^2 \equiv d(p)$ ist in $\mathbb{Z}$ nicht lösbar.
   Dann bleibt p prim.
3. $p|\delta_F$.
   Dann ist p verzweigt.

Beweis

1. Sei $a^2 \equiv d(p)$, dann gilt:

$$\begin{aligned}(p, a+\sqrt{d})(p, a-\sqrt{d}) &= (p)(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}) \\ &= (p)\end{aligned}$$

   Die letzte Gleichheit gilt, denn $(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}) = (1)$, enthält die teilerfremden Elemente p und $2a$. Weiterhin sind die beiden Ideale $(p, a+\sqrt{d})(p, a-\sqrt{d})$ nicht gleich, da sie sonst p und $2a$ enthielten. Es würde folgen $(p) = (1)$. Somit zerfällt p.

2. Angenommen $|D/\mathfrak{p}| = p$.
   Dann wäre die Injektion

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow D/\mathfrak{p}$$

   aus Ordnungsgründen eine Bijektion. Dann gibt es ein $a \in \mathbb{Z}/p\mathbb{Z}$, sodass

$$a \equiv \sqrt{d} \cdot (p)$$

Und Quadrieren liefert:

$$a^2 \equiv d \cdot (p)$$

Haben also Lösung von $x^2 \equiv d(p)$ gefunden. Widerspruch zur Annahme. Somit bleibt p prim.

3.

$$\begin{aligned}(p,\sqrt{d})^2 &= (p)(p,\sqrt{d},\frac{d}{p}) \\ &= (p)\end{aligned}$$

Die letzte Gleichheit gilt, denn $(p,\sqrt{d},\frac{d}{p})$ enthält die teilerfremden Elemente p und $\frac{d}{p}$.

□

Satz 6 b Sei p nun die gerade rationale Primzahl.

1. $2 \nmid \delta_F$ und $d \equiv 1(8)$
   Dann zerfällt 2
2. $2 \nmid \delta_F$ und $d \equiv 5(8)$
   Dann bleibt 2 prim
3. $2|\delta_F$
   Dann ist 2 verzweigt

Beweis

1.

$$\begin{aligned}\left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) &= (2)\left(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8}\right) \\ &= (2)\end{aligned}$$

Die letzte Gleichheit gilt, da $\frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} = 1$

2. Angenommen es gilt $|D/(2)| = 2$
   $\Rightarrow \exists\ a \in \mathbb{Z}\ :\ a \equiv \frac{1+\sqrt{d}}{2}(2)$
   Es gilt:

$$\begin{aligned}\left(\frac{1+\sqrt{d}}{2}\right)^2 - \frac{1+\sqrt{d}}{2} + \frac{1-d}{4} &= 0 \\ \Rightarrow a^2 - a + \frac{1-d}{4} &\equiv 0(2)\end{aligned}$$

Also gilt $\frac{1-d}{4}$ ist gerade somit $d \equiv 1(8)$
Widerspruch zur Vorraussetzung.

3. $2|\delta_F$ Das heisst $d \equiv 2, 3(4)$.
   Falls $d \equiv 2(4)$ betrachte:

$$\begin{aligned}(2, \sqrt{d})^2 &= (4, 2\sqrt{d}, d) \\ &= (2) \cdot (2, \sqrt{d}, \frac{d}{2}) \\ &= (2)\end{aligned}$$

   Die letzte Gleichheit gilt, da 2 und $\frac{d}{2}$ teilerfremd.
   Falls $d \equiv 3(4)$ betrachte:

$$\begin{aligned}(2, 1+\sqrt{d})^2 &= (4, 2+2\sqrt{d}, 1+2\sqrt{d}+d) \\ &= (2) \cdot (2, 1+\sqrt{d}, \sqrt{d}+\frac{1+d}{2}) \\ &= (2)\end{aligned}$$

   Die letzte Gleichheit gilt, da 2 und $\sqrt{d} + \frac{1+d}{2}$ teilerfremd.

□

Bemerkung 7 Die Bedingungen in 6a lassen sich kürzer mit dem Legendre Symbol ausdrücken:

1. $p \nmid \delta_F$ und $x^2 \equiv d(p)$ ist in $\mathbb{Z}$ lösbar.$\Leftrightarrow (\frac{\delta_F}{p}) = 1$
2. $p \nmid \delta_F$ und $x^2 \equiv d(p)$ ist in $\mathbb{Z}$ nicht lösbar.$\Leftrightarrow (\frac{\delta_F}{p}) = -1$
3. $p|\delta_F$.$\Leftrightarrow (\frac{\delta_F}{p}) = 0$

Beweis Falls $\delta_F = d$, so ist obige Aussage trivial. Falls $\delta_F = 4d$, so ist:

$$\begin{aligned}\left(\frac{\delta_F}{p}\right) &= \left(\frac{4}{p}\right) \cdot \left(\frac{d}{p}\right) \\ &= \left(\frac{2}{p}\right)^2 \cdot \left(\frac{d}{p}\right) \\ &= \left(\frac{d}{p}\right)\end{aligned}$$