Quadratische Zahlkörper
Prof. Dr. Werner Bley
Probestudium 2018

Pascal Stucky

31. August 2018

Bei gefundenen Fehlern freue ich mich über eine Nachricht.
E-Mail: vorname.nachname [at] math.lmu.de.

Inhaltsverzeichnis

1 Die komplexen Zahlen **1**
1.1 Die natürlichen Zahlen . . . 1
1.2 Die ganzen Zahlen . . . 1
1.3 Die rationalen Zahlen . . . 1
1.3.1 Konstruktion von $\mathbb{Q}$ . . . 1
1.3.2 Einschub: Äquivalenzrelationen . . . 1
1.4 Die komplexen Zahlen . . . 5
1.4.1 Die komplexe Zahlenebene . . . 6
1.4.2 Die komplexe Konjugation . . . 6
1.4.3 Der komplexe Absolutbetrag . . . 6
1.4.4 Fundamentalsatz der Algebra . . . 7

2 Quadratische Zahlkörper **8**
2.1 Der Ganzheitsring . . . 9
2.2 Der Einheitskreis . . . 11
2.3 Einheiten in Ringen . . . 13
2.4 Zerlegbare und prime Elemente . . . 15
2.5 Faktorielle Ringe . . . 16
2.6 Hauptidealringe . . . 17
2.7 Euklidische Ringe . . . 19

3 Zwei diophantische Probleme **20**
3.1 Die ganzen Gaußschen Zahlen $\mathbb{Z}[i]$ . . . 20
3.2 Eulersches Kriterium . . . 20
3.3 Das zweite Problem . . . 23

Literatur **27**

Das Probestudium orientiert sich am Buch „Quadratische Zahlkörper“ von Franz Lemmermeyer ([Lem17]). Teile des ersten Kapitels sind dem Buch [EHH$^+$83] entnommen.

1 Die komplexen Zahlen

1.1 Die natürlichen Zahlen

Wir verwenden die aus der Schule bekannten *natürlichen Zahlen*

$$\mathbb{N} = \{1, 2, 3, ...\} \ .$$

Diese kann man axiomatisch charakterisieren durch die *Peano-Axiome*.

1.2 Die ganzen Zahlen

Ebenso bekannt sind die *ganzen Zahlen*

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} \ .$$

Hier kann man „vernünftig“ rechnen (addieren, subtrahieren, multiplizieren). Allerdings kann man hier noch nicht durch alle Zahlen dividieren, hierfür benötigen wir die *rationalen Zahlen*.

1.3 Die rationalen Zahlen

1.3.1 Konstruktion von $\mathbb{Q}$

Motivation. Betrachten wir zwei Darstellungen desselben Bruchs, so gilt

$$\frac{a}{b} = \frac{c}{d} \qquad \Longleftrightarrow \qquad ad = bc \ .$$

Formal definiert man auf der Menge

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \quad \ni (a, b)$$

eine *Äquivalenzrelation*

$$(a, b) \sim (c, d) \qquad :\Longleftrightarrow \qquad ad = bc \ .$$

Die Äquivalenzklasse von (a, b) taufen wir $\frac{a}{b}$.

1.3.2 Einschub: Äquivalenzrelationen

Definition 1.1. Eine *Äquivalenzrelation* auf einer Menge M ist ein Zeichen $\sim$, man sagt m_1 ist äquivalent zu m_2, in Zeichen $m_1 \sim m_2$, falls für alle $m_1, m_2, m_3 \in M$ folgendes gilt:

(1) $m_1 \sim m_1$ (reflexiv),

(2) $m_1 \sim m_2 \implies m_2 \sim m_1$ (symmetrisch),

(3) $m_1 \sim m_2, m_2 \sim m_3 \implies m_1 \sim m_3$ (transitiv).

Definition 1.2. Sei $\sim$ eine Äquivalenzrelation auf M. Sei $m \in M$. Dann heißt

$$[m] := \{n \in M \mid n \sim m\}$$

Äquivalenzklasse von m.

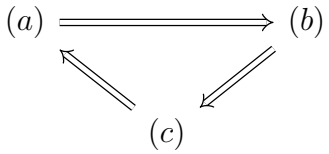
Lemma 1.3 (Hilfssatz)**.** *Sei $\sim$ eine Äquivalenzrelation auf M. Dann sind folgende Aussagen äquivalent:*

(a) $[m] = [n]$,

(b) $[m] \cap [n] \neq \emptyset$,

(c) $m \sim n$.

Beweis. Wir zeigen



„$(a) \implies (b)$“: Diese Folgerung ist klar.
„$(b) \implies (c)$“: Sei $k \in [m] \cap [n]$, d.h.

$$\left.\begin{matrix} k \sim m \\ k \sim n \end{matrix}\right\} \overset{(2)}{\implies} \left.\begin{matrix} m \sim k \\ k \sim n \end{matrix}\right\} \overset{(3)}{\implies} m \sim n \ .$$

„$(c) \implies (a)$“: Hier zeigen wir:

(i) $[m] \subseteq [n]$,

(ii) $[n] \subseteq [m]$.

Zu (i): Sei $k \in [m]$. Dann gilt

$$\left.\begin{matrix} k \sim m \\ m \sim n \end{matrix}\right\} \overset{(3)}{\implies} k \sim n \overset{(2)}{\implies} k \in [n] \ .$$

Zu (ii): Diese Aussage folgt analog. □

Bemerkung. Aus (1) folgt $m \in [m]$, also gilt stets $[m] \neq \emptyset$.

Fazit. Man kann M als paarweise disjunkte Vereinigung über seine Äquivalenzklassen schreiben.

Beispiel 1.4. Wir definieren eine Äquivalenzrelation auf $\mathbb{Z}$. Sei $m \in \mathbb{N}$. Dann ist für $a, b \in \mathbb{Z}$

$$\begin{aligned} a \equiv b \mod m \quad &:\iff \quad m \text{ teilt } a - b \text{ in } \mathbb{Z} \\ &\iff a \text{ und } b \text{ lassen bei Teilen durch } m \text{ denselben Rest.} \end{aligned}$$

Übung 1.5. *Zeige: Dies ist eine Äquivalenzrelation.*

Sei $r \in \mathbb{Z}$. Dann gilt:

$$[r] = \{r + km \mid k \in \mathbb{Z}\} \ .$$

Wir benutzen die Bezeichnung $\overline{r} := [r]$.

Konkret: Sei $m = 3$. Dann ist

$$\begin{aligned} \overline{0} &= \{3k \mid k \in \mathbb{Z}\} = \{..., -3, 0, 3, 6, ...\} \ , \\ \overline{1} &= \{1 + 3k \mid k \in \mathbb{Z}\} = \{..., -5, -2, 1, 4, 7, 10, ...\} \ , \\ \overline{2} &= \{2 + 3k \mid k \in \mathbb{Z}\} = \{..., -1, 2, 5, 8, ...\} \ . \end{aligned}$$

Allgemein: Man hat die Äquivalenzklassen $\overline{0}, \overline{1}, ..., \overline{m-1}$.

Auf der Menge der Äquivalenzklassen kann man eine Addition und eine Multiplikation definieren:

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a + b} \ , \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b} \ . \end{aligned}$$

Beispiele 1.6. Sei $m = 10$. Dann ist

$$\begin{aligned} \overline{5} \cdot \overline{7} &= \overline{35} = \overline{5} \ , \\ \overline{5} + \overline{7} &= \overline{12} = \overline{2} \ . \end{aligned}$$

Die rationalen Zahlen $\mathbb{Q}$ bilden einen *Körper*.

Definition 1.7. Ein *Körper* ist ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und zwei Verknüpfungen

$$\begin{aligned} + \ : \ K \times K &\longrightarrow K \\ (a, b) &\longmapsto a + b \ , \\ \cdot \ : \ K \times K &\longrightarrow K \\ (a, b) &\longmapsto a \cdot b (= ab) \ , \end{aligned}$$

sodass folgende Axiome erfüllt sind:

(a) $(K, +)$ ist eine abelsche Gruppe,

(b) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe,

(c) Es gilt das Distributivgesetz, d.h. für alle $a, b, c \in K$ gilt

$$a \cdot (b + c) = ab + ac \ .$$

Beispiele 1.8. Aus der Schule kennt man die Körper $\mathbb{Q}$ und $\mathbb{R}$.

Definition 1.9. Eine *Gruppe* ist ein Paar $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung

$$\begin{aligned} * : \ G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \ , \end{aligned}$$

sodass gilt:

(i) Für alle $a, b, c \in G$ gilt

$$a * (b * c) = (a * b) * c \qquad \text{(Assoziativität)}.$$

(ii) Es gibt ein Element $e \in G$, sodass für alle $a \in G$ gilt:

$$a * e = e * a = a \qquad \text{(Existenz eines neutralen Elements)}.$$

(iii) Zu jedem $a \in G$ gibt es ein $b \in G$ mit

$$a * b = b * a = e \qquad \text{(Existenz eines inversen Elements)}.$$

Falls zusätzlich gilt

(iv) Für alle $a, b \in G$ ist $a * b = b * a$,

so nennt man G *abelsch* (oder *kommutativ*).

Beispiele 1.10. (1) $(\mathbb{Q}, +)$ ist abelsche Gruppe mit neutralem Element 0 und Inversem $-a$.

(2) Schreibe $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ oder allgemein $K^\times := K \setminus \{0\}$. Dann ist $(\mathbb{Q}^\times, \cdot)$ eine abelsche Gruppe mit neutralem Element 1 und Inversem $\frac{1}{a} = a^{-1}$.

(3) Rechnen mit Resten:

$\mathbb{Z}/m\mathbb{Z}$ sei die Menge der Äquivalenzklassen bzgl. $a \equiv b \mod m$.

$\mathbb{Z}/10\mathbb{Z}$ ist kein Körper, denn:

$$\underbrace{\overline{2}}_{\neq \overline{0}} \cdot \underbrace{\overline{5}}_{\neq \overline{0}} = \overline{10} = \overline{0}$$

$\mathbb{Z}/3\mathbb{Z}$ ist ein Körper. Wir rechnen die Existenz des Inversen nach:

$$\begin{aligned} \overline{1}^{-1} &= \overline{1} \ , \\ \overline{2}^{-1} &= \overline{2} \ , \end{aligned}$$

denn $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$. Weiter ist $-\overline{a} = \overline{-a}$, konkret heißt das

$$\overline{1} + \overline{2} = \overline{3} = \overline{0}$$

und somit

$$\begin{aligned} -\overline{1} &= \overline{2} \ , \\ -\overline{2} &= \overline{1} \ . \end{aligned}$$

Als weiteres konkretes Beispiel berechnen wir die Multiplikationstabelle für $\mathbb{Z}/5\mathbb{Z}$:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Daraus lesen wir ab:

$$\begin{aligned}\overline{1}^{-1} &= \overline{1}\ ,\\ \overline{2}^{-1} &= \overline{3}\ ,\\ \overline{3}^{-1} &= \overline{2}\ ,\\ \overline{4}^{-1} &= \overline{4}\ .\end{aligned}$$

Insgesamt sehen wir so, dass $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ ein Körper ist.

Satz 1.11. *$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper, falls p eine Primzahl ist.*

1.4 Die komplexen Zahlen

Die reellen Zahlen haben einen Makel, z.B. hat $X^2 + 1$ keine Nullstelle in $\mathbb{R}$.
Wir erweitern $\mathbb{R}$ zu der Menge

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$$

wobei

$$i^2 = -1$$

ist.
Wir definieren eine Addition

$$(a + bi) + (c + di) := (a + c) + (b + d)i$$

und eine Multiplikation

$$(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$$

auf $\mathbb{C}$.

Satz 1.12. *$\mathbb{C}$ ist ein Körper.*

Beweisskizze. Den Nachweis der meisten Axiome erbringt man durch Nachrechnen. Das ist hier rein formal und nicht schwer. Wir begnügen uns hier deshalb mit der Angabe der neutralen Elemente und der Inversen.
Die neutralen Elemente bzgl. $+$ und $\cdot$ sind

$$\begin{aligned}0 &= 0 + 0 \cdot i\ ,\\ 1 &= 1 + 0 \cdot i\ .\end{aligned}$$

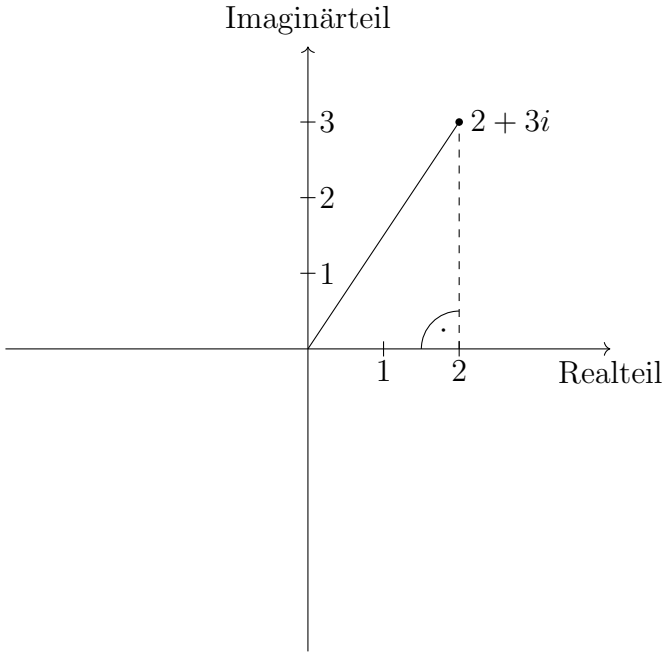
Die inversen Elemente bzgl. $+$ und $\cdot$ sind

$$\begin{aligned}-(a + bi) &= (-a) + (-b)i\ ,\\ (a + bi)^{-1} &= \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \qquad \text{für } (a, b) \neq (0, 0)\ .\end{aligned}$$

□

1.4.1 Die komplexe Zahlenebene

Wir stellen uns die komplexen Zahlen als Ebene vor und können wie unten eingezeichnet eine komplexe Zahl mit einem Punkt in dieser Ebene identifizieren:



1.4.2 Die komplexe Konjugation

Die komplexe Konjugation ist die Abbildung

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{C} \\ z = a + bi &\longmapsto \overline{z} = a - bi \ . \end{aligned}$$

Dies entspricht der Spiegelung an der x-Achse.

1.4.3 Der komplexe Absolutbetrag

Wir definieren für $z = a + bi$

$$|z| := \sqrt{a^2 + b^2} = \sqrt{z\overline{z}} \ .$$

Betrachtet man obigen Punkt in der komplexen Zahlenebene, so ist dies genau der Betrag des Ortsvektors, der sich aus dem Satz des Pythagoras ergibt.

Leichte Rechenregeln

Es gilt für $z = a + ib \in \mathbb{C}, z_1, z_2 \in \mathbb{C}$:

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2} \ , \\ \overline{z_1 \cdot z_2} &= \overline{z_1} \cdot \overline{z_2} \ , \\ z \in \mathbb{R} \quad &\Longleftrightarrow \quad \overline{z} = z \ , \\ |z|^2 &= z\overline{z} = a^2 + b^2 \ , \\ |z_1 z_2| &= |z_1| \, |z_2| \ . \end{aligned}$$

1.4.4 Fundamentalsatz der Algebra

Motivation. Das Polynom X^2+1 hat keine Nullstelle in $\mathbb{R}$, aber in $\mathbb{C}$, nämlich $\pm i$.

Satz 1.13 (Fundamentalsatz der Algebra)**.** *Jedes Polynom n-ten Grades $f \in \mathbb{C}[X]$ hat genau n Nullstellen (mit Vielfachheiten gezählt).*

Der Beweis wird am besten in der Funktionentheorie erbracht.

Beispiel 1.14. Sei $f(X) = aX^2 + bX + c$, $a, b, c \in \mathbb{R}$, $a \neq 0$. Dann hat $f(X)$ die Nullstellen

$$x_{1/2} = \frac{-b}{2a} \pm \frac{1}{2a}\sqrt{\underbrace{b^2 - 4ac}_{\in\mathbb{R}}} \, .$$

Es reicht also für $r \in \mathbb{R}$ eine Wurzel zu ziehen. Sei dazu $z \in \mathbb{C}$ mit $z^2 = r$. Dann:

$$\begin{aligned} r = 0 \quad &\Longrightarrow \quad z = 0 \, , \\ r > 0 \quad &\Longrightarrow \quad z = \pm\sqrt{r} \, , \\ r < 0 \quad &\Longrightarrow \quad z = \pm i\sqrt{|r|} \, . \end{aligned}$$

Konkrete Beispiele:

$$\begin{aligned} \sqrt{-2} &= i\sqrt{2} \, , \\ \sqrt{-m} &= i\sqrt{m} \, , \quad m \in \mathbb{N} \, . \end{aligned}$$

2 Quadratische Zahlkörper

Motivation. (1) Betrachte $Y^2 = X^3 + 1$.

Ziel: Es gibt nur endlich viele Punkte $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ mit $y^2 = x^3 + 1$, nämlich

$$(-1, 0),\ (0, \pm 1),\ (2, \pm 3).$$

(2) Sei p eine ungerade Primzahl.

Frage: Wann gibt es $x, y \in \mathbb{Z}$ mit

$$p = x^2 + y^2\ ?$$

Beispiele:

$$\begin{aligned} 2 &= 1^2 + 1^2\ , \\ 3 &\text{ geht nicht}, \\ 5 &= 1^2 + 2^2\ , \\ 7, 11 &\text{ geht nicht}, \\ 13 &= 2^2 + 3^2\ . \end{aligned}$$

Satz 2.1. *Es gibt genau dann $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$, wenn $p \equiv 1 \mod 4$ ist.*

Etwas genauer:

$$p = x^2 + y^2 = (x + iy)(x - iy)\ .$$

Hier ist

$$x + iy \in \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \underbrace{\{a + bi \mid a, b \in \mathbb{Q}\}}_{\text{Körper}}\ .$$

Definition 2.2. Sei $m \in \mathbb{Z} \setminus \{0, 1\}$ eine quadratfreie Zahl. Dann nennt man

$$\mathbb{Q}(\sqrt{m}) := \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

einen *quadratischen Zahlkörper*. Falls $m > 0$, so heißt $\mathbb{Q}(\sqrt{m})$ *reell-quadratisch*, andernfalls *imaginär-quadratisch*.

Definition 2.3. Sei $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$. Dann nennt man

$$\alpha' = \sigma(\alpha) := a - b\sqrt{m}$$

die *Konjugierte von α*. Weiter heißt

$$N(\alpha) := \alpha\alpha' = a^2 - b^2 m \in \mathbb{Q}$$

Norm von α,

$$\mathrm{Tr}(\alpha) := \alpha + \alpha' = 2a \in \mathbb{Q}$$

Spur von α.

Leichte Rechenregeln

Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$. Dann gilt:

$$\begin{aligned}
\sigma(\alpha+\beta) &= \sigma(\alpha)+\sigma(\beta)\ , \\
\sigma(\alpha\cdot\beta) &= \sigma(\alpha)\cdot\sigma(\beta)\ , \\
\sigma(\alpha) = \alpha \quad &\Longleftrightarrow \quad \alpha \in \mathbb{Q}\ , \\
N(\alpha\beta) &= N(\alpha)\cdot N(\beta)\ , \\
\mathrm{Tr}(\alpha+\beta) &= \mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)\ , \\
\mathrm{Tr}(r\alpha) &= r\,\mathrm{Tr}(\alpha)\ , \qquad r \in \mathbb{Q}\ .
\end{aligned}$$

Lemma 2.4. *Es gilt $N(\alpha) = 0$ genau dann, wenn $\alpha = 0$.*

Bemerkung. $\mathbb{Q}(\sqrt{m})$ ist abgeschlossen bzgl. $+$ und $\cdot$, denn:

$$\begin{aligned}
(a+b\sqrt{m})+(c+d\sqrt{m}) &= (a+c)+(b+d)\sqrt{m}\ , \\
(a+b\sqrt{m})\cdot(c+d\sqrt{m}) &= (ac+bdm)+(ad+bc)\sqrt{m}\ .
\end{aligned}$$

Das Inverse zu $\alpha = a+b\sqrt{m}$ bzgl. $+$ und $\cdot$ ist gegeben durch

$$\begin{aligned}
-\alpha &= (-a)+(-b)\sqrt{m} \in \mathbb{Q}(\sqrt{m})\ , \\
\alpha^{-1} &= \frac{\alpha'}{N(\alpha)} = \underbrace{\frac{a}{a^2-mb^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2-mb^2}}_{\in\mathbb{Q}}\sqrt{m}\ .
\end{aligned}$$

α^{-1} ist tatsächlich das Inverse, denn:

$$\alpha\cdot\alpha^{-1} = \frac{\alpha\alpha'}{N(\alpha)} = 1\ .$$

2.1 Der Ganzheitsring

$$\begin{array}{ccccc}
k = \mathbb{Q}(\sqrt{m}) & \supset & \mathcal{O}_k = \text{ganze Zahlen} \qquad & \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) & \supset \quad \{a+bi \mid a,b\in\mathbb{Z}\} \\
\big| & & \big| & \big| & \qquad\qquad \big| \\
\mathbb{Q} & \supset & \mathbb{Z} & \mathbb{Q} & \qquad\qquad \supset \qquad\quad \mathbb{Z}
\end{array}$$

Definition 2.5. Sei $k = \mathbb{Q}(\sqrt{m})$ und $\alpha \in k$. Dann heißt α *ganze algebraische Zahl*, falls

$$P_\alpha(X) := X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) \in \mathbb{Z}[X]\ .$$

Die Gesamtheit aller ganzen algebraischen Zahlen in k nennen wir $\mathcal{O}_k$.

Satz 2.6. *Es gilt*

$$\mathcal{O}_k = \{a+b\omega \mid a,b\in\mathbb{Z}\}$$

mit

$$\omega = \begin{cases} \sqrt{m}\ , & m \equiv 2 \text{ oder } 3 \mod 4\ , \\ \frac{1+\sqrt{m}}{2}\ , & m \equiv 1 \mod 4\ . \end{cases}$$

Beweis. „$\supseteq$“: Wir berechnen

$$\begin{aligned}\mathrm{Tr}(a+b\omega) &= \begin{cases} 2a \in \mathbb{Z} & m \equiv 2 \text{ oder } 3 \mod 4\,, \\ 2a+b \in \mathbb{Z} & m \equiv 1 \mod 4\,, \end{cases} \\ N(a+b\omega) &= a^2 + ab\,\mathrm{Tr}(\omega) + b^2 N(\omega) \\ &= \begin{cases} a^2 + b^2 m \in \mathbb{Z}\,, & m \equiv 2 \text{ oder } 3 \mod 4\,, \\ a^2 + ab + b^2 \underbrace{\dfrac{1-m}{4}}_{\in\mathbb{Z}} \in \mathbb{Z}\,, & m \equiv 1 \mod 4\,. \end{cases}\end{aligned}$$

„$\subseteq$“: Sei $\alpha = a + b\sqrt{m} \in \mathcal{O}_k$, $a, b \in \mathbb{Q}$, d.h.

$$\begin{aligned}\mathrm{Tr}(\alpha) &= 2a \in \mathbb{Z}\,, \\ N(\alpha) &= a^2 - b^2 m \in \mathbb{Z}\,.\end{aligned}$$

Daraus erhalten wir $a = \frac{a_1}{2}$ für ein $a_1 \in \mathbb{Z}$. Setzen wir dies in die zweite Bedingung ein, so erhalten wir

$$\frac{a_1^2}{4} - mb^2 = x$$

mit $x \in \mathbb{Z}$. Multiplikation mit 4 und umstellen liefert

$$\begin{aligned} & & a_1^2 - 4mb^2 &= 4x \in \mathbb{Z} \\ \Longrightarrow & & 4mb^2 &= a_1^2 - 4x \in \mathbb{Z} \\ \Longrightarrow & & b &= \frac{b_1}{2} \quad \text{mit } b_1 \in \mathbb{Z}\,. \end{aligned}$$

Die Bedingung $a^2 - mb^2 \in \mathbb{Z}$ ist äquivalent zu

$$a_1^2 - mb_1^2 \equiv 0 \mod 4\,. \tag{2.1}$$

1. Fall: $m \equiv 1 \mod 4$. Hier gilt

$$\begin{aligned} (2.1) \quad & \Longleftrightarrow & a_1^2 - b_1^2 &\equiv 0 \mod 4 \\ & \Longleftrightarrow & (a_1 - b_1)\underbrace{(a_1 + b_1)}_{a_1 - b_1 + 2b_1} &\equiv 0 \mod 4 \\ & \Longleftrightarrow & a_1 &\equiv b_1 \mod 2\,. \end{aligned}$$

Also gilt

$$\alpha = \frac{a_1}{2} + \frac{b_1}{2}\sqrt{m} = \underbrace{\frac{a_1 - b_1}{2}}_{\in\mathbb{Z}} + \underbrace{b_1}_{\in\mathbb{Z}} \frac{1+\sqrt{m}}{2}\,.$$

2. Fall: $m \equiv 2$ oder $3 \mod 4$. Dieser Fall bleibt als Übung.

□

Bemerkungen. (a) $\mathcal{O}_k$ ist abgeschlossen bzgl. + und $\cdot$.

(b) $\mathcal{O}_k$ ist also ein *Ring*, d.h. man kann in $\mathcal{O}_k$ rechnen wie in k, jedoch existieren keine Inversen bzgl. $\cdot$.

Beweis der Abgeschlossenheit. Die Abgeschlossenheit bzgl. + ist klar. Für $\cdot$ berechnen wir für $a, b, c, d \in \mathbb{Z}$

$$(a + b\omega)(c + d\omega) = \underbrace{ac + (ad + bc)\omega}_{\in \mathcal{O}_k} + bd\omega^2 \ .$$

Es reicht zu zeigen, dass $\omega^2 \in \mathcal{O}_k$ ist. Dazu:

$$\omega^2 = \begin{cases} m \ , & m \equiv 2 \text{ oder } 3 \mod 4 \ , \\ \frac{1+m+2\sqrt{m}}{4} \ , & m \equiv 1 \mod 4 \ . \end{cases}$$

Offensichtlich ist $m \in \mathcal{O}_k$, für den anderen Fall schreiben wir

$$\frac{1 + m + 2\sqrt{m}}{4} = \underbrace{\frac{m-1}{4}}_{\in \mathbb{Z}} + \underbrace{\frac{1+\sqrt{m}}{2}}_{=\omega} \in \mathcal{O}_k$$

□

Bemerkung. Im Fall $m \equiv 1 \mod 4$ gilt:

$$\mathcal{O}_k = \left\{ \frac{a + b\sqrt{m}}{2} \mid a, b \in \mathbb{Z}, \ a \equiv b \mod 2 \right\}$$

2.2 Der Einheitskreis

Sei $k = \mathbb{Q}(\sqrt{m})$. Sei

$$U_1 := \{\alpha \in k \setminus \{0\} \mid N(\alpha) = 1\} \ .$$

Elemente in U_1 kann man leicht konstruieren, nämlich für $\alpha \neq 0$

$$N\left(\frac{\alpha}{\alpha'}\right) = \frac{N(\alpha)}{N(\alpha')} = \frac{\alpha\alpha'}{\alpha'\alpha} = 1 \ .$$

Also gilt

$$\left\{ \frac{\alpha}{\alpha'} \mid \alpha \in k, \alpha \neq 0 \right\} \subseteq U_1 \ .$$

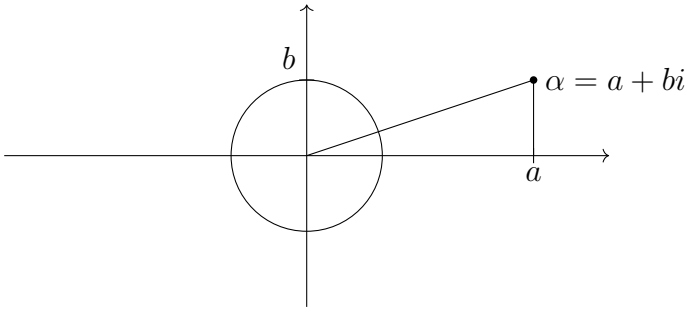
Hilberts Satz 90 besagt, dass auch die umgekehrte Inklusion gilt, also erhalten wir

$$\left\{ \frac{\alpha}{\alpha'} \mid \alpha \in k, \alpha \neq 0 \right\} = U_1 \ .$$

Sei speziell $k = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Dann ist für $a + bi \in k$ die Norm

$$N(a + bi) = a^2 + b^2$$

gerade das Quadrat der Länge des Vektors $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$.



Die rationalen Punkte auf dem Einheitskreis entsprechen genau den $\alpha = a + bi$, $a, b \in \mathbb{Q}$ in U_1, denn $1 = N(\alpha) = a^2 + b^2$. Außerdem ist

$$U_1 = \left\{ \frac{\alpha}{\alpha'} \mid \alpha \in k, \alpha \neq 0 \right\} .$$

Sei $\alpha = a + bi$, $a, b \in \mathbb{Q}$. Dann gilt

$$\frac{\alpha}{\alpha'} = \frac{a + bi}{a - bi} = \frac{(a + bi)^2}{a^2 + b^2} = \frac{a^2 - b^2}{a^2 + b^2} + \frac{2ab}{a^2 + b^2} \cdot i \ .$$

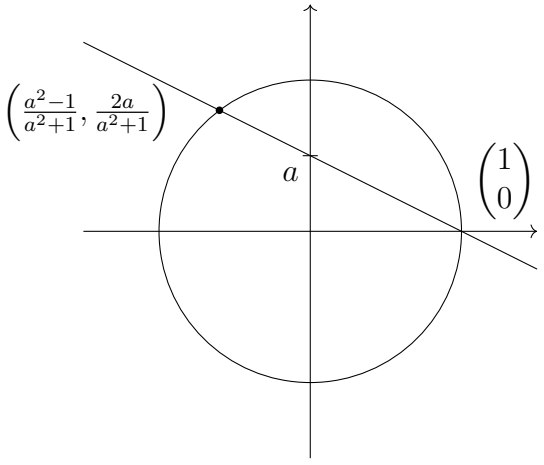
Also sind alle rationalen Punkte $\begin{pmatrix} x \\ y \end{pmatrix}$ auf dem Einheitskreis von der Form

$$x = \frac{a^2 - b^2}{a^2 + b^2} \ , \qquad y = \frac{2ab}{a^2 + b^2} \ , \qquad a, b \in \mathbb{Q} \ .$$

Beispiel 2.7. Sei $a = 2, b = 1$. Dann ist $x = \frac{3}{5}$ und $y = \frac{4}{5}$.

Falls $b \neq 0$ kann man a durch $\frac{a}{b}$ und b durch 1 ersetzen. Dann erhält man also alle Punkte $\begin{pmatrix} x \\ y \end{pmatrix}$ auf dem Einheitskreis mit $x, y \in \mathbb{Q}$ in der Form:

$$x = \frac{a^2 - 1}{a^2 + 1} \ , \qquad y = \frac{2a}{a^2 + 1} \ , \qquad a \in \mathbb{Q} \ .$$



2.3 Einheiten in Ringen

Unsere Ringe R sind stets kommutativ und *nullteilerfrei*, d.h. für alle $a, b \in R$ gilt:

$$ab = 0 \qquad \Longrightarrow \qquad a = 0 \text{ oder } b = 0 \ .$$

Beispiel 2.8. Sei $R = \mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{9}\}$. Dann gilt

$$\overline{2} \cdot \overline{5} = \overline{10} = \overline{0} = \overline{4} \cdot \overline{5} \ ,$$

d.h. $\overline{2}$ ist also ein Nullteiler.

In nullteilerfreien Ringen kann man kürzen:
Für $a, b, c \in R$ gilt:

$$\left.\begin{array}{l} ab = ac \\ a \neq 0 \end{array}\right\} \quad \Longrightarrow \quad b = c \ .$$

Beispiele 2.9. Beispiele für kommutative nullteilerfreie Ringe sind $\mathbb{Z}, \mathcal{O}_k$, jeder Körper, Polynome mit Koeffizienten in $\mathbb{Z}, \mathbb{Q}$.

Definition 2.10. Seien $a, b \in R$.

(a) Man sagt b teilt a, in Zeichen $b \mid a$, falls es $c \in R$ mit $a = bc$ gibt.

(b) Seien $a, b, m \in R$. Dann definiert man

$$a \equiv b \mod m \quad :\Longleftrightarrow \quad m \mid a - b \ .$$

Einfache Rechenregeln

(a)

$$\left.\begin{array}{ll} a \equiv b & \mod m \\ c \equiv d & \mod m \end{array}\right\} \quad \Longrightarrow \quad \begin{cases} a + c & \equiv b + d \mod m \\ a \cdot c & \equiv b \cdot d \mod m \end{cases}$$

(b) Es gelte für $n, m \in R$ $n \mid m$. Dann gilt

$$a \equiv b \mod m \quad \Longrightarrow \quad a \equiv b \mod n \ .$$

(c) Sei k ein quadratischer Zahlkörper und $R = \mathcal{O}_k$. Seien $a, b, m \in \mathbb{Z}$. Dann gilt

$$a \equiv b \mod m \text{ in } \mathcal{O}_k \quad \Longleftrightarrow \quad a \equiv b \mod m \text{ in } \mathbb{Z} \ .$$

Beweis von (c). Wir folgern

$$\begin{array}{rl} & a \equiv b \mod m \text{ in } \mathcal{O}_k \\ \Longleftrightarrow & m \mid a - b \text{ in } \mathcal{O}_k \\ \Longleftrightarrow & \exists \gamma \in \mathcal{O}_k \text{ sodass } a - b = m\gamma \\ \Longleftrightarrow & \exists \gamma \in \mathcal{O}_k \text{ mit } \gamma = \dfrac{a-b}{m} \in \mathcal{O}_k \end{array}$$

Also gilt mit Blatt 2, Aufgabe 4(a) $\gamma \in \mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$. Somit folgt $a \equiv b \mod m$ in $\mathbb{Z}$. □

Definition 2.11. Die Menge

$$R^\times := \{a \in R \mid \text{Es gibt } b \in R \text{ mit } ab = 1\}$$

nennt man die Gruppe der *Einheiten* von R.

Beispiele 2.12.

R	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Z}[i]$	$\mathbb{Q}[X]$	$\mathbb{Z}[\sqrt{2}]$
$R^\times$	$\{\pm 1\}$	$\mathbb{Q} \setminus \{0\}$	$\{\pm 1, \pm i\}$	$\mathbb{Q}^\times$	$\{\pm(1+\sqrt{2})^t \mid t \in \mathbb{Z}\}$

Erinnerung. Es ist

$$\mathcal{O}_k = \begin{cases} \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} , & m \equiv 2, 3 \mod 4 , \\ \left\{ \frac{a+b\sqrt{m}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \mod 2 \right\} , & m \equiv 1 \mod 4 . \end{cases}$$

Satz 2.13. *(a)* $\varepsilon \in \mathcal{O}_k^\times \iff N(\varepsilon) = \pm 1$.

(b) Sei $m \equiv 2, 3 \mod 4$ *und* $\varepsilon = a + b\sqrt{m}$, $a, b \in \mathbb{Z}$. *Dann entsprechen die Einheiten* $\varepsilon \in \mathcal{O}_k^\times$ *genau den Lösungen* $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ *mit* $a^2 - mb^2 = \pm 1$.

Sei $m \equiv 1 \mod 4$ *und* $\varepsilon = \frac{a+b\sqrt{m}}{2}$, $a, b \in \mathbb{Z}$, $a \equiv b \mod 2$. *Dann entsprechen die Einheiten* $\varepsilon \in \mathcal{O}_k^\times$ *genau den Lösungen* $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ *mit* $a^2 - mb^2 = \pm 4$.

Beweis. Die Aussage (b) folgt aus (a), da

$$N(a + b\sqrt{m}) = a^2 - b^2 m$$

und

$$N\left(\frac{a + b\sqrt{m}}{2}\right) = \frac{a^2 - b^2 m}{4} .$$

Für den Beweis von (a) sind zwei Richtungen zu zeigen.
„$\Longrightarrow$“: Sei $\varepsilon \in \mathcal{O}_k^\times$. Dann gibt es ein $\eta \in \mathcal{O}_k$ mit $\varepsilon\eta = 1$. Wenden wir die Norm auf diese Gleichung an erhalten wir

$$\underbrace{N(\varepsilon)}_{\in\mathbb{Z}} \underbrace{N(\eta)}_{\in\mathbb{Z}} = N(\varepsilon\eta) = N(1) = 1 \quad \text{in } \mathbb{Z} .$$

Somit folgt $N(\varepsilon) \in \mathbb{Z}^\times = \{\pm 1\}$.
„$\Longleftarrow$“: Sei $\varepsilon \in \mathcal{O}_k$ mit $N(\varepsilon) = \pm 1$. Dann gilt

$$\varepsilon^{-1} = \frac{\varepsilon'}{N(\varepsilon)} = \pm \underbrace{\varepsilon'}_{\in\mathcal{O}_k} \in \mathcal{O}_k .$$

□

Satz 2.14. *Sei* $m < 0$ *und* $k = \mathbb{Q}(\sqrt{m})$. *Dann gilt*

$$\mathcal{O}_k^\times = \begin{cases} \{\pm 1\} , & \text{falls } m \neq -1, -3 , \\ \{\pm 1, \pm i\} , & \text{falls } m = -1 , \\ \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\} , & \text{falls } m = -3 . \end{cases}$$

Beweis.

1. Fall: Sei $m \equiv 2, 3 \mod 4$. Gesucht sind die Lösungen von

$$a^2 - mb^2 = 1 \ .$$

Falls $m \neq -1$, so gibt es nur die Lösungen $(a, b) = (\pm 1, 0)$.
Für $m = -1$ hat $a^2 + b^2 = 1$ die Lösungen

$$(a, b) = (0, \pm 1), (\pm 1, 0) \ .$$

2. Fall: Sei $m \equiv 1 \mod 4$. Hier muss man

$$a^2 - mb^2 = 4$$

betrachten.
Falls $m < -3$, so hat man nur die Lösung $(a, b) = (\pm 2, 0)$.
Falls $m = -3$, so hat $a^2 + 3b^2 = 4$ die Lösungen

$$(a, b) = (\pm 2, 0), (\pm 1, \pm 1) \ .$$

□

2.4 Zerlegbare und prime Elemente

Ziel: Satz von der eindeutigen Primzahlzerlegung in $\mathcal{O}_k$?

Definition 2.15. Seien $a, b \in R$.

(a) a und b heißen *assoziiert*, in Zeichen $a \sim b$, falls es eine Einheit $u \in R^\times$ gibt mit $a = ub$.

(b) $a \in R \setminus R^\times$, $a \neq 0$, heißt *irreduzibel* oder *unzerlegbar*, falls aus $a = bc$ stets folgt $b \in R^\times$ oder $c \in R^\times$.

Äquivalent dazu ist: a hat keine *echten* Teiler, d.h. $b \mid a$ impliziert stets $b \in R^\times$ oder $b \sim a$.

(c) $p \in R \setminus R^\times$, $p \neq 0$, ist *prim*, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

Beispiel 2.16. Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Dann gilt

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \ ,$$

d.h. $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ aber keinen der Faktoren. Daher ist 2 nicht prim. In der Übung wird gezeigt: 2 ist irreduzibel.

Satz 2.17. *Primelemente sind irreduzibel.*

Bemerkung. Die Umkehrung ist im Allgemeinen falsch.

Beweis. Sei $p \in R \setminus R^\times$ prim und sei $p = ab$. Es ist zu zeigen, dass $a \in R^\times$ oder $b \in R^\times$ gilt.
Dazu folgern wir

$$\begin{aligned} & p = ab \\ \Longrightarrow \quad & p \mid ab \\ \Longrightarrow \quad & p \mid a \\ \Longrightarrow \quad & a = pc \\ \Longrightarrow \quad & p = pcb \\ \Longrightarrow \quad & p(cb - 1) = 0 \end{aligned}$$

Da R nullteilerfrei ist, folgt nun $cb = 1$ und somit $b \in R^\times$.
Man beachte, dass wir in der zweiten Folgerung auch den Fall $p \mid b$ erhalten könnten. In diesem Fall folgt analog zu oben $a \in R^\times$. □

Beispiel 2.18. Sei $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. Betrachte

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \ .$$

Behauptung: $2, 1 + \sqrt{-3}, 1 - \sqrt{-3}$ sind irreduzibel.
Als Beispiel zeigen wir 2 ist irreduzibel:
Sei $2 = \alpha\beta$. Es ist zu zeigen, dass diese Zerlegung nicht echt ist. Wenden wir die Norm an, so erhalten wir

$$4 = N(\alpha)N(\beta) \qquad \text{in } \mathbb{Z} \ .$$

Somit gilt $N(\alpha) \in \{1, 2, 4\}$.
Falls $N(\alpha) = 1$ ist, folgt $\alpha \in R^\times$.
Der Fall $N(\alpha) = 2$ tritt nicht ein, denn für $\alpha = a + b\sqrt{-3}$ mit $a, b \in \mathbb{Z}$ erhalten wir, dass

$$N(\alpha) = a^2 + 3b^2 = 2$$

keine Lösung in $\mathbb{Z}$ besitzt.
Falls $N(\alpha) = 4$, so ist $N(\beta) = 1$ und daher $\beta \in R^\times$.
Es ist klar, dass 2 nicht prim ist.

2.5 Faktorielle Ringe

Dies sind die Ringe, in denen der Satz von der eindeutigen Primzahlzerlegung gilt.

Definition 2.19. Ein Ring R heißt *faktoriell*, wenn folgende zwei Eigenschaften erfüllt sind:

(Z-1) Jedes $a \in R \setminus R^\times$, $a \neq 0$, ist Produkt von endlich vielen irreduziblen Elementen.

(Z-2) Irreduzible Elemente sind prim.

Betrachte zudem

(Z-3) Sei $a \in R$, $a \neq 0$, und sei

$$a = ep_1 \cdots p_s = e'q_1 \cdots q_t$$

mit irreduziblen p_i, q_j und $e, e' \in R^\times$. Dann ist $s = t$ und nach eventueller Umnummerierung gilt $p_i \sim q_i$ für $1 \leq i \leq s$.

Beispiel 2.20. Es ist

$$10 = 1 \cdot 2 \cdot 5 = (-1) \cdot (-5) \cdot 2$$

in $\mathbb{Z}$.

Satz 2.21. *Sei R ein Ring und es gelte (Z-1). Dann gilt*

$$\textit{(Z-2)} \qquad \Longleftrightarrow \qquad \textit{(Z-3)} \ .$$

Beweis. „$\Longrightarrow$“: Sei $ep_1 \cdots p_s = e'q_1 \cdots q_t$. Dann teilt p_1 das Produkt $q_1 \cdots q_t$ und da p_1 prim ist folgt noch Umnummerierung $p_1 \mid q_1$. Da q_1 irreduzibel ist, muss $p_1 \sim q_1$ gelten, d.h. es gibt ein $u \in R^\times$ mit $p_1 = uq_1$. Somit erhalten wir

$$euq_1p_2 \cdots p_s = e'q_1 \cdots q_t \ .$$

Da R nullteilerfrei ist, können wir nun q_1 kürzen und erhalten

$$(eu)p_2 \cdots p_s = e'q_2 \cdots q_t \ .$$

Nun folgt $p_2 \mid q_2 \cdots q_t$ und wir können die obigen Schritte wiederholen. Nach s-facher Anwendung folgt $s = t$ und $p_i \sim q_i$.
„$\Longleftarrow$“: Sei a irreduzibel. Es ist zu zeigen, dass a prim ist. Hierfür gelte $a \mid xy$. Angenommen $a \nmid x$, dann ist zu zeigen $a \mid y$. Da $a \mid xy$ gibt es also ein $b \in R$ mit $xy = ab$. Wegen der *Eindeutigkeit* der Zerlegungen folgt, dass a das y teilt. □

Beispiele 2.22. (1) $\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{-3}]$ sind nicht faktoriell.

(2) $\mathbb{Z}$ ist faktoriell.

2.6 Hauptidealringe

Definition 2.23. Eine nichtleere Teilmenge $I \subseteq R$ heißt *Ideal*, falls

(a) $a, b \in I \quad \Longrightarrow \quad a + b \in I$,

(b) $r \in R, a \in I \quad \Longrightarrow \quad ra \in I$.

Beispiele 2.24. (1) $\{0\}$ und R sind Ideale.

(2) Sei R ein Körper.

Behauptung: Dann gibt es nur die zwei Ideale $\{0\}$ und R.

Beweis. Sei $\{0\} \neq I$ ein Ideal. Es ist zu zeigen, dass $I = R$ ist. Sei $x \in I$, $x \neq 0$. Dann ist

$$1 = \underbrace{\frac{1}{x}}_{\in R} \cdot \underbrace{x}_{\in I} \in I \ .$$

Sei jetzt $y \in R$. Dann gilt

$$y = \underbrace{y}_{\in R} \cdot \underbrace{1}_{\in I} \in I \ ,$$

also ist $I = R$. □

(3) Sei $R = \mathbb{Z}$ und sei $a \in \mathbb{Z}$. Dann ist

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$$

ein Ideal. Solche Ideale nennt man *Hauptideale*.

Behauptung: Jedes Ideal in $\mathbb{Z}$ ist von dieser Form.

Beweis. Das Ideal $I = \{0\}$ ist von dieser Form, denn $\{0\} = 0\mathbb{Z}$.

Sei also nun $I \neq \{0\}$. Sei

$$a := \min(I \cap \mathbb{N}) \ .$$

Hierbei ist zu beachten, dass für $a \in I$ auch $-a \in I$ ist, d.h. I enthält auf jeden Fall eine natürliche Zahl. Wir wollen nun zeigen, dass $I = a\mathbb{Z}$ für dieses spezielle a gilt:

„$\supseteq$“: Für $r \in \mathbb{Z}$ ist $ra \in I$, da $a \in I$ ist.

„$\subseteq$“: Sei $b \in I$. Teilen wir b durch a mit Rest, so erhalten wir

$$b = qa + r$$

mit $q \in \mathbb{Z}$ und $0 \leq r < a$. Es folgt nun

$$r = \underbrace{\underbrace{b}_{\in I} - q \underbrace{\underbrace{a}_{\in I}}_{\in I}}_{\in I} \in I$$

und daraus erhalten wir $r = 0$. □

(4) Sei $a \in R$. Dann ist $aR = \{ra \mid r \in R\}$ ein *Hauptideal*.

Definition 2.25. Ein Ring R heißt *Hauptidealring*, falls jedes Ideal ein Hauptideal ist.

Satz 2.26 (ohne Beweis)**.** *Hauptidealringe sind faktoriell.*

Motivation. Ringe $\supsetneq$ faktorielle Ringe $\supsetneq$ Hauptidealringe $\supsetneq$ euklidische Ringe

2.7 Euklidische Ringe

Definition 2.27. Ein Ring R heißt *euklidisch*, falls es eine Funktion

$$f : R \longrightarrow \mathbb{N}_0$$

gibt, sodass:

(E-1) $f(a) = 0 \iff a = 0$,

(E-2) Zu $a \in R$ und $b \in R \setminus \{0\}$ gibt es $q, r \in R$ mit $a = qb + r$ und $f(r) < f(b)$.

Beispiele 2.28. (1) Der Ring $R = \mathbb{Z}$ mit $f(a) := |a|$ ist euklidisch.

(2) Sei K ein Körper, dann ist $K[X]$ euklidisch mit $f(g) := \deg(g) + 1$ für $g \in K[X]$, $g \neq 0$ und $f(0) := 0$.

Satz 2.29. *Euklidische Ringe sind Hauptidealringe.*

Beweis. Es ist klar, dass $I = \{0\} = 0R$ ein Hauptideal ist.

Sei also nun $I \neq \{0\}$. Sei $a \in I$, sodass $f(a) \neq 0$ und minimal ist.

Behauptung: Es gilt $I = aR$.
„$\supseteq$“: Diese Inklusion ist klar, da $a \in I$ ist.
„$\subseteq$“: Sei $b \in I$. Teilen mit Rest liefert $b = qa + r$ mit $f(r) < f(a)$. Dann ist

$$r = b - qa \in I$$

und somit folgt $r = 0$. □

Ziel: Wir wollen zeigen, dass

$$p = x^2 + y^2 = (x + yi)(x - yi) \qquad \iff \qquad p \equiv 1 \mod 4 \ .$$

Dies führt zum Rechnen in $\mathbb{Z}[i]$. Wir wollen daher nun zeigen, dass $\mathbb{Z}[i]$ euklidisch ist.

3 Zwei diophantische Probleme

3.1 Die ganzen Gaußschen Zahlen $\mathbb{Z}[i]$

Satz 3.1. *$Z[i]$ ist euklidisch bzgl. $f(\alpha) = N(\alpha)$.*

Beweis. (E-1) ist offensichtlich, da

$$N(a+bi) = a^2 + b^2 = 0 \qquad \Longleftrightarrow \qquad a = b = 0 \ .$$

Für (E-2) seien $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Es ist zu zeigen, dass es $\gamma, \rho \in \mathbb{Z}[i]$ gibt mit $\alpha = \gamma\beta + \rho$ und $N(\rho) < N(\beta)$.
Sei dazu

$$\frac{\alpha}{\beta} = \widetilde{a} + \widetilde{b}i$$

mit $\widetilde{a}, \widetilde{b} \in \mathbb{Q}$. Runde nun, d.h. wähle $a, b \in \mathbb{Z}$ mit

$$|\widetilde{a} - a| \leq \frac{1}{2} \ ,$$
$$\left|\widetilde{b} - b\right| \leq \frac{1}{2} \ .$$

Setze $\gamma := a + bi$. Dann gilt

$$\alpha = \gamma\beta + \underbrace{(\alpha - \gamma\beta)}_{=:\rho} \ .$$

Es ist noch zu zeigen, dass $N(\rho) < N(\beta)$. Hierfür betrachten wir

$$\begin{aligned} & N(\rho) < N(\beta) \\ \Longleftrightarrow \qquad & 1 > N\left(\frac{\rho}{\beta}\right) = N\left(\frac{\alpha}{\beta} - \gamma\right) = N((\widetilde{a} - a) + (\widetilde{b} - b)i) = \underbrace{\underbrace{(\widetilde{a} - a)^2}_{\leq \frac{1}{4}} + \underbrace{(\widetilde{b} - b)^2}_{\leq \frac{1}{4}}}_{\leq \frac{1}{2}} \ . \end{aligned}$$

□

Folgerung 3.2. $\mathbb{Z}[i]$ ist faktoriell.

3.2 Eulersches Kriterium

Sei $p \neq 2$ eine Primzahl. Dann gilt

$$\exists x \in \mathbb{Z} \text{ mit } -1 \equiv x^2 \mod p \quad \Longleftrightarrow \quad p \equiv 1 \mod 4 \ .$$

Beispiele 3.3. (a) Wir betrachten $p = 5$:

k	1	2	3	4	5	6	7	8
$\overline{2}^k$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$

Wir finden also $2^2 \equiv -1 \mod 5$.

(b) Sei nun $p = 7$:

k	1	2	3	4	5	6
$\overline{3}^k$	$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$	$\overline{1}$

(c) Sei $p = 13$:

k	1	2	3	4	5	6	7	8	9	10	11	12
$\overline{2}^k$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{6}$	$\overline{12}$	$\overline{11}$	$\overline{9}$	$\overline{5}$	$\overline{10}$	$\overline{7}$	$\overline{1}$

In diesem Fall gilt $8^2 \equiv -1 \mod 13$.

Allgemein gilt:

Satz 3.4. *Sei p eine Primzahl. Dann gibt es $\omega \in \mathbb{Z}/p\mathbb{Z}$ mit*

$$\{\omega^k \mid k = 1, ..., p-1\} = (\mathbb{Z}/p\mathbb{Z})^\times \ .$$

Satz 3.5. *Sei $p \neq 2$ eine Primzahl. Dann gilt:*

$$\exists x, y \in \mathbb{Z} \text{ mit } p = x^2 + y^2 \qquad \Longleftrightarrow \qquad p \equiv 1 \mod 4 \ .$$

Erinnerung. $\mathbb{Z}[i]$ ist faktoriell, d.h. es gilt der Satz von der eindeutigen Primzahlzerlegung.

Satz 3.6 (Zerlegungsgesetz in $\mathbb{Z}[i]$)**.** *Sei p eine Primzahl in $\mathbb{Z}$. Für die Zerlegung von p in $\mathbb{Z}[i]$ gibt es die folgenden Möglichkeiten:*

(1) Falls $p = 2$, so ist

$$2 = i(1-i)^2$$

die Zerlegung in $\mathbb{Z}[i]$, d.h. $1-i$ ist bis auf Assoziiertheit der einzige irreduzible Teiler von 2.

(2) Falls $p \equiv 3 \mod 4$, so ist p irreduzibel, also auch prim, in $\mathbb{Z}[i]$.

(3) Falls $p \equiv 1 \mod 4$, so ist $p = \pi\pi'$ für prime Elemente π, π' ($\pi = a + bi, \pi' = a - bi$). Es gilt $\pi \nsim \pi'$.

Beispiele 3.7. Wir betrachten zum Beispiel

$$p = 5 = \underbrace{(1+2i)}_{\pi}\underbrace{(1-2i)}_{\pi'} = 1^2 + 2^2 \ ,$$
$$p = 13 = (2+3i)(2-3i) = 2^2 + 3^2 = N(2+3i) \ .$$

Beweis von Satz 3.6. (1) Es gilt $N(1-i) = 2$ und mit Blatt 3, Aufgabe 1 folgt nun, dass $1-i$ irreduzibel, also auch prim, ist.

(2) Angenommen p ist reduzibel, dann gibt es ein irreduzibles π mit $\pi \mid p$. Dann folgt

$$N(\pi) \mid N(p) = p^2$$

und somit $N(\pi) = p$. Sei $\pi = a + bi$ mit $a, b \in \mathbb{Z}$. Es gilt

$$N(\pi) = a^2 + b^2 = p \ .$$

Wir betrachten die Quadrate modulo 4:

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$

Betrachten wir nun die obige Gleichung modulo 4 so erhalten wir $p \equiv 0, 1, 2 \mod 4$. Dies ist ein Widerspruch.

(3) Aus dem Eulerschen Kriterium folgt, dass es ein $x \in \mathbb{Z}$ gibt mit

$$-1 \equiv x^2 \mod p \ .$$

Somit teilt p

$$(x - i)(x + i) = x^2 + 1 \ .$$

Da p keinen der beiden Faktoren teilt, ist p nicht irreduzibel. Also ist

$$p = \pi\widetilde{\pi}$$

mit irreduziblen Elementen $\pi, \widetilde{\pi} \in \mathbb{Z}[i]$.

Beobachtung: $\pi \mid p \quad \Longrightarrow \quad \pi' \mid p' = p$.

Behauptung: π und π' sind nicht assoziiert (Diese Behauptung impliziert dann $\widetilde{\pi} \sim \pi'$).

Beweis der Behauptung. Sei $\pi = a + bi$, $a, b \in \mathbb{Z}$. Angenommen $\pi \sim \pi'$. Dann folgt

$$\frac{\pi'}{\pi} = \frac{(\pi')^2}{N(\pi)} = \frac{a^2 - b^2}{p} + \frac{2ab}{p} i \in \mathbb{Z}[i] \ .$$

Also gilt

(i) $p \mid a^2 - b^2$,

(ii) $p \mid 2ab$.

Aus (ii) folgt $p \mid a$ oder $p \mid b$.

Falls $p \mid a$ folgt mit (i) $p \mid b$ und somit $p \mid \pi$ in $\mathbb{Z}[i]$. Anwenden der Norm liefert nun $p^2 \mid N(p) = p$, dies ist ein Widerspruch.

Falls $p \mid b$ folgt analog aus (i) $p \mid a$ und genauso wie oben letztendlich $p^2 \mid N(\pi) = p$, also erhalten wir auch hier einen Widerspruch.

□

Aus der Behauptung folgt somit (3).

□

Der Beweis von Satz 3.5 ist eine unmittelbare Konsequenz von Satz 3.6:

Beweis von Satz 3.5. „$\Longrightarrow$“: Sei

$$p = x^2 + y^2 \ .$$

Wir bereits festgestellt, dass die Quadrate modulo 4 gerade $\overline{0}$ und $\overline{1}$ sind. In obiger Gleichung ergeben sich durch Kombination der verschiedenen Möglichkeiten nun die Fälle $p \equiv 0, 1, 2 \mod 4$. Da $p \neq 2$ ist p ungerade, d.h. die einzige verbleibende Möglichkeit ist $p \equiv 1 \mod 4$.

„$\Longleftarrow$“: Sei $p \equiv 1 \mod 4$, dann ist nach Satz 3.6 $p = \pi\pi'$ für $\pi = a + bi$ irreduzibel. Dann gilt

$$p^2 = N(p) = N(\pi)N(\pi')$$

und somit

$$p = N(\pi) = a^2 + b^2 \ .$$

□

Beispiele 3.8. Wir betrachten

$$\begin{aligned} 13 &= 2^3 + 3^2 = N(2 + 3i) \ , \\ 17 &= 1^2 + 4^2 = N(1 + 4i) \ , \\ 221 &= 13 \cdot 17 = N((2 + 3i)(1 + 4i)) = N((2 - 12) + i(8 + 3)) = 10^2 + 11^2 \ . \end{aligned}$$

3.3 Das zweite Problem

Wir wollen nun die Gleichung $Y^2 = X^3 + 1$ untersuchen. Hierfür rechnen wir in den Eisensteinschen Zahlen $\mathbb{Z}[\rho]$ (wobei $\rho = \frac{-1+\sqrt{-3}}{2}$). Die Einheiten sind gegeben durch

$$\mathbb{Z}[\rho]^\times = \{(-\rho)^i \mid i = 0, 1, ..., 5\} \ .$$

Satz 3.9. *Die Gleichung $Y^2 = X^3 + 1$ hat nur die ganzzahligen Lösungen*

$$(-1, 0), \ (0, \pm 1), \ (2, \pm 3) \ .$$

Der Beweis zu Satz 3.9 wird aus Satz 3.10 folgen.

Satz 3.10. *Seien $\alpha, \beta, \gamma \in \mathbb{Z}[\rho]$ und es gelte:*

$$\alpha + \beta + \gamma = 0 \ , \qquad \alpha\beta\gamma = 2\mu^3 \quad \textit{mit } \mu \in \mathbb{Z}[\rho] \ .$$

Dann gilt nach einer geeigneten Permutation $\alpha = 0$ oder $\beta = \gamma$.

Beweis von Satz 3.9 aus Satz 3.10. Sei $(x, y) \in \mathbb{Z}^2$ eine Lösung von

$$Y^2 = X^3 + 1 \ . \tag{3.1}$$

Setze

$$\begin{aligned} \alpha &= 1 - y \ , \\ \beta &= 1 + y \ , \\ \gamma &= -2 \ . \end{aligned}$$

Dann gilt

$$\begin{aligned} \alpha + \beta + \gamma &= 0 \ , \\ \alpha\beta\gamma &= -2(1 - y^2) = 2x^3 \ , \end{aligned}$$

wobei im letzten Schritt die Gleichung (3.1) verwendet wurde. Also können wir $\mu = x$ setzen.
Aus Satz 3.10 folgt nun

$$\begin{aligned} \alpha = 0 \quad &\Longrightarrow \quad y = 1, x = 0 \quad \longrightarrow (0, 1) \ , \\ \beta = 0 \quad &\Longrightarrow \quad y = -1, x = 0 \quad \longrightarrow (0, -1) \ , \\ \alpha = \beta \quad &\Longrightarrow \quad y = 0, x = -1 \quad \longrightarrow (-1, 0) \ , \\ \alpha = \gamma \quad &\Longrightarrow \quad y = 3, x = 2 \quad \longrightarrow (2, 3) \ , \\ \beta = \gamma \quad &\Longrightarrow \quad y = -3, x = 2 \quad \longrightarrow (2, -3) \ . \end{aligned}$$

□

Beweis von Satz 3.10. Wie bei $\mathbb{Z}[i]$ kann man zeigen, dass $\mathbb{Z}[\rho]$ euklidisch ist. In $\mathbb{Z}[\rho]$ gilt der Satz von der eindeutigen Primzahlzerlegung.

Beobachtung: 2 ist irreduzibel in $\mathbb{Z}[\rho]$.

Wir beweisen Satz 3.10 durch Widerspruch. Sei dazu (α, β, γ) ein Gegenbeispiel. Ohne Einschränkung können wir annehmen, dass α, β, γ paarweise teilerfremd sind, denn falls z.B. α und β einen gemeinsamen Teiler π hätten, so würde wegen

$$\alpha + \beta + \gamma = 0$$

π auch γ teilen. Teile also α, β, γ durch π.
Wir nehmen nun an, dass (α, β, γ) ein Gegenbeispiel ist, so dass $0 < N(\alpha\beta\gamma)$ minimal ist und α, β, γ paarweise teilerfremd sind. Wir werden im Folgenden zeigen, dass

man aus einem solchen Gegenbeispiel ein Gegenbeispiel $(\alpha_1, \beta_1, \gamma_1)$ mit paarweise teilerfremden $\alpha_1, \beta_1, \gamma_1$ und $0 < N(\alpha_1\beta_1\gamma_1) < N(\alpha\beta\gamma)$ konstruieren kann. Dies ist ein Widerspruch.
Wegen der paarweisen Teilerfremdheit gilt:

$$\begin{aligned}\alpha &= 2(-\rho)^a A_1^3 \ , \\ \beta &= (-\rho)^b B_1^3 \ , \\ \gamma &= (-\rho)^c C_1^3 \ ,\end{aligned}$$

mit $a, b, c \in \{0, ..., 5\}$ und paarweise teilerfremden $A_1, B_1, C_1 \in \mathbb{Z}[\rho]$.

Bemerkung. Dies ist die entscheidende Stelle. Hier braucht man, dass $\mathbb{Z}[\rho]$ faktoriell ist.

Wegen $-1 = (-1)^3$ kann man annehmen

$$\begin{aligned}\alpha &= 2\rho^a A_1^3 \ , \\ \beta &= \rho^b B_1^3 \ , \\ \gamma &= \rho^c C_1^3 \ ,\end{aligned}$$

mit $a, b, c \in \{0, 1, 2\}$. Ohne Einschränkung können wir $a = 0$ annehmen.
Also:

$$\begin{aligned}\alpha &= 2A_1^3 \ , \\ \beta &= \rho^b B_1^3 \ , \\ \gamma &= \rho^c C_1^3 \ ,\end{aligned}$$

mit $b, c \in \{0, 1, 2\}$.
Wir benötigen nun folgendes

Lemma 3.11. *Sei $z \in \mathbb{Z}[\rho]$. Dann gilt*

$$\begin{array}{rcrcr} z^3 \equiv 0 \mod 2 & & \textit{oder} & & z^3 \equiv 1 \mod 2 \\ \textit{falls } z \equiv 0 \mod 2 & & & & \textit{falls } z \not\equiv 0 \mod 2 \ . \end{array}$$

Beweis. In $\mathbb{Z}[\rho]$ gibt es genau die Reste $\overline{a + b\rho}$ mit $a, b \in \{0, 1\}$. Z.B. ist nun

$$\begin{aligned}&\rho^3 = 1 \equiv 1 \mod 2 \\ &(1+\rho)^3 = (1 + 2\rho + \rho^2)(1+\rho) \equiv (1+\rho^2)(1+\rho) = 1 + \rho + \rho^2 + 1 = 1 \mod 2.\end{aligned}$$

□

Es gilt

$$\begin{aligned}0 \equiv a &\equiv \beta + \gamma \\ &\equiv \rho^b B_1^3 + \rho^c C_1^3 \\ &\overset{3.11}{\equiv} \rho^b + \rho^c \\ &\equiv \rho^b(1 + \rho^{c-b}) \mod 2 \ .\end{aligned}$$

Damit folgt $2 \mid \rho^b(1+\rho^{c-b})$ und somit auch $2 \mid 1+\rho^{c-b}$, d.h. es muss $b=c$ gelten. Betrachten wir nun

$$\underbrace{(A_1B_1C_1)^3}_{\equiv 1 \mod 2}\rho^{2b} = \underbrace{\mu^3}_{\equiv 1 \mod 2}$$

so folgt

$$\rho^{2b} \equiv 1 \mod 2$$

und daher $b=0$.

Insgesamt erhalten wir also

$$\begin{aligned}\alpha &= 2A_1^3 \ , \\ \beta &= B_1^3 \ , \\ \gamma &= C_1^3 \ ,\end{aligned}$$

für paarweise teilerfremde $A_1, B_1, C_1 \in \mathbb{Z}[\rho]$.
Setze nun

$$\begin{aligned}\alpha_1 &= B_1 + C_1 \ , \\ \beta_1 &= \rho B_1 + \rho^2 C_1 \ , \\ \gamma_1 &= \rho^2 B_1 + \rho C_1 \ .\end{aligned}$$

Wir überprüfen nun, dass $(\alpha_1, \beta_1, \gamma_1)$ ebenfalls ein Gegenbeispiel ist. Es gilt

$$\alpha_1 + \beta_1 + \gamma_1 = B_1(1+\rho+\rho^2) + C_1(1+\rho+\rho^2) = 0$$

und

$$\alpha_1\beta_1\gamma_1 = B_1^3 + C_1^3 = \beta + \gamma = -\alpha = -2A_1^3 = 2(-A_1)^3.$$

Damit sind die Voraussetzungen des Satzes erfüllt mit $\mu = -A_1$. Wir müssen als nächstes zeigen, dass wir ein neues Gegenbesipiel haben. Wegen $\alpha_1\beta_1\gamma_1 = -\alpha \neq 0$ gilt

$$\alpha_1 \neq 0 \text{ und } \beta_1 \neq 0 \text{ und } \alpha_1 \neq 0.$$

Aus $\alpha_1 = \gamma_1$ würde folgen:

$$\begin{aligned}& B_1 + C_1 = \rho^2 B_1 + \rho C_1 \\ \Longrightarrow\ & B_1(1-\rho^2) = C_1(\rho - 1) = C_1\rho(1-\rho^2) \\ \Longrightarrow\ & B_1 = \rho C_1 \\ \Longrightarrow\ & \beta = \gamma.\end{aligned}$$

Dies ist ein Widerspruch, da ja per Annahme (α, β, γ) ein Gegenbeispiel ist.
Ebenso schließt man die Fälle $\alpha_1 = \beta_1$ und $\beta_1 = \gamma_1$ aus.
Letzlich müssen wir zeigen, dass $(\alpha_1, \beta_1, \gamma_1)$ ein kleineres Gegenbeispiel ist. Es gilt:

$$N(\alpha_1\beta_1\gamma_1) = N(-\alpha) = N(\alpha) \mid N(\alpha\beta\gamma).$$

Also ist $0 < N(\alpha_1\beta_1\gamma_1) \leq N(\alpha\beta\gamma)$. Wir müssen nun nur noch ausschließen, dass hier Gleichheit gilt. Aus $N(\alpha_1\beta_1\gamma_1) = N(\alpha) = N(\alpha\beta\gamma)$ würde aber $N(\beta) = N(\gamma) = 1$ folgen. Damit wären B_1, C_1 Einheiten in $\mathbb{Z}[\rho]$ und $\beta = \pm 1, \gamma = \pm 1$. Da (α, β, γ) ein Gegenbeispiel ist, gilt $\beta \neq \gamma$, so dass die Gleichheit $\alpha + \beta + \gamma = 0$ impliziert, dass $\alpha = 0$ gilt, wieder im Widerspruch dazu, dass (α, β, γ) ein Gegenbeispiel ist. $\square$

Literatur

[EHH+83] Ebbinghaus, H. D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Prestel, A. und Remmert, R.: *Zahlen*, Band 1 der Reihe *Grundwissen Mathematik [Basic Knowledge in Mathematics]*. Springer-Verlag, Berlin, 1983, ISBN 3-540-12666-X. https://doi.org/10.1007/978-3-642-96783-2, Edited and with an introduction by K. Lamotke.

[Lem17] Lemmermeyer, Franz: *Quadratische Zahlkörper: Eine Einführung mit vielen Beispielen*. Springer-Verlag, 2017.