KAPITEL 8

Integritätsringe

Wir haben die Vorlesung begonnen mit dem Studium von Eigenschaften der natürlichen und ganzen Zahlen. Im Folgenden werden wir betrachten, welche Eigenschaften sich auch auf andere Ringe übertragen lassen.

1. Einführung und Beispiele

Wir wiederholen nochmals die Definition:

DEFINITION. *Ein Ring R heißt* **Integritätsring** *(oder* **Integritätsbereich***), wenn R kommutativ ist, $1 \neq 0$ gilt und für $x, y \in R$ gilt:*

$$xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0.$$

Die letzte Bedingung lässt sich auch so formulieren:

$$x \neq 0 \text{ und } y \neq 0 \quad \Longrightarrow \quad xy \neq 0,$$

oder mit anderen Worten: Ein Produkt ist genau dann 0, wenn einer der Faktoren 0 ist.

Beispiele:

(1) $\mathbb{Z}$ ist ein Integritätsring.
(2) Körper sind Integritätsringe, also $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p = \mathbb{Z}_p$ für alle Primzahlen p.
(3) Unterringe von Integritätsringen sind Integritätsringe. Unterringe von Körpern sind Integritätsringe.
(4) Ist R ein Integritätsring, so ist auch der Polynomring $R[x]$ ein Integritätsring.
(5) Ist R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal, so ist der Faktorring $R/\mathfrak{p}$ ein Integritätsring. (Dies war die Definition eines Primideals.)

Für uns wichtige Beispiele sind Unterringe von sogenannten **quadratischen Zahlkörpern**, die in folgendem Satz behandelt werden.

SATZ. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$. Sei $\sqrt{d} \in \mathbb{C}$ eine Quadratwurzel von d. Dann gilt:*

(1) $\sqrt{d} \notin \mathbb{Q}$.
(2) *Für $a, b, a', b' \in \mathbb{Q}$ gilt*
$$a + b\sqrt{d} = a' + b'\sqrt{d} \quad \Longleftrightarrow \quad a = a' \text{ und } b = b'.$$
(3) *Für $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ gilt*
$$\begin{aligned} (a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \quad \text{und} \\ (a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) &= (a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d}. \end{aligned}$$
(4) *Es ist*
$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$
(5) $\mathbb{Q}[\sqrt{d}]$ *ist ein Körper. Für $(a, b) \neq (0, 0)$ gilt*
$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{(a + b\sqrt{d})(a - b\sqrt{d})} = \frac{a - b\sqrt{d}}{a^2 - db^2} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}.$$

Datei: alg_intringe.tex. Version vom 5.4.2024

(6) *Die Abbildung*
$$\mathrm{N} : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}, \quad a + b\sqrt{d} \mapsto (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$
ist multiplikativ, d.h. für $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ gilt
$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$
Außerdem gilt für $\alpha \in \mathbb{Q}[\sqrt{d}]$
$$\mathrm{N}(\alpha) = 0 \quad \Longleftrightarrow \quad \alpha = 0.$$
Die Abbildung N *wird* **Normabbildung** *genannt.*

Die behaupteten Eigenschaften sind so aufgeschrieben, dass sie klar oder leicht nachprüfbar sind.

Bemerkungen:

(1) Üblicherweise schreibt man i statt $\sqrt{-1}$.
(2) Im Fall $d < 0$ ist die Norm einfach das Quadrat des komplexen Absolutbetrags:
$$\mathrm{N}(\alpha) = |\alpha|^2.$$

2. Der Quotientenkörper eines Integritätsrings

Ist K ein Körper und $R \subseteq K$ ein Unterring, so ist R ein Integritätsring. Der kleinste Körper, der R enthält, ist dann
$$\{\frac{a}{b} \in K : a \in R, b \in R \setminus \{0\}\},$$
wie man mit den üblichen Bruchrechenregeln sieht. Man nennt ihn den **Quotientenkörper** von R und schreibt manchmal Quot(R). (Wir benutzen die übliche Bruchschreibweise $\frac{a}{b}$ für ab^{-1} und die entsprechenden Bruchrechenregeln.)

Beispiele:

(1) Der Quotientenkörper von $\mathbb{Z}$ ist $\mathbb{Q}$.
(2) Für $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ ist
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$
ein Ring mit dem quadratischen Zahlkörper
$$\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}$$
als Quotientenkörper.

Hat man zu einem Integritätsring keinen „natürlichen“ Quotientenkörper, so kann man sich einen mit folgender Konstruktion erstellen:

Konstruktion eines Quotientenkörpers zu einem Integritätsring R: Wir führen auf der Menge
$$M = \{(a, b) : a \in R, b \in R \setminus \{0\}\}$$
eine Relation $\sim$ ein:
$$(a, b) \sim (a', b') \quad \Longleftrightarrow \quad ab' = a'b.$$
Dies ist eine Äquivalenzrelation:

- *Reflexivität:* $(a, b) \sim (a, b)$.
- *Symmetrie:* $(a, b) \sim (a', b') \Longrightarrow (a', b') \sim (a, b)$.
- *Transitivität:* $(a, b) \sim (a', b'), (a', b') \sim (a'', b'') \Longrightarrow (a, b) \sim (a'', b'')$. Denn aus
$$(a, b) \sim (a', b') \implies ab' = a'b \implies ab'b'' = a'bb'' \implies ab'' \cdot b' = a'bb'',$$
$$(a', b') \sim (a'', b'') \implies a'b'' = a''b' \implies a'bb'' = a''bb' \implies a'bb'' = a''b \cdot b'$$
folgt $ab'' \cdot b' = a''b \cdot b'$, also wegen $b' \neq 0$ dann $ab'' = a''b$, und damit $(a, b) \sim (a'', b'')$. (Hier geht wesentlich ein, dass R ein Integritätsring ist.)

Die Äquivalenzklasse von (a,b) bezeichnen wir mit $\frac{a}{b}$, die Menge der Äquivalenzklassen mit

$$\mathrm{Quot}(R) = \{\frac{a}{b} : a \in R, b \in R \setminus \{0\}\}.$$

Dann gilt also

$$\frac{a}{b} = \frac{a'}{b'} \quad \Longleftrightarrow \quad (a,b) \sim (a',b') \quad \Longleftrightarrow \quad ab' = a'b.$$

- Addition und Multiplikation werden in $\mathrm{Quot}(R)$ so eingeführt:
$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \quad \text{und} \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$
Natürlich muss man zeigen, dass diese Verknüpfungen wohldefiniert sind, d.h. unabhängig von den ausgewählten Repräsentanten, was wir hier aber nicht machen.
- Es gilt
$$\frac{0}{1} = \frac{a}{b} \quad \Longleftrightarrow \quad 0 \cdot b = a \cdot 1 \quad \Longleftrightarrow \quad a = 0, \quad \text{also} \quad \frac{0}{1} = \{(0,b) : b \in R \setminus \{0\}\}$$
und
$$\frac{1}{1} = \frac{a}{b} \quad \Longleftrightarrow \quad 1 \cdot b = a \cdot 1 \quad \Longleftrightarrow \quad a = b, \quad \text{also} \quad \frac{1}{1} = \{(a,a) : a \in R \setminus \{0\}\}.$$
- Nun zeigt man, dass $\mathrm{Quot}(R)$ ein kommutativer Ring mit Null $\frac{0}{1}$ und Eins $\frac{1}{1}$ ist.
- Ist $\frac{a}{b} \in \mathrm{Quot}(R)$ mit $\frac{a}{b} \neq \frac{0}{1}$, so ist $a \neq 0$, also $\frac{b}{a} \in \mathrm{Quot}(R)$. Dann ist
$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$
Also ist
$$(\frac{a}{b})^{-1} = \frac{b}{a}.$$
Jedes von 0 verschiedene Element ist also invertierbar, weswegen $\mathrm{Quot}(R)$ ein Körper ist. Man nennt ihn den **Quotientenkörper** von R.
- Die Abbildung
$$R \to \mathrm{Quot}(R), \quad a \mapsto \frac{a}{1}$$
ist ein injektiver Ringhomomorphismus, weswegen man auch R als Teilmenge von $\mathrm{Quot}(R)$ betrachten kann.

Beispiele:

(1) Ist K ein Körper und x eine Unbestimmte über K, so schreibt man $K(x)$ für den Quotientenkörper des Polynomrings $K[x]$:
$$K(x) = \mathrm{Quot}(K[x]) = \{\frac{f}{g} : f, g \in K[x], g \neq 0\}.$$

(2) Ist R ein Integritätsring und K ein Körper mit $R \subseteq K$, so ist $\mathrm{Quot}(R)$ isomorph zum kleinsten Unterkörper von K, der R enthält.

Das folgende Lemma charakterisiert Einheiten mit Hilfe des Quotientenkörpers.

LEMMA. *Sei R ein Integritätsring mit Quotientenkörper K. Dann gilt für $a \in R \setminus \{0\}$:*

$$a \in R^* \quad \Longleftrightarrow \quad \frac{1}{a} \in R.$$

Beweis: $\Longrightarrow$ Ist $a \in R^*$, so gibt es ein $b \in R$ mit $ab = 1$. Dann ist aber $\frac{1}{a} = b \in R$.
$\Longleftarrow$ Ist $\frac{1}{a} \in R$, so ist $a \cdot \frac{1}{a} = 1$, also $a \in R^*$. ■

Beispiel: Wir betrachten Zahlen in $\mathbb{Z}[\sqrt{3}]$. Es ist

$$\frac{1}{1+\sqrt{3}} = \frac{1-\sqrt{3}}{(1+\sqrt{3})(1-\sqrt{3})} = \frac{1-\sqrt{3}}{-2} = -\frac{1}{2} + \frac{1}{2}\sqrt{3} \notin \mathbb{Z}[\sqrt{3}].$$

Also ist $1+\sqrt{3}$ keine Einheit in $\mathbb{Z}[\sqrt{3}]$. Weiter gilt

$$\frac{1}{2+\sqrt{3}} = \frac{2-\sqrt{3}}{(2+\sqrt{3})(2-\sqrt{3})} = \frac{2-\sqrt{3}}{1} = 2-\sqrt{3} \in \mathbb{Z}[\sqrt{3}],$$

also ist $2+\sqrt{3}$ eine Einheit in $\mathbb{Z}[\sqrt{3}]$.

3. Teilbarkeit

DEFINITION. *Sei R ein Integritätsring. Zwei Elemente $a, b \in R$ heißen* **assoziiert**, *in Zeichen $a \sim b$, wenn es eine Einheit $u \in R^*$ gibt mit $b = au$, d.h. wenn sich a und b multiplikativ nur um eine Einheit unterscheiden.*

Beispiele:

(1) In $\mathbb{Z}$ sind nur ± 1 Einheiten. Ganze Zahlen sind also genau dann assoziiert, wenn sie sich nur ums Vorzeichen unterscheiden.
(2) Ist K ein Körper, so sind die Einheiten des Polynomrings $K[x]$ genau die Konstanten $\neq 0$. Zwei Polynome sind also assoziiert, wenn sie sich nur um eine multiplikative Konstante unterscheiden.

Das folgende Lemma ist leicht zu beweisen:

LEMMA. *Sei R ein Integritätsring mit Quotientenkörper K.*

(1) *Assoziiertheit ist eine Äquivalenzrelation.*
(2) *Für $a \in R$ gilt:*
$$a \sim 0 \quad\Longleftrightarrow\quad a = 0.$$
(3) *Für $a \in R$ gilt:*
$$a \sim u \text{ für ein } u \in R^* \quad\Longleftrightarrow\quad a \in R^*.$$
(4) *Für $a, b \in R \setminus \{0\}$ gilt:*
$$a \sim b \quad\Longleftrightarrow\quad \frac{a}{b} \in R \text{ und } \frac{b}{a} \in R.$$

Wichtiger ist folgende Eigenschaft:

SATZ. *Für Elemente a, b eines Integritätsrings R gilt:*
$$(a) = (b) \quad\Longleftrightarrow\quad a \sim b.$$
(Dabei bezeichnet (a) das von a erzeugte Hauptideal $Ra = \{ra : r \in R\}$.)

Beweis:

- $\Longrightarrow$ Aus $(a) = (b)$ folgt $b \in (a)$ und $a \in (b)$, also gibt es $r, s \in R$ mit $b = ra$ und $a = sb$. Dann ist $a = sb = sra$, also
$$a(1 - sr) = 0.$$
Fall $a = 0$: Dann ist auch $b = 0$, und wegen $0 = 1 \cdot 0$ gilt $a \sim b$.
Fall $a \neq 0$: Dann folgt $1 = sr$, also sind r und s Einheiten, was $a \sim b$ beweist.
- $\Longleftarrow$ Sei $a \sim b$, d.h. $b = au$ mit $u \in R^*$. Dann gilt $b \in (a)$, also $(b) \subseteq (a)$. Wegen $u^{-1} \in R$ folgt aus $a = u^{-1}b$ dann $a \in (b)$, also $(a) \subseteq (b)$. Zusammen ergibt sich $(a) = (b)$. ■

Teilbarkeit wird wie im Ring $\mathbb{Z}$ definiert:

DEFINITION. *Sei R ein Integritätsring. Für $a, b \in R$ sagt man „a* **teilt** *b“ (oder „a ist ein* **Teiler** *von b“ oder „b ist ein* **Vielfaches** *von a“) und schreibt $a \mid b$, falls ein $c \in R$ existiert mit $b = da$. Teilt a die b nicht, so schreibt man $a \nmid b$.*

Viele Teilbarkeitsregeln übertragen sich von $\mathbb{Z}$ auf einen Integritätsring R, sodass wir hier nicht ausführlich darauf eingehen. Ein paar Eigenschaften seien aber erwähnt:

Satz. *Sei R ein Integritätsring (mit Quotientenkörper K).*

(1) *Für $a, b \in R$ gilt*
$$a \mid b \quad \iff \quad (b) \subseteq (a).$$
(2) *Für $a, b \in R$ und $u, v \in R^*$ gilt:*
$$a \mid b \quad \iff \quad ua \mid vb.$$
Anders ausgedrückt mit $a, a', b, b' \in R$:
$$a \sim a' \text{ und } b \sim b' \quad \Longrightarrow \quad \Big(a \mid b \iff a' \mid b'\Big).$$
(3) *Für $a, b \in R$ gilt:*
$$a \mid b \quad \iff \quad b \equiv 0 \bmod (a).$$
(4) *Für $a \in R \setminus \{0\}$ und $b \in R$ gilt:*
$$a \mid b \quad \iff \quad \frac{b}{a} \in R.$$

Beweis: Die Aussagen folgen fast unmittelbar aus den Definitionen. ■

Wir werden im Folgenden Beispiele mit Ringen der Art $\mathbb{Z}[\sqrt{d}]$ behandeln. Daher stellen wir im folgenden Satz ein paar Eigenschaften zusammen:

Satz. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$. Dann ist*
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$
ein Integritätsring mit Quotientenkörper
$$\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}.$$
Die Normabbildung $\mathrm{N} : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ ist gegeben durch
$$\mathrm{N}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$
Es gilt für $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$:

(1) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, *d.h. die Norm ist multiplikativ.*
(2) $\mathrm{N}(\alpha) = 0 \iff \alpha = 0$.
(3) *Die Einheiten von $\mathbb{Z}[\sqrt{d}]$ lassen sich mit der Normabbildung so charakterisieren:*
$$\alpha \in \mathbb{Z}[\sqrt{d}]^* \quad \iff \mathrm{N}(\alpha) = \pm 1,$$
also für $a, b \in \mathbb{Z}$
$$a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^* \quad \iff \quad a^2 - db^2 = \pm 1.$$
(4) *Für die Teilbarkeit gilt:*
$$\alpha \mid \beta \quad \Longrightarrow \quad \mathrm{N}(\alpha) \mid \mathrm{N}(\beta).$$
(5) *Teilbarkeit lässt sich für $\alpha \neq 0$ so charakterisieren:*
$$\alpha \mid \beta \quad \iff \quad \frac{\overline{\alpha}\beta}{\mathrm{N}(\alpha)} \in \mathbb{Z}[\sqrt{d}].$$
Dabei ist $\overline{\alpha} = a - b\sqrt{d}$ für $\alpha = a + b\sqrt{d}$.
(6) *Für $a, b, m, n \in \mathbb{Z}$ gilt*
$$m \mid a + b\sqrt{d} \quad \iff \quad m \mid a \text{ und } m \mid b.$$
Außerdem
$$m \mid n \text{ in } R \quad \iff \quad m \mid n \text{ in } \mathbb{Z}.$$
(7) *Für $\alpha \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}$ gilt*
$$\left|\mathbb{Z}[\sqrt{d}]/(\alpha)\right| = |\mathrm{N}(\alpha)|.$$

Beweis: Wir beweisen nur, was nicht schon zuvor erwähnt wurde.

(3) $\Longrightarrow$ Ist $\alpha \in \mathbb{Z}[\sqrt{d}]^*$, so gibt es ein $\beta \in \mathbb{Z}[\sqrt{d}]$ mit $\alpha\beta = 1$. Normbildung liefert
$$\mathrm{N}(\alpha)\mathrm{N}(\beta) = 1.$$
Wegen $\mathrm{N}(\alpha), \mathrm{N}(\beta) = 1$ folgt $\mathrm{N}(\alpha) \in \{\pm 1\}$.
$\Longleftarrow$ Ist $\mathrm{N}(a + b\sqrt{d}) = \pm 1$, so ist
$$\pm 1 = a^2 - b^2 d = (a + b\sqrt{d})(a - b\sqrt{d}),$$
woraus man sofort sieht, dass $a + b\sqrt{d}$ eine Einheit ist.

(4) Gilt $\alpha \mid \beta$, so gibt es ein $\gamma \in \mathbb{Z}[\sqrt{d}]$ mit $\beta = \alpha\gamma$. Normbildung liefert
$$\mathrm{N}(\beta) = \mathrm{N}(\alpha)\mathrm{N}(\gamma), \quad \text{also} \quad \mathrm{N}(\alpha) \mid \mathrm{N}(\beta).$$

(5) Ist $\alpha = a + b\sqrt{d}$ und $\overline{\alpha} = a - b\sqrt{d}$, so gilt für $\alpha \neq 0$:
$$\alpha \mid \beta \quad \Longleftrightarrow \quad \frac{\beta}{\alpha} \in \mathbb{Z}[\sqrt{d}] \quad \Longleftrightarrow \quad \frac{\overline{\alpha}\beta}{\overline{\alpha}\alpha} \in \mathbb{Z}[\sqrt{d}] \quad \Longleftrightarrow \quad \frac{\overline{\alpha}\beta}{\mathrm{N}(\alpha)} \in \mathbb{Z}[\sqrt{d}],$$
was zu zeigen war.

(6) Es gilt:
$$\begin{aligned} m \mid a + b\sqrt{d} \quad &\Longleftrightarrow \quad a + b\sqrt{d} = m(a' + b'\sqrt{d}) \text{ für Zahlen } a', b' \in \mathbb{Z} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad a = ma' \text{ und } b = mb' \text{ mit Zahlen } a', b' \in \mathbb{Z} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad m \mid a \text{ und } m \mid b. \end{aligned}$$
Die zweite Aussage ist ein Spezialfall der ersten mit $a = n$ und $b = 0$.

(7) Ein Beweis findet sich im Anhang zu diesem Kapitel. ■

Beispiel: In $\mathbb{Z}[\sqrt{3}]$ gilt
$$\mathrm{N}(1 + \sqrt{3}) = -2 \quad \text{und} \quad \mathrm{N}(2 + \sqrt{3}) = 1,$$
also hat man
$$1 + \sqrt{3} \notin \mathbb{Z}[\sqrt{3}]^* \quad \text{und} \quad 2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]^*.$$

Im imaginärquadratischen Fall, d.h. für $d < 0$ sind die Einheiten der Ringe $\mathbb{Z}[\sqrt{d}]$ einfach anzugeben:

Folgerung. *Für $d \in \mathbb{Z}_{<0}$ gilt:*
$$\mathbb{Z}[\sqrt{d}]^* = \{x + y\sqrt{d} : x^2 + |d|y^2 = 1\} = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & \text{für } d = -1, \\ \{\pm 1\} & \text{für } d \leq -2. \end{cases}$$

Bemerkung: Im reellquadratischen Fall d.h. für $d > 0$ (und $d \in \mathbb{N} \setminus \{n^2 : n \in \mathbb{N}\}$) ist die Einheitengleichung
$$x^2 - dy^2 = \pm 1.$$
Solche Gleichungen bezeichnet man auch als **Pellsche Gleichungen**. Die Gleichung $x^2 - dy^2 = 1$ hat unendlich viele Lösungen, worauf wir hier aber nicht näher eingehen. Beispielsweise gilt
$$\mathbb{Z}[\sqrt{2}]^* = \{\pm(1 + \sqrt{2})^k : k \in \mathbb{Z}\}.$$

Bemerkung:

(1) In $\mathbb{Z}$ gibt es nur die Einheiten ± 1, daher sind zu $a \in \mathbb{Z}$ nur $\pm a$ assoziiert.

(2) In $\mathbb{Z}[i]$ (mit $i^2 = -1$) gibt es die Einheiten $\pm 1, \pm i$. Wegen
$$-(a + bi) = -a - bi, \quad i(a + bi) = -b + ai, \quad (-i)(a + bi) = b - ai$$
sind zu $a + bi \in \mathbb{Z}[i]$ genau die Elemente
$$a + bi, \quad -a - bi, \quad b - ai, \quad -b + ai$$
assoziiert.

(3) In reellquadratischen Ringen $\mathbb{Z}[\sqrt{d}]$ (mit $d > 0$) sieht man die Assoziiertheit nicht immer auf den ersten Blick. Wegen
$$2+\sqrt{3} \in \mathbb{Z}[\sqrt{3}]^* \quad \text{und} \quad (2+\sqrt{3})\cdot\sqrt{3} = 3+2\sqrt{3}$$
sind beispielsweise die Elemente $\sqrt{3}$ und $3+2\sqrt{3}$ im Ring $\mathbb{Z}[\sqrt{3}]$ assoziiiert.

Definition. *Sei R ein Integritätsring. Ein Element $a \in R \setminus (R^* \cup \{0\})$ heißt* **irreduzibel***, wenn für alle $b, c \in R$ mit $a = b \cdot c$ eine der folgenden äquivalenten Aussagen folgt:*

- *$b \in R^*$ oder $c \in R^*$.*
- *$a \sim b$ oder $a \sim c$.*
- *$(a) = (b)$ oder $(a) = (c)$.*

(Das Element a lässt sich also nur trivial zerlegen als $a = u \cdot (u^{-1}a) = (u^{-1}a) \cdot u$ mit einer Einheit u.)

Beispiel: In $\mathbb{Z}$ sind die irreduziblen Elemente genau die Zahlen $\pm p$, wo p eine Primzahl ist. Man hat nur die trivalen Zerlegungen
$$p = 1 \cdot p = (-1)\cdot(-p) = p \cdot 1 = (-p)\cdot(-1)$$
und
$$-p = 1 \cdot (-p) = (-1)\cdot p = (-p)\cdot 1 = p \cdot (-1).$$

Beispiel: Wir betrachten in $\mathbb{Z}[\sqrt{-7}]$ das Element $\alpha = 1+\sqrt{-7}$ mit Norm 8. Ist α irreduzibel? Wir setzen an: $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{Z}[\sqrt{-7}]$. Es folgt durch Normbildung
$$8 = \mathrm{N}(\beta)\mathrm{N}(\gamma),$$
wobei wir o.E. $\mathrm{N}(\beta) \le \mathrm{N}(\gamma)$ annehmen können. Dann ist
$$\mathrm{N}(\beta) \in \{1, 2\}.$$
Ist $\mathrm{N}(\beta) = 1$, so ist β eine Einheit, also ist $\alpha = \beta\gamma$ nur eine triviale Zerlegung. Aus
$$\mathrm{N}(x + y\sqrt{-7}) = x^2 + 7y^2$$
sieht man sofort, dass 2 nicht als Norm vorkommt, d.h. es gibt kein Element $\beta \in \mathbb{Z}[\sqrt{-7}]$ mit $\mathrm{N}(\beta) = 2$. Daher ist $\alpha = 1 + \sqrt{-7}$ irreduzibel.

Bemerkung: Ist R ein Integritätsring, so gilt für $g, h \in R[x]$ die Gradformel
$$\mathrm{grad}(gh) = \mathrm{grad}(g) + \mathrm{grad}(h).$$
Will man ein Polynom $f \in R[x]$ vom Grad $n \ge 1$ auf Irreduzibilität untersuchen, also
$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
so kann man den Ansatz $f = gh$ machen mit $g, h \in R[x]$ und $\mathrm{grad}(f) = \mathrm{grad}(g) + \mathrm{grad}(h)$, also
$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \quad \text{und} \quad h = c_{n-m}x^{n-m} + c_{n-m-1}x^{n-m-1} + \cdots + c_1 x + c_0.$$
Die Zahlen $b_m, \ldots, b_0, c_{n-m}, \ldots, c_0$ sind unbekannt. Durch Ausmultiplizieren und Koeffizientenvergleich erhält man Gleichungen für $b_m, \ldots, c_0$, die man versuchen kann zu lösen.

Satz. *Sei K ein Körper und $f \in K[x]$.*

(1) *Ist $\mathrm{grad}(f) = 1$, so ist f irreduzibel.*
(2) *Ist $\mathrm{grad}(f) \in \{2, 3\}$, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.*
(3) *Ist $\mathrm{grad}(f) \ge 2$ und findet man ein $x_0 \in K$ mit $f(x_0) = 0$, so gibt es ein $g \in K[x]$ vom Grad $\mathrm{grad}(f) - 1$ mit $f(x) = (x - x_0)\cdot g(x)$, insbesondere ist f nicht irreduzibel.*

Beweis:

(1) Ist $\mathrm{grad}(f) = 1$, so folgt aus $f = gh$ die Gradgleichung $1 = \mathrm{grad}(f) = \mathrm{grad}(g) + \mathrm{grad}(h)$, also $\mathrm{grad}(g) = 0$ oder $\mathrm{grad}(h) = 0$. Dann ist also $g \in K^*$ oder $h \in K^*$, was die Irreduzibilität von f beweist.

(2) Sei nun $\mathrm{grad}(f) \in \{2,3\}$. Wir nehmen an, dass f nicht irreduzibel ist. Dann gibt es $g, h \in K[x]$ mit $f = gh$ und $\mathrm{grad}(g), \mathrm{grad}(h) \geq 1$. O.E. können wir $\mathrm{grad}(g) \leq \mathrm{grad}(h)$ annehmen. Aus $\mathrm{grad}(f) = \mathrm{grad}(g) + \mathrm{grad}(h)$ folgt dann $\mathrm{grad}(g) = 1$, also $g = b_1 x + b_0$. Dann ist $-\frac{b_0}{b_1}$ eine Nullstelle von g und damit auch von f.
Ist umgekehrt $x_0 \in K$ eine Nullstelle von f, so liefert Polynomdivision eine Zerlegung

$$f = q \cdot (x - x_0) + r \qquad \text{mit } \mathrm{grad}(r) < 1.$$

Setzen wir $x = x_0$ ein, so ergibt sich $0 = r(0)$, woraus wegen $\mathrm{grad}(f) < 1$ sofort $r = 0$ und damit

$$f = q \cdot (x - x_0)$$

folgt. Dann ist aber f nicht irreduzibel.
(3) Dies haben wir bereits in (2) gezeigt. ■

Lemma. *Sei R ein Integritätsring. Für $a \in R$ gilt dann:*

$$a \text{ irreduzibel} \quad \Longleftrightarrow \quad (0) \subsetneq (a) \subsetneq R \text{ und } \Big((a) \subseteq (b) \subseteq R \Longrightarrow (a) = (b) \text{ oder } (b) = R\Big).$$

Bemerkung: Bei den ganzen Zahlen sind die irreduziblen Elemente bis auf Assoziiertheit genau die Primzahlen. Ist p eine Primzahl, so war auch folgende Eigenschaft wichtig:

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b.$$

Es stellt sich heraus, dass dies eine wichtige Eigenschaft ist, die in allgemeinen Integritätsringen nicht aus der Irreduzibilität folgt.

Definition. *Sei R ein Integritätsring. Ein Element $p \in R \setminus (R^* \cup \{0\})$ heißt* **Primelement** *oder* **prim***, wenn für alle $a, b \in R$ die Implikation gilt:*

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b.$$

Beispiel: In $\mathbb{Z}$ sind die Primelemente genau die Zahlen $\pm p$ für Primzahlen p.

Lemma. *Sei R ein Integritätsring. Dann gilt:*
(1) *Ist $p \in R$ ein Primelement, so ist p irreduzibel.*
(2) *Für $p \in R \setminus \{0\}$ gilt:*

$$p \text{ Primelement} \quad \Longleftrightarrow \quad (p) \text{ Primideal.}$$

Beweis:
(1) Sei p ein Primelement. Wir setzen an $p = ab$ um die Irreduzibilität zu zeigen. Aus $p = ab$ folgt aber $p \mid ab$, also gilt $p \mid a$ oder $p \mid b$. O.E. gelte $p \mid a$. Dann gibt es ein $c \in R$ mit $a = pc$. Insgesamt erhalten wir

$$p = ab = pcb, \qquad \text{also} \qquad 1 = bc.$$

Es folgt $b \in R^*$, also $p \sim b$, was die Irreduzibilität von p beweist.
(2) Für $p \in R \setminus \{0\}$ sind äquivalent:

$$\begin{aligned} (p) \text{ Primideal} \quad &\Longleftrightarrow \quad xy \in (p) \Longrightarrow x \in (p) \text{ oder } y \in (p) \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad (xy) \subseteq (p) \Longrightarrow (x) \subseteq (p) \text{ oder } (y) \subseteq (p) \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad p \mid xy \Longrightarrow p \mid x \text{ oder } p \mid y \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad p \text{ Primelement.} \end{aligned}$$

Damit ist alles bewiesen. ■

Bemerkung: In einem Integritätring R ist (0) ein Primideal, aber 0 ist (nach Definition) kein Primelement.

Beispiel: Wir haben gesehen, dass $1+\sqrt{-7}$ in $\mathbb{Z}[\sqrt{-7}]$ irreduzibel ist. Ist $1+\sqrt{-7}$ ein Primelement? Aus $(1+\sqrt{-7})(1-\sqrt{-7}) = 8$ sieht man, dass

$$1+\sqrt{-7} \mid 2 \cdot 4$$

gilt. Nun ist aber

$$\frac{2}{1+\sqrt{-7}} = \frac{1-\sqrt{-7}}{4} \notin \mathbb{Z}[\sqrt{-7}] \quad \text{und} \quad \frac{4}{1+\sqrt{-7}} = \frac{1-\sqrt{-7}}{2} \notin \mathbb{Z}[\sqrt{-7}],$$

also gilt

$$1+\sqrt{-7} \nmid 2 \quad \text{und} \quad 1+\sqrt{-7} \nmid 4.$$

Daher ist $1+\sqrt{-7}$ kein Primelement.

Definition. *Seien a, b Elemente eines Integritätsrings R.*

(1) *$d \in R$ heißt ein* **größter gemeinsamer Teiler** *(ggT) von a und b, wenn gilt*
- *$d \mid a$ und $d \mid b$.*
- *$d' \mid a$ und $d' \mid b \Longrightarrow d' \mid d$.*

(2) *$e \in R$ heißt ein* **kleinstes gemeinsames Vielfaches** *(kgV) von a und b, wenn gilt*
- *$a \mid e$ und $b \mid e$.*
- *$a \mid e'$ und $b \mid e' \Longrightarrow e \mid e'$.*

Bemerkungen:

(1) Da man in einem Integritätsring im Allgemeinen keine Anordnung wie in $\mathbb{Z}$ gegeben hat, erfolgt die Definition von ggT und kgV über eine Charakterisierung, wie sie auch in $\mathbb{Z}$ gilt. (In $\mathbb{Z}$ hatten wir zusätzlich noch $\mathrm{ggT}(a,b) \geq 0$ und $\mathrm{kgV}(a,b) \geq 0$ gefordert.)

(2) ggT und kgV müssen nicht existieren.

(3) Ist d ein ggT von $a, b \in R$, so sind die größten gemeinsamen Teiler von a und b genau die zu d assoziierten Elemente.

(4) Ist e ein kgV von $a, b \in R$, so sind die kleinsten gemeinsamen Vielfachen von a und b genau die zu e assoziierten Elemente.

Beispiel: Wir betrachten den Ring $\mathbb{Z}[\sqrt{-3}]$. Die Einheiten sind ± 1. Hier ist eine Liste mit den Elementen aus R mit Norm ≤ 16:

$\mathrm{N}(\alpha)$	α
0	0
1	± 1
3	$\pm\sqrt{-3}$
4	$\pm(1+\sqrt{-3})$, $\pm(1-\sqrt{-3})$, ± 2
7	$\pm(2+\sqrt{-3})$, $\pm(2-\sqrt{-3})$
9	± 3
12	$\pm 2\sqrt{-3}$, $\pm(3+\sqrt{-3})$, $\pm(3-\sqrt{-3})$
13	$\pm(1+2\sqrt{-3})$, $\pm(1-2\sqrt{-3})$
16	$\pm(2+2\sqrt{-3})$, $\pm(2-2\sqrt{-3})$, ± 4

(1) Die Zahlen 4 und $2+2\sqrt{-3}$ haben beide Norm 16. Da 2 und 8 als Normen nicht vorkommen, müssen nichttriviale Teiler der beiden Zahlen die Norm 4 haben. Man findet, dass

$$\pm(1+\sqrt{-3}), \quad \pm(1-\sqrt{-3}), \quad \pm 2$$

gemeinsame Teiler der beiden Zahlen sind. Da die drei Zahlen nicht assoziiert sind, kann es keinen größten gemeinsamen Teiler geben.

(2) Wir betrachten die Zahlen 2 und $1+\sqrt{-3}$, die beide Norm 4 haben. Gemeinsame Vielfache sind die Zahlen mit Norm 16:
$$\pm(2+2\sqrt{-3}), \quad \pm(2-2\sqrt{-3}), \quad \pm 4.$$
Da die Zahlen nicht assoziiert sind, kann es kein kgV geben.

(3) Wir betrachten 2 und $1+\sqrt{-3}$, beide mit Norm 4. Da es keine Elemente mit Norm 2 gibt, ist 1 ein ggT der beiden Zahlen.

Im letzten Beispiel sieht man einen Ring R mit Elementen a, b, die einen ggT, aber kein kgV besitzen. Dagegen gilt folgender Satz:

Satz. *Sei R ein Integritätsring und $a, b \in R \setminus \{0\}$, sodass a und b ein kgV e besitzen. Dann gilt:*

(1) *$d = \frac{ab}{e}$ ist ein ggT von a und b.*

(2) *$de = ab$, also $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) \sim ab$.*

4. Euklidische Ringe

Definition. *Sei R ein Integritätsring. Eine Funktion $\nu : R \to \mathbb{N}_0$ heißt* **euklidische Bewertungsfunktion**, *wenn für alle $a, b \in R$ mit $b \neq 0$ Zahlen $r, q \in R$ existieren mit*
$$a = qb + r \quad \text{und} \quad \nu(r) < \nu(b).$$
Ein Integritätsring R heißt **euklidischer Ring**, *wenn es eine euklidische Bewertungsfunktion für R gibt. (Wir sagen auch, R hat eine* **Division mit Rest**.*)*

Beispiele:

(1) $\mathbb{Z}$ ist ein euklidischer Ring mit der Bewertungsfunktion $\nu(x) = |x|$: Zu $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren $q, r \in \mathbb{Z}$ mit
$$a = qb + r \text{ und } 0 \leq r < |b|, \quad \text{was insbesondere} \quad |r| < |b|$$
liefert.

(2) Ist K ein Körper, so ist der Polynomring $K[x]$ ein euklidischer Ring: Zu $a, b \in K[x]$ mit $b \neq 0$ existieren Polynome $q, r \in K[x]$ mit
$$a = qb + r \quad \text{und} \quad \mathrm{grad}(r) < \mathrm{grad}(b).$$
Wegen $\mathrm{grad}(0) = -\infty$ erhält man eine zugehörige euklidische Bewertungsfunktion ν, wenn man setzt
$$\nu(f) = \begin{cases} 0 & \text{für } f = 0, \\ \mathrm{grad}(f) + 1 & \text{für } f \neq 0. \end{cases}$$

Bemerkung: Ist R ein Integritätsring, sind $a, b \in R$ mit $b \neq 0$, so hat man natürlich die triviale Zerlegung
$$a = 0 \cdot b + a,$$
die Gleichung $a = qb + r$ hat also die Lösung $q = 0$ und $r = a$. Bei einem euklidischen Ring sollte r „kleiner als“ b sein. Dazu dient die euklidische Bewertungsfunktion.

Auch in $\mathbb{Z}[i]$ hat man eine Division mit Rest. Zuvor erinnern wir an eine Schreibweise: Für $x \in \mathbb{R}$ bezeichnet $\lfloor x \rceil$ eine x nächstliegende ganze Zahl. Es ist $|x - \lfloor x \rceil| \leq \frac{1}{2}$. Im Fall $x \in \frac{1}{2} + \mathbb{Z}$ kann man für $\lfloor x \rceil$ sowohl $x - \frac{1}{2}$ also auch $x + \frac{1}{2}$ wählen. Wir werden häufig
$$\lfloor x \rceil = \left\lfloor x + \frac{1}{2} \right\rfloor$$
benutzen.

Satz. *Sind $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$, so ist*

$$\frac{a}{b} = u + vi \in \mathbb{Q}[i] \text{ mit } u, v \in \mathbb{Q}.$$

Definiert man

$$q = \lfloor u \rceil + \lfloor v \rceil i \quad \text{und} \quad r = a - qb,$$

so gilt

$$a = qb + r \quad \text{und} \quad \mathrm{N}(r) \leq \frac{1}{2}\mathrm{N}(b) < \mathrm{N}(b).$$

Insbesondere ist die Norm eine euklidische Bewertungsfunktion und $\mathbb{Z}[i]$ ein euklidischer Ring.
Noch etwas konkreter: Schreibt man $a = a_0 + a_1 i$, $b = b_0 + b_1 i$ mit $a_0, a_1, b_0, b_1 \in \mathbb{Z}$, berechnet man

$$\begin{array}{c} z_0 = a_0 b_0 + a_1 b_1, \quad z_1 = a_1 b_0 - a_0 b_1, \quad n = b_0^2 + b_1^2, \\ q_0 = \left\lfloor \dfrac{2z_0 + n}{2n} \right\rfloor \quad \text{und} \quad q_1 = \left\lfloor \dfrac{2z_1 + n}{2n} \right\rfloor, \\ r_0 = a_0 - q_0 b_0 + q_1 b_1 \quad \text{und} \quad r_1 = a_1 - q_0 b_1 - q_1 b_0, \end{array}$$

so gilt

$$q = q_0 + q_1 i \quad \text{und} \quad r = r_0 + r_1 i.$$

Beweis: Hier ist $\mathrm{N}(x + yi) = x^2 + y^2 = |x + iy|^2$ mit dem komplexen Absolutbetrag. Es ist

$$\begin{aligned} \mathrm{N}(r) &= |r|^2 = |a - qb|^2 = \left|\frac{a}{b} - q\right|^2 |b|^2 = \left|(u + vi) - (\lfloor u \rceil + \lfloor v \rceil i)\right|^2 |b|^2 = \\ &= \left|(u - \lfloor u \rceil) + (v - \lfloor v \rceil)i\right|^2 |b|^2 = \left((u - \lfloor u \rceil)^2 + (v - \lfloor v \rceil)^2\right) |b|^2 \leq \\ &\leq \left((\frac{1}{2})^2 + (\frac{1}{2})^2\right) |b|^2 = \frac{1}{2}|b|^2 = \frac{1}{2}\mathrm{N}(b). \end{aligned}$$

Daraus folgt die Behauptung.
Zu der Konkretisierung: Mit $a = a_0 + a_1 i$, $b = b_0 + b_1 i$ und $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ gilt:

$$\frac{a}{b} = \frac{a_0 + a_1 i}{b_0 + b_1 i} = \frac{(a_0 + a_1 i)(b_0 - b_1 i)}{(b_0 + b_1 i)(b_0 - b_1 i)} = \frac{(a_0 b_0 + a_1 b_1) + (a_1 b_0 - a_0 b_1)i}{b_0^2 + b_1^2}.$$

Definiert man also

$$z_0 = a_0 b_0 + a_1 b_1, \quad z_1 = a_1 b_0 - a_0 b_1, \quad n = b_0^2 + b_1^2,$$

so gilt

$$\frac{a}{b} = \frac{z_0}{n} + \frac{z_1}{n} i.$$

Wir wollen die Koeffizienten runden und definieren $q = q_0 + q_1 i \in \mathbb{Z}[i]$ durch

$$q_0 = \left\lfloor \frac{z_0}{n} \right\rceil = \left\lfloor \frac{z_0}{n} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{2z_0 + n}{2n} \right\rfloor \quad \text{und} \quad q_1 = \left\lfloor \frac{z_1}{n} \right\rceil = \left\lfloor \frac{z_1}{n} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{2z_1 + n}{2n} \right\rfloor.$$

Damit bilden wir $r = a - qb$, also

$$\begin{aligned} r &= a - qb = (a_0 + a_1 i) - (q_0 + q_1 i)(b_0 + b_1 i) = \\ &= (a_0 + a_1 i) - (q_0 b_0 - q_1 b_1 + q_0 b_1 i + q_1 b_0 i) = \\ &= (a_0 - q_0 b_0 + q_1 b_1) + (a_1 - q_0 b_1 - q_1 b_0) i. \end{aligned}$$

Mit

$$r_0 = a_0 - q_0 b_0 + q_1 b_1 \quad \text{und} \quad r_1 = a_1 - q_0 b_1 - q_1 b_0$$

gilt daher $r = r_0 + r_1 i$.
Dabei haben wir als Rundungsfunktion

$$\lfloor x \rceil = \left\lfloor x + \frac{1}{2} \right\rfloor$$

benutzt. ■

Bemerkung: Kennt man für einen euklidischen Ring eine zugehörige **Division mit Rest**, so kann man leicht den euklidischen Algorithmus und den erweiterten euklidischen Algorithmus auf diesen Ring übertragen.

Satz (Euklidischer Algorithmus). *Sei R ein euklidischer Ring mit einer euklidischen Bewertungsfunktion $\nu : R \to \mathbb{N}_0$.*

- *Es sei ein Verfahren bekannt, wie man zu $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ bestimmt mit*
$$a = qb + r \text{ und } \nu(r) < \nu(b).$$

Seien $a, b \in R$ gegeben. Rekursiv werden Elemente $a_i \in R$ definiert, wobei man mit $a_0 = a$ und $a_1 = b$ beginnt. Sind für einen Index $i \geq 0$ die Zahlen a_i und a_{i+1} bereits definiert, so unterscheidet man:

- *Ist $a_{i+1} = 0$, so bricht man ab. (Es sei n der größte Index mit $a_{n+1} = 0$.)*
- *Ist $a_{i+1} \neq 0$, so dividiert man a_i durch a_{i+1} und erhält den Quotienten q_i und den Rest a_{i+2}:*
$$a_i = q_i a_{i+1} + a_{i+2} \text{ mit } \nu(a_{i+2}) < \nu(a_{i+1}).$$
(Wegen $0 \leq \nu(a_{i+2}) < \nu(a_{i+1})$ hört das Verfahren nach endlich vielen Schritten auf.)

Explizit ergibt sich das Schema (im Fall $a_1 \neq 0$):

$$\begin{array}{rcl} a_0 &=& q_0 a_1 + a_2 \quad \text{mit} \quad 0 < \nu(a_2) < \nu(a_1), \\ a_1 &=& q_1 a_2 + a_3 \quad \text{mit} \quad 0 < \nu(a_3) < \nu(a_2), \\ &\vdots& \\ a_i &=& q_i a_{i+1} + a_{i+2} \quad \text{mit} \quad 0 < \nu(a_{i+2}) < \nu(a_{i+1}), \\ &\vdots& \\ a_{n-2} &=& q_{n-2} a_{n-1} + a_n \quad \text{mit} \quad 0 < \nu(a_n) < \nu(a_{n-1}), \\ a_{n-1} &=& q_{n-1} a_n + 0. \end{array}$$

Dann ist a_n ein größter gemeinsamer Teiler von a und b.

Beweis: Aus $a_i = q_i a_{i+1} + a_{i+2}$ folgt für $d \in R$:
$$d \mid a_i \text{ und } d \mid a_{i+1} \quad \Longleftrightarrow \quad d \mid a_{i+1} \text{ und } d \mid a_{i+2}.$$
Damit erhält man
$$\begin{array}{rl} d \mid a \text{ und } d \mid b & \Longleftrightarrow \; d \mid a_0 \text{ und } d \mid a_1 \; \Longleftrightarrow \; d \mid a_1 \text{ und } d \mid a_2 \; \Longleftrightarrow \\ & \Longleftrightarrow \; d \mid a_2 \text{ und } d \mid a_2 \; \Longleftrightarrow \; \ldots \; \Longleftrightarrow \; d \mid a_{n-2} \text{ und } d \mid a_{n-1} \; \Longleftrightarrow \\ & \Longleftrightarrow \; d \mid a_{n-1} \text{ und } d \mid a_n \; \Longleftrightarrow \; d \mid a_n. \end{array}$$
Hieraus sieht man zunächst, dass a_n ein gemeinsamer Teiler von a und b ist, dann, dass a_n auch ein größter gemeinsamer Teiler von a und b ist. ■

Beispiel: Wir wollen in $\mathbb{Z}[i]$ einen ggT von $2 + 11i$ und $9 - 8i$ bestimmen. Wir setzen $a_0 = 2 + 11i$ und $a_1 = 9 - 8i$.

- Wir berechnen
$$\frac{a_0}{a_1} = \frac{2 + 11i}{9 - 8i} = -\frac{14}{29} + \frac{23}{29} i \approx -0.48 + 0.79i, \quad \text{setzen deshalb} \quad q_0 = i$$
und bilden damit
$$a_2 = a_0 - q_0 a_1 = (2 + 11i) - i(9 - 8i) = -6 + 2i.$$
- Wir berechnen
$$\frac{a_1}{a_2} = \frac{-6 + 2i}{9 - 8i} = -\frac{7}{4} + \frac{3}{4} i = -1.75 + 0.75i, \quad \text{setzen deshalb} \quad q_1 = -2 + i$$
und bilden damit
$$a_3 = a_1 - q_1 a_2 = (9 - 8i) - (-2 + i)(-6 + 2i) = -1 + 2i.$$

- Wir berechnen
$$\frac{a_2}{a_3} = \frac{-6+2i}{-1+2i} = 2+2i, \quad \text{setzen deshalb} \quad q_2 = 2+2i$$
und bilden damit
$$a_4 = a_2 - q_2 a_3 = (-6+2i) - (2+2i)(-1+2i) = 0.$$

Wir schreiben dies nochmals auf:
$$\begin{aligned} a_0 &= q_0 a_1 + a_2, \\ a_1 &= q_1 a_2 + a_3, \\ a_2 &= q_2 a_3 + 0. \end{aligned}$$
Also ist
$$a_3 = -1+2i$$
ein ggT der Zahlen $2+11i$ und $9-8i$. (Assoziiert zu $-1+2i$ sind die Zahlen $-1+2i$, $1-2i$, $2+i$, $-2-i$.)

Bemerkung: Kennt man für einen euklidischen Ring eine passende Division mit Rest, so kann man ggTs mit dem euklidischen Algorithmus berechnen. Wir haben für $\mathbb{Z}[i]$ dazu eine Python-Funktion geschrieben:

```
# Eine Zahl a aus Z[i] ist als Paar a=(a0,a1) mit a=a0+a1*i einzugeben.
def div_rest(a,b):
  a0,a1=a
  b0,b1=b
  z0,z1,n=a0*b0+a1*b1,a1*b0-a0*b1,b0**2+b1**2
  q0,q1=(2*z0+n)//(2*n),(2*z1+n)//(2*n)
  r0,r1=a0-q0*b0+q1*b1,a1-q0*b1-q1*b0
  return (r0,r1)

def ggT_Zi(a,b):
  while b!=(0,0):
    a,b=b,div_rest(a,b)
  return a
```

Auch der erweiterte euklidische Algorithmus überträgt sich auf allgemeine euklidische Ringe:

Satz (Erweiterter euklidischer Algorithmus). *Sei R ein euklidischer Ring mit einer euklidischen Bewertungsfunktion $\nu : R \to \mathbb{N}_0$.*

- *Es sei ein Verfahren bekannt, wie man zu $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ bestimmt mit*
$$a = qb + r \text{ und } \nu(r) < \nu(b).$$

Seien $a, b \in R$. Man definiert rekursiv Folgen $q_i, a_i, x_i, y_i \in R$ durch folgende Vorschrift:

- *$a_0 = a$, $a_1 = b$, $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$.*
- *Sind $a_i, a_{i+1}, x_i, x_{i+1}, y_i, y_{i+1}$ bereits definiert, so unterscheidet man:*
  - *Ist $a_{i+1} = 0$, so endet die Konstruktion.*
  - *Ist $a_{i+1} \neq 0$, so dividiert man a_i durch a_{i+1} und erhält einen Quotienten q_i und einen Rest a_{i+2} mit*
  $$a_i = q_i a_{i+1} + a_{i+2} \text{ mit } \nu(a_{i+2}) < \nu(a_{i+1}).$$
  Damit definiert man
  $$x_{i+2} = x_i - q_i x_{i+1} \quad \text{und} \quad y_{i+2} = y_i - q_i y_{i+1}.$$

Dann gilt
$$a_i = x_i a + y_i b \text{ für } 0 \leq i \leq n+1,$$
und a_n ist ein größter gemeinsamer Teiler von a und b mit
$$a_n = x_n a + y_n b.$$

Beweis: Dass a_n ein größter gemeinsamer Teiler ist, haben wir schon beim euklidischen Algorithmus bewiesen. Wir zeigen durch Induktion, dass

$$a_i = x_i a + y_i b \text{ für } i = 0, \dots, n+1$$

gilt. Für $i = 0$ und $i = 1$ folgt dies aus der Definition von x_0, y_0, x_1, y_1. Ist nun $i \geq 0$ und die Aussage bereits für i und $i+1$ gezeigt, also

$$\begin{aligned} a_i &= x_i a + y_i b, \\ a_{i+1} &= x_{i+1} a + y_{i+1} b, \end{aligned}$$

so folgt sofort

$$\begin{aligned} x_{i+2} a + y_{i+2} b &= (x_i - q_i x_{i+1}) a + (y_i - q_i y_{i+1}) b = \\ &= (a x_i + y_i b) - q_i (x_{i+1} a + y_{i+1} b) = a_i - q_i a_{i+1} = a_{i+2}, \end{aligned}$$

also die Behauptung. ■

Wir geben noch ein paar wichtige theoretische Anwendungen.

Satz. *In einem euklidischen Ring R ist jedes Ideal ein Hauptideal.*

Beweis: Sei R euklidisch bzgl. der Funktion $\nu : R \to \mathbb{N}_0$. Sei $\mathfrak{a}$ ein Ideal in R. Ist $\mathfrak{a} = \{0\} = (0)$, so ist $\mathfrak{a}$ ein Hauptideal. Sei nun $\mathfrak{a} \neq \{0\}$. Dann wählen wir $a \in \mathfrak{a} \setminus \{0\}$ mit

$$\nu(a) = \min\{\nu(x) : x \in \mathfrak{a} \setminus \{0\}\}.$$

Natürlich gilt $(a) \subseteq \mathfrak{a}$. Sei nun $x \in \mathfrak{a}$. Wir „dividieren x durch a" und erhalten dann $q, r \in R$ mit

$$x = qa + r \text{ mit } \nu(r) < \nu(a).$$

Mit $x, a \in \mathfrak{a}$ gilt auch $r \in \mathfrak{a}$. Nach Wahl von a folgt wegen $\nu(r) < \nu(a)$ sofort $r = 0$, und damit $x = qa \in (a)$, also $\mathfrak{a} \subseteq (a)$. Insgesamt ergibt sich $\mathfrak{a} = (a)$. Also ist $\mathfrak{a}$ Hauptideal. ■

Bemerkung: Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom vom Grad ≥ 1. Ist $g \in K[x]$ mit $f \nmid g$. Da f irreduzibel ist, ist 1 ein ggT von f und g, man findet mit dem erweiterten euklidischen Algorithmus Polynome $a, b \in K[x]$ mit

$$af + bg = 1.$$

Dann ist $bg \equiv 1 \bmod (f)$, also $\overline{b} \cdot \overline{g} = 1$ in $K[x]/(f)$. Mit dem erweiterten euklidischen Algorithmus kann man also inverse Elemente in $K[x]/(f)$ berechnen.

Bemerkung: Sei R ein euklidischer Ring mit einer euklidischen Bewertungsfunktion $\nu : R \to \mathbb{N}_0$.

(1) Man kann ν leicht abändern, da es nur auf den Größenvergleich von Elementen ankommt. Beispielsweise ist auch ν' mit $\nu'(a) = \nu(a) + 1$ eine euklidische Bewertungsfunktion für R.

(2) Definiert man

$$\widetilde{\nu}(a) = \min\{\nu(b) : b \sim a\},$$

so ist $\widetilde{\nu}$ eine euklidische Bewertungsfunktion für R, wobei assoziierte Elemente den gleichen $\widetilde{\nu}$-Wert haben. (Für $\mathbb{Z}$ und $K[x]$ ist dies bereits erfüllt.)

Satz. *Sei R ein euklidischer Ring mit der Bewertungsfunktion ν. Sei*

$$\nu(R) = \{n_0, n_1, n_2, \dots\} \text{ mit } n_0 < n_1 < n_2 < \dots$$

Dann gilt:

(1) $\nu(a) = n_0 \iff a = 0$.

(2) $\nu(a) = n_1 \Longrightarrow a \in R^*$.

(3) *Ist $\nu(a) = n_2$, dann hat jede Restklasse aus $R/(a)$ einen Repräsentanten aus $R^* \cup \{0\}$. Insbesondere folgt im Fall $|R^*| < \infty$*

$$|R/(a)| \leq 1 + |R^*|.$$

Beweis:

(1) Ist $a \in R \setminus \{0\}$, so können wir 0 durch a dividieren und erhalten eine Darstellung

$$0 = qa + r \text{ mit } \nu(r) < \nu(a),$$

woraus $\nu(a) > n_0$ folgt. Also:

$$a \neq 0 \quad \Longrightarrow \quad \nu(a) > n_0.$$

Damit folgt sofort (1).

(2) Sei $a \in R$ mit $\nu(a) = n_1$. Dann ist $a \neq 0$ und wir können 1 durch a dividieren:

$$1 = qa + r \text{ mit } \nu(r) < \nu(a).$$

Es folgt $\nu(r) < n_1$, also $\nu(r) = n_0$ und damit $r = 0$. Also gilt $1 = qa$, was beweist, dass a eine Einheit ist.

(3) Sei $a \in R$ mit $\nu(a) = n_2$. Dann ist $a \neq 0$. Sei $x \in R$ beliebig. Wir dividieren x durch a und erhalten eine Darstellung

$$x = qa + r \text{ mit } \nu(r) < \nu(a).$$

Dann ist $x \equiv r \bmod (a)$ und $\nu(r) \in \{n_0, n_1\}$, also $r \in R^* \cup \{0\}$, was die Behauptung beweist. ■

Die vorangegangenen Überlegungen haben erstaunliche Konsequenzen:

Folgerung. *Ist $d \in \mathbb{Z}$ und $d \leq -4$, so ist $\mathbb{Z}[\sqrt{d}]$ kein euklidischer Ring.*

Beweis: Im Fall $d \leq -4$ gilt $\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\}$. Wir nehmen an, $\mathbb{Z}[\sqrt{d}]$ ist euklidisch mit einer euklidischen Bewertungsfunktion ν. Sei

$$\nu(\mathbb{Z}[\sqrt{d}]) = \{n_0, n_1, n_2, \dots\} \text{ mit } n_0 < n_1 < n_2 < \dots.$$

Nach eventueller Abänderung von ν können wir annehmen, dass gilt

$$\nu(a) = n_0 \iff a = 0 \quad \text{und} \quad \nu(a) = n_1 \iff a \in \{\pm 1\}.$$

Wir wählen ein $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ mit $\nu(\alpha) = n_2$. Da es nur 2 Einheiten gibt, liefert der letzte Satz

$$|\mathbb{Z}[\sqrt{d}]/(\alpha)| \leq 3.$$

Es folgt

$$a^2 + |d|b^2 = a^2 - db^2 = \mathrm{N}(\alpha) = |\mathbb{Z}[\sqrt{d}]/(\alpha)| \leq 3.$$

Wegen $|d| \geq 4$ bleibt nur die Möglichkeit $b = 0$ und $a \in \{0, \pm 1\}$, also $\alpha \in \{0, \pm 1\}$ und damit $\nu(\alpha) \in \{n_0, n_1\}$, ein Widerspruch. Die Annahme ist also falsch, d.h. $\mathbb{Z}[\sqrt{d}]$ ist kein euklidischer Ring. ■

Bemerkungen:

(1) Auch $\mathbb{Z}[\sqrt{-2}]$ ist ein euklidischer Ring. Sind $a, b \in \mathbb{Z}[\sqrt{-2}]$ mit $b \neq 0$, ist

$$\frac{a}{b} = u + v\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}],$$

setzt man

$$q = \lfloor u \rceil + \lfloor v \rceil \sqrt{-2} \quad \text{und} \quad r = a - qb,$$

so gilt

$$a = qb + r \quad \text{und} \quad \mathrm{N}(r) < \mathrm{N}(b).$$

Der Beweis funktioniert genau wie für den Ring $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$.

(2) Auch die Ringe

$$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}], \quad \mathbb{Z}[\frac{1+\sqrt{-7}}{2}], \quad \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$$

sind euklidisch bezüglich der Normfunktion.

5. Hauptidealringe

Definition. *Ein Integritätsring R heißt* **Hauptidealring**, *wenn jedes Ideal von R ein Hauptideal ist.*

Beispiele:

(1) $\mathbb{Z}$ ist ein Hauptidealring, denn die Ideale von $\mathbb{Z}$ sind genau
$$(n) = \mathbb{Z}\, n = \{kn : k \in \mathbb{Z}\} \text{ für } n \in \mathbb{N}_0.$$
(2) Jeder euklidische Ring ist ein Hauptidealring, wie wir im letzten Abschnitt gezeigt haben.
(3) Ist K ein Körper, so ist $K[x]$ ein Hauptidealring, da $K[x]$ sogar euklidisch ist.
(4) $\mathbb{Z}[x]$ ist kein Hauptidealring, denn beispielsweise ist $(2, x)$ kein Hauptideal, wie wir bereits gesehen haben.

Bemerkung: Nicht jeder Hauptidealring ist ein euklidischer Ring. Beispielsweise ist $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ ein Hauptidealring, aber kein euklidischer Ring. (Dies ist nicht offensichtlich.)

Satz. *Sei R ein Hauptidealring und seien $a, b \in R$. Dann existieren ggT und kgV von a und b und es gilt:*

(1) *Ist $d \in R$ mit $(a) + (b) = (d)$, so ist d ein ggT von a und b.*
(2) *Ist $e \in R$ mit $(a) \cap (b) = (e)$, so ist e ein kgV von a und b.*
(3) *$ab \sim de$.*

Beweis:

- Aus $(a) + (b) = (d)$ folgt $(a) \subseteq (d)$ und $(b) \subseteq (d)$, also $d \mid a$ und $d \mid b$. Sei nun d' ein gemeinsamer Teiler von a und b, d.h. $d' \mid a$ und $d' \mid b$. Dann gilt $a \in (d')$ und $b \in (d')$, also $(a) + (b) = (a, b) \subseteq (d')$, und damit $(d) \subseteq (d')$. Dies impliziert $d' \mid d$. Nach Definition ist daher d ein ggT von a und b.
- Aus $(a) \cap (b) = (e)$ folgt $(e) \in (a)$ und $(e) \in (b)$, also $a \mid e$ und $b \mid e$. Das Element e ist also ein gemeinsames Vielfaches von a und b. Sei e' irgendein gemeinsames Vielfaches von a und b. Dann gilt $a \mid e'$ und $b \mid e'$, also $(e') \subseteq (a)$ und $(e') \subseteq (b)$, was $(e') \subseteq (a) \cap (b) = (e)$, und damit $e \mid e'$ liefert. Daher ist e ein kgV von a und b.
- Im Fall $a = 0$ ist $(b) = (d)$ und $e = 0$, also $ab = 0 = de$, und analog im Fall $b = 0$. Daher können wir im Folgenden $a, b \neq 0$ annehmen.
  - Aus $\frac{ab}{d} = a \cdot \frac{b}{d} = \frac{a}{d} \cdot b$ und $\frac{a}{d}, \frac{b}{d} \in R$ folgt
  $$a \mid \frac{ab}{d} \quad \text{und} \quad b \mid \frac{ab}{d},$$
  also ist $\frac{ab}{d}$ ein gemeinsames Vielfaches von a und b, was zu
  $$e \mid \frac{ab}{d},$$
  und damit zu $de \mid ab$ führt. Dies bedeutet
  $$(ab) \subseteq (de).$$
  - Aus $a \mid e$ und $b \mid e$ folgt $ab \mid be$ und $ab \mid ae$, also $ae, be \in (ab)$, und damit
  $$(de) = e(a, b) = (ae, be) \subseteq (ab).$$

  Insgesamt erhalten wir $(ab) = (de)$, und damit
  $$ab \sim de,$$
  wie behauptet. ■

LEMMA. *Ist R ein Hauptidealring und $a_i \in R$ eine Folge von Elementen aus R mit*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq (a_i) \subseteq (a_{i+1}) \subseteq \ldots,$$

so gibt es einen Index n mit

$$(a_n) = (a_{n+1}) = (a_{n+2}) = (a_{n+3}) = \ldots,$$

d.h. die Idealfolge (a_i) wird irgendwann stationär.

Beweis:

- Wir bilden
$$\mathfrak{a} = \bigcup_{i\geq 1}(a_i) = \bigcup_{i\geq 1} R\, a_i.$$
Wir zeigen, dass $\mathfrak{a}$ ein Ideal in R ist.
  - *Behauptung:* $0 \in \mathfrak{a}$.
  Dies folgt sofort aus $0 \in (a_1) \subseteq \mathfrak{a}$.
  - *Behauptung:* $a, a' \in \mathfrak{a} \Longrightarrow a + a' \in \mathfrak{a}$.
  Sind $a, a' \in \mathfrak{a}$, so gibt es Indizes i, j mit $a \in (a_i)$ und $a' \in (a_j)$. O.E. können wir $i \leq j$ annehmen. Wegen $(a_i) \subseteq (a_j)$ gilt dann $a, a' \in (a_j)$, woraus sofort $a + a' \in (a_j)$, und damit $a + a' \in \mathfrak{a}$ folgt.
  - *Behauptung:* $r \in R, a \in \mathfrak{a} \Longrightarrow ra \in \mathfrak{a}$.
  Sei $r \in R$ und $a \in \mathfrak{a}$. Dann gibt es einen Index i mit $a \in (a_i)$. Da (a_i) ein Ideal ist, gilt $ra \in (a_i)$, und damit auch $ra \in \mathfrak{a}$.
- Da R ein Hauptidealring ist, gibt es ein $\widetilde{a} \in R$ mit
$$\mathfrak{a} = (\widetilde{a}),$$
woraus insbesondere
$$(a_i) \subseteq (\widetilde{a}) \text{ für alle } i \geq 1$$
folgt. Wegen $\widetilde{a} \in \mathfrak{a} = \bigcup_{i\geq 1}(a_i)$ gibt es einen Index n mit $\widetilde{a} \subseteq (a_n)$. Dann ist $(\widetilde{a}) \subseteq (a_n)$ und wir erhalten
$$(a_i) \subseteq (\widetilde{a}) \subseteq (a_n) \text{ für alle } i \geq 1.$$
Wegen $(a_n) \subseteq (a_i)$ für alle $i \geq n$ folgt dann aus $(a_i) \subseteq (a_n) \subseteq (a_i)$ (für $i \geq n$) sofort
$$(a_n) = (a_i) \text{ für alle } i \geq n,$$
was wir zeigen wollten. ■

Beispiel: In $\mathbb{Z}$ gilt: $(a) \subseteq (b) \iff b \mid a$. Daher kann man leicht Idealfolgen angeben:

$$(100) \subsetneq (50) \subsetneq (25) \subsetneq (5) \subsetneq (1) = \mathbb{Z}$$

oder

$$(100) \subseteq (20) \subsetneq (10) \subseteq (2) \subsetneq (1) = \mathbb{Z}.$$

Bemerkung: Es gibt Integritätsringe, in denen nicht jede aufsteigende Hauptidealfolge stationär wird. Ein Beispiel dafür ist der Ring

$$R = \{f \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\} = \{a_0 + \sum_{i\geq 1} a_i x^i \in \mathbb{Q}[x] : a_0 \in \mathbb{Z}, a_1, a_2, a_3, \dots \in \mathbb{Q}\}$$

der rationalen Polynome, die in 0 eine ganze Zahl als Wert annehmen. Die einzigen Einheiten sind ± 1, d.h. $R^* = \{\pm 1\}$. Eine echt aufsteigende Folge von Hauptidealen ist

$$(x) \subsetneq \left(\frac{1}{2}x\right) \subsetneq \left(\frac{1}{4}x\right) \subsetneq \left(\frac{1}{8}x\right) \subsetneq \cdots \subsetneq \left(\frac{1}{2^n}x\right) \subsetneq \ldots$$

(R ist ein Beispiel eines nichtnoetherschen Ringes.)

Lemma. *Ist R ein Hauptidealring, so lässt sich jedes Element $a \in \setminus(R^* \cup \{0\})$ als Produkt von endlich vielen irreduziblen Elementen schreiben, d.h. zu $a \in R \setminus (R^* \cup \{0\})$ existieren irreduzible Elemente $q_1, \dots, q_r \in R$ mit*

$$a = q_1 q_2 \dots q_r.$$

Beweis: Wir betrachten die Menge

$$S = \{a \in R \setminus (R^* \cup \{0\}) : a \text{ ist nicht Produkt von endlich vielen irreduziblen Elementen}\}.$$

Wir wollen zeigen, dass S die leere Menge ist.

(1) *Behauptung:* Ist $a \in S$, so gibt es ein $a' \in S$ mit $(a) \subsetneq (a')$.
Beweis: Das Element a kann nicht irreduzibel sein, da es ein S ist. Also gibt es $b, c \in R \setminus R^*$ mit $a = bc$. Dann ist $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Wären b und c Produkte von irreduziblen Elementen, so auch $a = bc$. O.E. können wir daher annehmen, dass b nicht Produkt von irreduziblen Elementen ist, d.h. $b \in S$. Setzen wir $a' = b$, so gilt also $(a) \subsetneq (a')$ und $a' \in S$.

(2) *Behauptung:* Ist $a_1 \in S$, so gibt es eine Folge a_i von Elementen $a_i \in S$ mit

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots \subsetneq (a_i) \subsetneq (a_{i+1}) \subsetneq \dots$$

Beweis: Ausgehend von a_1 konstruieren wir rekursiv eine Folge a_i mit $a_i \in S$. Ist a_i bereits definiert, so finden wir mit (1) ein $a_{i+1} \in S$ mit $(a_i) \subsetneq (a_{i+1})$.

(3) *Behauptung:* $S = \emptyset$.
Beweis: Wäre $S \neq \emptyset$, so könnten wir mit (2) eine echt aufsteigende Hauptidealfolge

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4) \subsetneq \dots$$

konstruieren. Solche Folgen existieren aber nach dem vorangegangenen Lemma in einem Hauptidealring nicht. ∎

Wir haben gesehen, dass Primelemente irreduzibel sind. In Hauptidealringen gilt auch die Umkehrung:

Satz. *Sei R ein Hauptidealring. Dann gilt für $a \in R$:*

$$a \text{ irreduzibel} \iff a \text{ prim} \iff (a) \text{ maximales Ideal.}$$

Beweis: Sei $a \in R$ irreduzibel. Dafür gab es folgende Charakterisierung mit Idealen:

$$(0) \subsetneq (a) \subsetneq R \quad \text{und} \quad \Big((a) \subseteq (b) \subseteq R \Longrightarrow (a) = (b) \text{ oder } (b) = R\Big).$$

Die erste Bedingung bedeutet $a \in R \setminus (R^* \cup \{0\})$. Da R Hauptidealring ist, bedeutet die zweite Bedingung, dass für alle Ideale $\mathfrak{a}$ die Implikation

$$(a) \subseteq \mathfrak{a} \subseteq R \implies (a) = \mathfrak{a} \text{ oder } \mathfrak{a} = R$$

gilt. Dann ist aber (a) ein maximales Ideal, insbesondere ein Primideal und damit a ein Primelement. Dass jedes Primelement auch irreduzibel ist, gilt sogar in allgemeinen Integritätsringen. ∎

Lemma. *Ist R ein Integritätsring, sind $p_1, \dots, p_r, q_1, \dots, q_s$ (nicht notwendig verschiedene) Primelement mit*

$$p_1 \dots p_r = q_1 \dots q_s,$$

so gilt $r = s$ und es gibt eine Permutation σ mit $q_i \sim p_{\sigma(i)}$ für $i = 1, \dots, r$. D.h. bis auf die Reihenfolge der Faktoren ist die Zerlegung in ein Produkt von Primelementen eindeutig.

Beweis: Wir beweisen dies durch Induktion nach r.

- **Fall $r = 1$:** Wir haben

$$p_1 = q_1 \dots q_s.$$

Da p_1 irreduzibel und die q_i keine Einheiten sind, folgt sofort $s = 1$ und $p_1 = q_1$.

- **Fall** $r \geq 2$**:** Sei
$$p_1 \dots p_r = q_1 \dots q_s.$$
Da p_1 ein Primelement ist und die linke Seite teilt, folgt aus $p_1 \mid q_1 \dots q_s$, dass p_1 einen der Faktoren teilt. Nach Umbenennen können wir o.E. $p_1 \mid q_1$ annehmen. Die Irreduzibilität liefert dann mit $q_1 = \frac{q_1}{p_1} \cdot p_1$ sofort $q_1 \sim p_1$. Sei $u = \frac{q_1}{p_1} \in R^*$. Dann folgt
$$p_2 p_3 \dots p_r = (uq_2) q_3 \dots q_s.$$
Aus der Induktionsvoraussetzung folgt $s = r$ und die Existenz einer Permutation τ mit
$$uq_2 \sim p_{\tau(2)} \quad \text{und} \quad q_i \sim p_{\tau(i)} \text{ für } i = 3, \dots, r.$$
Insgesamt erhalten wir daher
$$q_1 \sim p_2 \quad \text{und} \quad q_i \sim p_i \text{ für } i = 2, \dots, r.$$

Damit ist die Behauptung durch Induktion bewiesen. ■

Wir erhalten damit ein Analogon zum Fundamentalsatz der Arithmetik:

Satz. *Ist R ein Hauptidealring, so ist jedes Element $a \in R \setminus (R^* \cup \{0\})$ ein Produkt von irreduziblen Elementen:*
$$a = p_1 \dots p_r.$$
Diese Darstellung ist bis auf Reihenfolge und Assoziiertheit eindeutig, d.h. gilt für irreduzible Elemente $q_1, \dots, q_s$
$$a = q_1 \dots q_s,$$
so gilt $r = s$ und es gibt eine Permutation σ mit $q_i \sim p_{\sigma(i)}$ für $i = 1, \dots, r$.

Bemerkungen:

(1) Die praktische Durchführung der Zerlegung in irreduzible Elemente ist nicht immer einfach, wie schon das Beispiel der ganzen Zahlen zeigt.
(2) Die eindeutige Zerlegung in ein Produkt irreduzibler Elemente gibt es auch in anderen Ringen, die **faktorielle Ringe** genannt werden. Davon handelt der nächste Abschnitt.

6. Faktorielle Ringe

Definition. *Ein* **faktorieller Ring** *ist ein Integritätsring R, wenn folgende Bedingungen erfüllt sind:*

(1) *Jede von 0 verschiedene Nichteinheit $a \in R$, d.h. $a \in R \setminus (R^* \cup \{0\})$, ist Produkt von irreduziblen Elementen, d.h. es gibt irreduzible Elemente $p_1, \dots, p_r \in R$ mit*
$$a = p_1 \dots p_r.$$
(2) *Die Darstellung als Produkt von irreduziblen Elementen ist bis auf Reihenfolge und Assoziiertheit eindeutig, d.h. d.h. sind $q_1, \dots, q_s$ irreduzible Elemente mit*
$$p_1 \dots p_r = q_1 \dots q_s,$$
so gilt $r = s$ und es gibt eine Permutation σ der Indizes $1, \dots, r$ mit
$$q_i \sim p_{\sigma(i)}.$$

Damit können wir einen Satz des vorangegangenen Abschnitts auch so formulieren:

Satz. *Jeder Hauptidealring ist ein faktorieller Ring.*

Beispiele: Die für uns wichtigsten Beispiele von Hauptidealringen sind euklidische Ringe. Damit ist klar, dass die euklidischen Ringe

- $\mathbb{Z}$,
- $\mathbb{Z}[i]$,
- $K[x]$ für einen Körper K

faktorielle Ringe sind.

Bemerkung: In $\mathbb{Z}$ ist (beispielsweise)

$$-75 = 3 \cdot 5 \cdot (-5).$$

Es ist sinnvoll, assoziierte Elemente zusammenzufassen:

$$-75 = (-1) \cdot 3 \cdot 5^2.$$

Dies wird auch im Folgenden so gehandhabt.

Unmittelbar aus der Definition erhält man folgende Darstellung:

SATZ. *Sei R ein faktorieller Ring und P ein Repräsentantensystem der irreduziblen Elemente von R modulo Assoziiertheit. Dann hat jedes Element $a \in R \setminus \{0\}$ eine eindeutige Darstellung*

$$a = u \prod_{p \in P} p^{a_p} \quad \text{mit} \quad u \in R^*, \quad a_p \in \mathbb{N}_0, \quad |\{p \in P : a_p > 0\}| < \infty.$$

Man schreibt

$$v_p(a) = a_p$$

und nennt $v_p(a)$ die **p-adische Bewertung**.

Bemerkungen und Beispiele:

(1) In $\mathbb{Z}$ sind die irreduziblen Elemente die Primzahlen p und das Negative davon $-p$. Nur ± 1 sind Einheiten. Als Repräsentantensystem der irreduziblen Elemente modulo Assoziiertheit wählt man üblicherweise die Primzahlen, also

$$P = \{p : p \text{ ist Primzahl}\} = \{2, 3, 5, 7, 11, 13, \dots\}.$$

Jede ganze Zahl $n \in \mathbb{Z} \setminus \{0\}$ schreibt sich dann eindeutig in der Form

$$n = \varepsilon \cdot \prod_{p \in P} p^{v_p(n)} \text{ mit } \varepsilon \in \{\pm 1\}.$$

(2) Im Polynomring $K[x]$ über einem Körper sind die Einheiten die Konstanten $\neq 0$. Ist $f \in K[x]$ mit $\operatorname{grad}(f) = n \geq 1$, also

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

so ist

$$f \sim x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}.$$

Als Repräsentantensystem der irreduziblen Elemente modulo Assoziiertheit kann man daher die Menge der normierter irreduziblen Polynome wählen:

$$P = \{f \in K[x] : f \text{ ist irreduzibel und normiert}\}.$$

Beispielsweise ergibt sich in $\mathbb{Q}[x]$

$$8x^3 - 4x^2 - 2x + 1 = 8 \cdot (x + \frac{1}{2}) \cdot (x - \frac{1}{2})^2.$$

Die im folgenden Satz erwähnten Eigenschaften haben wir alle schon für den Ring $\mathbb{Z}$ kennengelernt.

SATZ. *Sei R ein faktorieller Ring und P ein Repräsentantensystem der irreduziblen Elemente von R modulo Assoziiertheit. Dann gilt:*

(1) *Jedes irreduzible Element ist prim.*
(2) *Die Teilbarkeit lässt sich so charakterisieren:*

$$u_a \prod_{p \in P} p^{a_p} \mid u_b \prod_{p \in P} p^{b_p} \quad \Longleftrightarrow \quad a_p \leq b_p \text{ für alle } p \in P.$$

(3) *ggT und kgV existieren in R: Ist*

$$a = u_a \prod_{p \in P} p^{a_p} \quad \textit{und} \quad b = u_b \prod_{p \in P} p^{b_p},$$

so ist

$$\prod_{p \in P} p^{\min(a_p, b_p)}$$

ein ggT von a und b und

$$\prod_{p \in P} p^{\max(a_p, b_p)}$$

ein kgV von a und b. Bei festgewähltem Repräsentantensystem P kann man auch definieren

$$\mathrm{ggT}(a,b) = \prod_{p \in P} p^{\min(a_p, b_p)} \quad \textit{und} \quad \mathrm{kgV}(a,b) = \prod_{p \in P} p^{\max(a_p, b_p)}.$$

Es gilt dann

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) \sim ab.$$

Ist a oder b Null, so kann man die vorangegangenen Formeln nicht anwenden. Es gilt aber:
- *Für $a \in R$ ist a ein ggT von a und 0.*
- *Für $a \in R$ ist 0 ein kgV von a und 0.*

Beweis:

(1) Sei $r \in R$ irreduzibel. O.E. können wir $r \in P$ annehmen. Seien $a, b \in R$ mit $r \mid ab$. Natürlich können wir $a \neq 0$, $b \neq 0$ annehmen, da sonst alles klar ist. Wir schreiben

$$a = u_a \prod_{p \in P} p^{a_p}, \quad b = u_b \prod_{p \in P} p^{b_p}.$$

Aus $r \mid ab$ folgt dann

$$rc = ab \text{ mit } c = u_c \prod_{p \in P} p^{c_p}.$$

Dann ist

$$r^{1+c_r} \cdot \prod_{p \neq r} p^{c_p} = r^{a_r + b_r} \cdot \prod_{p \neq r} p^{a_p + b_p},$$

woraus

$$1 \leq a_r + b_r$$

folgt. Also gilt o.E. $a_r \geq 1$. Damit gilt $r \mid a$. Also ist r ein Primelement.

(2) Dies beweist man genau wie in $\mathbb{Z}$.

(3) Dies folgt (wie in $\mathbb{Z}$) unmittelbar aus (2). ■

Bemerkung: Da in einem faktoriellen Ring jedes irreduzible Element auch prim ist, kann man statt „Repräsentantensystem der irreduziblen Elemente von R modulo Assoziiertheit“ auch sagen „Repräsentantensystem der Primelemente von R modulo Assoziiertheit“.

Beispiel: Im Ring $\mathbb{Z}[\sqrt{-3}]$ ist das Element 2 irreduzibel, aber aus

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

sieht man schnell, dass 2 kein Primelement ist. Daher ist $\mathbb{Z}[\sqrt{-3}]$ kein faktorieller Ring.

Wie in $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$ erhält man auch für den Quotientenkörper eines faktoriellen Rings eine eindeutige Primfaktorzerlegung:

Satz. *Sei R ein faktorieller Ring mit Quotientenkörper K. Sei P ein Repräsentantensystem der irreduziblen Elemente von R. Dann besitzt jedes $a \in K \setminus \{0\}$ eine eindeutige Darstellung*

$$a = u \prod_{p \in P} p^{a_p} \qquad \textit{mit} \qquad u \in R^*, \quad a_p \in \mathbb{Z}, \quad |\{p \in P : a_p \neq 0\}| < \infty.$$

Man schreibt

$$v_p(a) = a_p$$

und nennt $v_p(a)$ die p-adische Bewertung von a.

Beispiel: In $\mathbb{Q}$ gilt

$$-\frac{35}{12} = (-1) \cdot 2^{-2} \cdot 3^{-1} \cdot 5^1 \cdot 7^1,$$

also ist

$$v_2(\frac{-35}{12}) = -2, \quad v_3(\frac{-35}{12}) = -1, \quad v_5(\frac{-35}{12}) = 1, \quad v_7(\frac{-35}{12}) = 1, \quad v_p(\frac{-35}{12}) = 0 \text{ für } p > 7.$$

Es gibt eine Reihe von Charakterisierungen faktorieller Ringe. Wir erwähnen zwei davon in den nachfolgenden Sätzen:

Satz. *Sei R ein Integritätsring und $P \subseteq R$ eine Teilmenge, sodass sich jedes $a \in R \setminus \{0\}$ eindeutig schreiben lässt als*

$$a = u \cdot \prod_{p \in P} p^{a_p} \qquad \textit{mit} \qquad u \in R^*, \quad a_p \in \mathbb{N}_0, \quad |\{p \in P : a_p > 0\}| < \infty.$$

Dann ist R ein faktorieller Ring.

Eine weitere Charakterisierung enthält folgender Satz:

Satz. *Ein Integritätsring R ist genau dann faktoriell, wenn folgende beiden Bedingungen erfüllt sind:*

(1) *Sind a_i in R mit*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq (a_4) \subseteq \ldots,$$

so gibt es einen Index n mit

$$(a_n) = (a_{n+1}) = (a_{n+1}) = \ldots,$$

d.h. jede aufsteigende Folge von Hauptidealen wird irgendwann stationär.

(2) *Jedes irreduzible Element ist ein Primelement.*

7. Polynome über faktoriellen Ringen

Wir beginnen zur Motivation mit einem Beispiel:

Beispiel: Wir betrachten in $\mathbb{Q}[x]$ das Polynom

$$f = \frac{4}{5}x^4 + \frac{20}{3}x + \frac{8}{7}.$$

Ein gemeinsamer Nenner ist $3 \cdot 5 \cdot 7 = 105$. Wenn wir diesen ausklammern, erhalten wir

$$f = \frac{1}{105}\left(84x^4 + 700x + 120\right) \qquad \text{mit} \qquad 84x^4 + 700x + 120 \in \mathbb{Z}[x].$$

Nun ist $\mathrm{ggT}(84, 700, 120) = 4$, also klammern wir auch noch 4 aus:

$$f = \frac{4}{105}\left(21x^4 + 175x + 30\right).$$

Dabei gilt jetzt

$$21x^4 + 175x + 30 \in \mathbb{Z}[x] \qquad \text{mit} \qquad \mathrm{ggT}(21, 175, 30) = 1.$$

Ähnliche Zerlegungen wollen wir für Polynome über faktoriellen Ringen betrachten.

DEFINITION. *Sei R ein faktorieller Ring mit Quotientenkörper K und p ein Primelement in R. Für*

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x] \setminus \{0\}$$

definieren wir

$$v_p(f) = \min(v_p(a_0), v_p(a_1), \ldots, v_p(a_n)).$$

Beispiel: Für

$$f = \frac{4}{5}x^4 + \frac{20}{3}x + \frac{8}{7} \in \mathbb{Q}[x]$$

gilt

$$v_2(f) = 2, \quad v_3(f) = -1, \quad v_5(f) = -1, \quad v_7(f) = -1, \quad v_p(f) = 0 \text{ für alle Primzahlen } p \neq 2, 3, 5, 7.$$

Bemerkungen: Sei R ein faktorieller Ring mit Quotientenkörper K.

(1) Ist p ein Primelement in R und sind $c \in K \setminus \{0\}$ und $f \in K[x] \setminus \{0\}$, so gilt
$$v_p(cf) = v_p(c) + v_p(f).$$
(2) Für $a \in K \setminus \{0\}$ gibt es (bis auf Assoziiertheit) nur endliche viele Primelemente p mit $v_p(a) \neq 0$. Daher gibt es für ein $f \in K[x] \setminus \{0\}$ (bis auf Assoziiertheit) auch nur endlich viele Primelemente p mit $v_p(f) \neq 0$. Dies benötigen wir in der folgenden Definition.

DEFINITION. *Sei R ein Integritätsring mit Quotientenkörper K und P ein Repräsentantensystem der Primelemente modulo Assoziiertheit. Für $f \in K[x] \setminus \{0\}$ definieren wir den* **Inhalt** *$I(f)$ durch*

$$I(f) = \prod_{p \in P} p^{v_p(f)}.$$

(Wählt man statt P ein anderes Repräsentantensystem der Primelemente, so ändert sich $I(f)$ um eine Einheit.)

Beispiel: Für obiges Polynom

$$f = \frac{4}{5}x^4 + \frac{20}{3}x + \frac{8}{7} \in \mathbb{Q}[x]$$

gilt

$$I(f) = \frac{4}{105} \quad \text{und} \quad f = I(f) \cdot (21x^4 + 175x + 30).$$

Bemerkung: Ist R ein faktorieller Ring mit Quotientenkörper K und P ein Repräsentantensystem der Primideale modulo Assoziiertheit, dann gilt für $c \in K \setminus \{0\}$ und $f \in K[x] \setminus \{0\}$

$$I(cf) = I(c)I(f) \quad \text{und} \quad I(c) \sim c.$$

DEFINITION. *Ist R ein faktorieller Ring, dann heißt ein Polynom*

$$f = a_0 + a_1x + \cdots + a_nx^n \in R[x] \setminus \{0\}$$

primitiv*, wenn*

$$\mathrm{ggT}(a_0, a_1, \ldots, a_n) \sim 1$$

gilt.

LEMMA. *Sei R ein faktorieller Ring mit Quotientenkörper K und P ein Repräsentantensystem der Primelemente.*

(1) *Für $f \in K[x] \setminus \{0\}$ gilt: $f \in R[x] \iff I(f) \in R$.*
(2) *Ein Polynom $f \in K[x] \setminus \{0\}$ ist genau dann primitiv, wenn $I(f) = 1$ gilt.*

(3) *Definiert man für ein Polynom* $f \in K[x] \setminus \{0\}$

$$f^* = \frac{1}{I(f)} \cdot f \in K[x] \setminus \{0\},$$

so ist $f^* \in R[x]$ *primitiv und es gilt*

$$f = I(f) \cdot f^*.$$

Beweis:

(1) Die Richtung $\Longrightarrow$ ist klar. Sei umgekehrt $I(f) \in R$. Dann gilt $v_p(f) \geq 0$ für alle $p \in R$. Schreibt man $f = a_0 + a_1 x + \cdots + a_n x^n$, so folgt $v_p(a_i) \geq 0$ für alle i und alle $p \in P$. Dann gilt aber $a_i \in R$ für alle i, und damit $f \in R[x]$.

(2)
- Ist $f \in K[x] \setminus \{0\}$ primitiv, so ist $f \in R[x]$, also

  $$f = a_0 + a_1 x + \cdots + a_n x^n \text{ mit } a_i \in R.$$

  Dann ist $v_p(f) \geq 0$. Wegen $\mathrm{ggT}(a_0, a_1, \ldots, a_n) = 1$ gibt es für jedes Primelement p einen Index i mit $v_p(a_i) = 0$, woraus dann $v_p(f) = 0$ folgt. Damit erhält man $I(f) = 1$.
- Sei umgekehrt $I(f) = 1$. Dann gilt $v_p(f) = 0$ für alle $p \in P$. Es folgt $v_p(a_i) \geq 0$ für alle i und p, woraus $a_i \in R$ folgt. Aus $v_p(f) = 0$ folgt dann $p \nmid \mathrm{ggT}(a_0, a_1, \ldots, a_n)$, woraus schließlich $\mathrm{ggT}(a_0, a_1, \ldots, a_n) = 1$ folgt. Also ist f primitiv.

(3) Es ist

$$I(f^*) = I(\frac{1}{I(f)} \cdot f) = I(\frac{1}{I(f)}) \cdot I(f) = \frac{1}{I(f)} \cdot I(f) = 1,$$

also ist f^* primitiv. Der Rest ist klar. ■

Satz (Lemma von Gauß). *Sei R ein faktorieller Ring mit Quotientenkörper K und P ein Repräsentantensystem der Primelemente von R modulo Assoziiertheit. Für Polynome $f, g \in K[x] \setminus \{0\}$ gilt dann*

$$I(fg) = I(f)I(g).$$

Insbesondere ist das Produkt primitiver Elemente wieder primitiv.

Beweis:

(1) Seien $f^*, g^* \in R[x] \setminus \{0\}$ primitive Polynome. Sei

$$f^* g^* = c_0 + c_1 x + \cdots + c_n x^n \in R[x].$$

- Sei p ein Primelement in R. Dann ist mit $R/(p)$ auch $(R/(p))[x]$ ein Integritätsring. Wir betrachten den Reduktionshomomorphismus

  $$\phi : R[x] \to (R/(p))[x], \quad \sum_{i \geq 0} a_i x^i \mapsto \sum_{i \geq 0} \overline{a_i} x^i.$$

  Da $f*$ und $g*$ primitiv sind, sind nicht alle Koeffizienten von f^* und g^* durch p teilbar, also ist

  $$\phi(f^*) \neq 0 \quad \text{und} \quad \phi(g^*) \neq 0.$$

  Daher ist auch

  $$\phi(f^* g^*) = \phi(f^*)\phi(g^*) \neq 0.$$

  Das bedeutet, dass nicht alle Koeffizienten von $f^* g^*$ durch p teilbar sind: Es gibt einen Index i mit $p \nmid c_i$. Dies impliziert

  $$v_p(f^* g^*) = 0.$$

- Da die vorangegangene Beobachtung für alle Primelemente von R gilt, folgt

  $$I(f^* g^*) = 1,$$

  d.h. $f^* g^*$ ist primitiv.

(2) Wir zerlegen

$$f = I(f) \cdot f^* \quad \text{und} \quad g = I(g) \cdot g^*.$$

Dann sind f^* und g^* primitiv. Nach (1) ist auch f^*g^* primitiv, d.h. $I(f^*g^*) = 1$. Es folgt

$$I(fg) = I(I(f) \cdot f^* \cdot I(g) \cdot g^*) = I(f)I(g)I(f^*g^*) = I(f)I(g),$$

was zu zeigen war. ■

Beispiel: Über $\mathbb{Z}$ (mit Quotientenkörper $\mathbb{Q}$) betrachten wir

$$f = \frac{1}{2}x^2 + \frac{2}{3}x + \frac{3}{4} \quad \text{und} \quad g = \frac{4}{5}x + \frac{5}{4}.$$

Es ist

$$f = \frac{1}{12}\left(6x^2 + 8x + 9\right) \quad \text{und} \quad g = \frac{1}{20}\left(16x + 25\right).$$

Für das Produkt gilt

$$fg = \frac{2}{5}x^3 + \frac{139}{120}x^2 + \frac{43}{30}x + \frac{15}{16} = \frac{1}{240}\left(96x^3 + 278x^2 + 344x + 225\right).$$

Es ist

$$I(fg) = \frac{1}{240} = \frac{1}{12} \cdot \frac{1}{20} = I(f) \cdot I(g).$$

Folgerung. *Sei R ein faktorieller Ring mit Quotientenkörper K und P ein Repräsentantensystem der Primelemente modulo Assoziiertheit. Ist $f \in R[x] \setminus \{0\}$ und sind $g, h \in K[x]$ mit*

$$f = gh.$$

Zerlegen wir

$$f = I(f) \cdot f^*, \quad g = I(g) \cdot g^*, \quad h = I(h) \cdot h^*$$

mit primitiven Polynomen f^*, g^*, h^*, so gilt

$$f^* = g^*h^* \quad \textit{und} \quad f = I(f) \cdot g^* \cdot h^*.$$

Lemma. *Sei R ein faktorieller Ring mit Quotientenkörper K.*

(1) *Ein Element $p \in R$ ist genau dann irreduzibel in $R[x]$, wenn p irreduzibel in R ist.*
(2) *Ein Polynom $f \in R[x] \setminus \{0\}$ vom Grad ≥ 1 ist genau dann irreduzibel in $R[x]$, wenn f primitiv und irreduzibel in $K[x]$ ist.*

Beweis: Wir wählen ein Repräsentantensystems P der Primelemente von R modulo Assoziiertheit. Wir wissen, dass die Einheiten von $R[x]$ genau die Einheiten von R sind.

(1) Hat $p \in R\setminus\{0\}$ eine Zerlegung $p = ab$ mit $a, b \in R[x]$, so folgt aus $0 = \text{grad}(p) = \text{grad}(a) + \text{grad}(b)$ sofort $a, b \in R$. Wegen $R[x]^* = R^*$ folgt damit sofort die Behauptung.
(2)
- $\Longrightarrow$ Sei f irreduzibel in $R[x]$. In $R[x]$ gilt dann die Zerlegung

$$f = I(f) \cdot f^* \text{ mit } \text{grad}(f^*) = \text{grad}(f) \geq 1.$$

Die Zerlegung $f = I(f) \cdot f^*$ muss trivial sein, d.h. $I(f) = 1$, f ist also primitiv. Seien nun $g, h \in K[x]$ mit $f = gh$. Dann folgt mit den Bezeichnungen der vorangegangenen Folgerung, also $g = I(g) \cdot g^*$, $h = I(h) \cdot h^*$

$$f = I(f) \cdot g^* \cdot h^* = g^* \cdot h^*.$$

$f = g^* \cdot h^*$ ist eine Zerlegung in $R[x]$, die daher trivial sein muss, d.h. g^* oder h^* ist eine Einheit in R. Dann ist aber g oder h konstant, was zeigt, dass f irreduzibel in $K[x]$ ist.

- $\Longleftarrow$ Sei nun $f \in R[x]$ primitiv und irreduzibel in $K[x]$. Wir setzen an $f = gh$ mit $g, h \in R[x]$. Aus $I(f) = 1$ und $I(f) = I(g)I(h)$ folgt $I(g) = I(h) = 1$, und damit
$$f = g^* \cdot h^*,$$
wobei wir die Zerlegungen $g = I(g) \cdot g^*$ und $h = I(h) \cdot h^*$ benutzt haben. Da f in $K[x]$ irreduzibel ist, ist g^* oder h^* konstant. Die Primitivität von g^* und h^* impliziert dann $g^* \in R^*$ oder $h^* \in R^*$. Daher ist f irreduzibel in $R[x]$. ■

Bemerkung: Sei R ein faktorieller Ring mit Quotientenkörper K und P ein Repräsentantensystem der Primelemente modulo Assoziiertheit. $K[x]$ ist ein euklidischer Ring und damit faktoriell. Sei Q ein Repräsentantensystem der irreduziblen Polynome in $K[x]$ modulo Konstanten. Zerlegen wir $q \in Q$
$$q = I(q) \cdot q^*,$$
so können wir in Q das Polynom durch q^* ersetzen. Damit können wir erreichen, dass alle Polynome in Q aus $R[x]$ und primitiv sind, insbesondere sind sie dann auch irreduzibel in $R[x]$. Dies benutzen wir nun:

SATZ. *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann ist auch der Polynomring $R[x]$ ein faktorieller Ring. Genauer:*

- *Sei $P \subseteq R$ ein Repräsentantensystem der Primelemente von R modulo Assoziiertheit.*
- *Sei $Q \subseteq K[x]$ ein Repräsentantensystem der irreduziblen Polynome von $K[x]$ modulo Konstanten. Q kann so gewählt werden, dass jedes $q(x) \in Q$ ein primitives Polynom aus $R[x]$ ist. (Dann ist $q(x)$ in $R[x]$ irreduzibel.)*

Dann hat jedes $f \in R[x] \setminus \{0\}$ eine eindeutige Darstellung
$$f(x) = u \cdot \prod_{p \in P} p^{d_p} \cdot \prod_{q(x) \in Q} q(x)^{e_q} \quad \textit{mit} \quad d_p, e_q \in \mathbb{N}_0 \quad \textit{und} \quad u \in R^*.$$
(Natürlich gilt $|\{p \in P : d_p \geq 1\}| < \infty$ und $|\{q \in Q : e_q \geq 1\}| < \infty$.) Die irreduziblen Elemente von $R[x]$ sind genau die Elemente, die zu einem Element aus $P \cup Q$ assoziiert sind.

Beweis:

- Nach dem vorangegangenen Lemma sind die Elemente von $P \cup Q$ irreduzibel in $R[x]$.
- Nach der Vorbemerkung können wir die Repräsentanten der irreduziblen Elemente des euklidischen Rings $K[x]$ so wählen, dass sie aus $R[x]$ und primitiv sind. Dann hat $f \in R[x] \setminus \{0\}$ eine eindeutige Zerlegung
$$f(x) = c \cdot \prod_{q \in Q} q(x)^{e_q} \quad \text{mit} \quad c \in K^*, \quad e_q \in \mathbb{N}_0, \quad |\{q \in Q : e_q > 0\}| < \infty,$$
insbesondere sind die Zahlen e_q eindeutig bestimmt.
- Warum gilt $c \in R \setminus \{0\}$? Es ist $c = I(c) \cdot c^*$, wobei c^* primitiv ist und Grad 0 hat. Also ist $c^* \in R^*$. Wir können also schreiben
$$c = I(c) \cdot u \quad \text{mit} \quad u \in R^*.$$
- Mit $I(q) = 1$ für $q \in Q$ erhalten wir
$$I(c) = I(c) \cdot \prod_{q \in Q} I(q)^{e_q} = I\left(c \cdot \prod_{q \in Q} q(x)^{e_q}\right) = I(f).$$
- Wir haben jetzt
$$f(x) = c \cdot \prod_{q \in Q} q(x)^{e_q} = u \cdot I(f) \cdot \prod_{q \in Q} q(x)^{e_q}.$$
- Wegen $f \in R[x] \setminus \{0\}$ ist $I(f) \in R$ und hat eine eindeutige Zerlegung
$$I(f) = \prod_{p \in P} p^{d_p} \quad \text{mit} \quad d_p \in \mathbb{N}_0, \quad |\{p \in P : d_p > 0\}| < \infty.$$

- Damit ergibt sich insgesamt:

$$f = u \cdot \prod_{p \in P} p^{d_p} \cdot \prod_{q \in Q} q(x)^{e_q}.$$

Die Zahlen e_q sind eindeutig bestimmt wegen der eindeutigen Primfaktorzerlegung in $K[x]$, die Zahlen d_p sind eindeutig bestimmt wegen der eindeutigen Primfaktorzerlegung von $I(f)$ in R.

- Ist $r \in R[x]$ irreduzibel, so gibt es eine Darstellung

$$r = u \cdot \prod_{p \in P} p^{d_p} \cdot \prod_{q \in Q} q^{e_q}$$

wie oben. Da r keine Einheit ist, gilt

$$\sum_{p \in P} d_p + \sum_{q \in Q} e_q \geq 1.$$

Wäre $\sum_p d_p + \sum_q e_q \geq 2$, so wäre r offensichtlich reduzibel. Also folgt

$$\sum_{p \in P} d_p + \sum_{q \in Q} e_q = 1.$$

Daher ist entweder

$$r \sim p \text{ für ein } p \in P \quad \text{oder} \quad r \sim q \text{ für ein } q \in Q.$$

Dies beweist die letzte Behauptung. ■

Bemerkungen:

(1) Da $\mathbb{Z}$ faktoriell ist, ist auch der Polynomring $\mathbb{Z}[x]$ faktoriell. Allerdings ist $\mathbb{Z}[x]$ kein Hauptidealring, wie wir bereits gesehen haben.

(2) Was bietet sich als Repräsentantensystem der irreduziblen Elemente modulo Assoziiertheit für $\mathbb{Z}[x]$ an? Für die Konstanten nehmen wir wieder die Primzahlen:

$$P = \{p : p \text{ Primzahl}\}.$$

Wegen $\mathbb{Z}[x]^* = \{\pm 1\}$ sind zwei Polynome f, g genau dann assoziiert, wenn sie sich nur ums Vorzeichen unterscheiden: $f = \pm g$. Für das Repräsentantensystem der irreduziblen Polynome wählen wir daher

$$Q = \{a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] : a_n x^n + \cdots + a_n \text{ ist irreduzibel und primitiv und } a_n \geq 1\}.$$

SAGE benutzt diese Konvention. Vereinbart man den Polynomring $\mathbb{Z}[x]$ mit `Z.<x>=ZZ[]`, so erhält man mit `factor(f)` eine Faktorisierung der obigen Art.

Beispiel: In $\mathbb{Z}[x]$ gilt folgende Primfaktorzerlegung:

$$f = -18x^6 + 24x^5 + 84x^4 - 136x^3 + 80x^2 - 124x + 80 = (-1) \cdot 2 \cdot (3x - 4) \cdot (3x^5 - 14x^3 + 4x^2 - 8x + 10).$$

Polynome in mehreren Unbestimmten: Ist R ein kommutativer Ring, so kann man den Polynomring $R[x_1, \ldots, x_n]$ in den Unbestimmten $x_1, \ldots, x_n$ rekursiv durch

$$R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$$

einführen. Damit ergibt sich dann folgendes Beispiel:

Beispiel: Ist R ein faktorieller Ring, so ist auch der Polynomring $R[x_1, \ldots, x_n]$ in den Unbestimmten $x_1, \ldots, x_n$ faktoriell.

8. Irreduzibilitätskriterien für Polynome über faktoriellen Ringen

Bemerkungen: Sei R ein faktorieller Ring mit Quotientenkörper K. Sei außerdem ein Repräsentantensystem P der Primelemente von R fest gewählt, sodass der Inhalt $I(f)$ eines Polynoms $f \in K[x] \setminus \{0\}$ wohldefiniert ist.

(1) Ist $f \in R[x] \setminus \{0\}$ und sind $g, h \in K[x]$ mit
$$f = g \cdot h,$$
so haben wir zuvor gesehen, dass gilt
$$f = I(f) \cdot g^* \cdot h^*.$$
Dabei ist $\operatorname{grad}(g) = \operatorname{grad}(g^*)$ und $\operatorname{grad}(h) = \operatorname{grad}(h^*)$. Wenn wir also die Irreduzibilität von f in $K[x]$ zeigen wollen und den Ansatz $f = gh$ mit $g, h \in K[x]$ und $\operatorname{grad}(g) \geq 1$, $\operatorname{grad}(h) \geq 1$ machen, so können wir o.E. $g, h \in R[x]$ annehmen.

(2) Wir haben zuvor gezeigt, dass für $f \in R[x]$ mit $\operatorname{grad}(f) \geq 1$ gilt:
$$f \text{ irreduzibel in } R[x] \iff f \text{ irreduzibel in } K[x] \text{ und } f \text{ primitiv}.$$
Dass man auf „primitiv“ auf der rechten Seite nicht verzichten kann, sieht man am Beispiel $f = 2x \in \mathbb{Z}[x]$: Das Polynom ist irreduzibel in $\mathbb{Q}[x]$, aber reduzibel in $\mathbb{Z}[x]$.

SATZ (Eisenstein-Kriterium). *Sei R ein faktorieller Ring mit Quotientenkörper K und $f = a_nx^n + \cdots + a_1x + a_0 \in R[x]$ ein Polynom vom Grad $n \geq 1$. Ist $p \in R$ ein Primelement mit*
$$p \nmid a_n, \quad p \mid a_{n-1}, \quad p \mid a_{n-2}, \quad \ldots \quad p \mid a_1, \quad p \mid a_0 \quad \textit{und} \quad p^2 \nmid a_0,$$
so ist f irreduzibel in $K[x]$.

Beweis: Wir nehmen an, wir haben eine Zerlegung
$$f = gh \text{ mit } g, h \in K[x] \text{ und } \operatorname{grad}(g) \geq 1, \operatorname{grad}(h) \geq 1.$$
Wie zuvor bemerkt, können wir (nach eventueller Abänderung von g und h um Konstanten) $g, h \in R[x]$ annehmen. Wir schreiben
$$g = b_kx^k + \cdots + b_1x + b_0 \quad \text{und} \quad h = c_\ell x^\ell + \cdots + c_1x + c_0.$$
Es ist
$$a_n = b_kc_\ell \quad \text{und} \quad a_0 = b_0c_0.$$
Wegen $p \mid a_0$, $p^2 \nmid a_0$ können wir o.E.
$$b_0 \not\equiv 0 \bmod p \quad \text{und} \quad c_0 \equiv 0 \bmod p$$
annehmen. Wegen $p \nmid a_n$ gilt
$$b_k \not\equiv 0 \bmod p \quad \text{und} \quad c_\ell \not\equiv 0 \bmod p.$$
Wegen $c_0 \equiv 0 \bmod p$ und $c_\ell \not\equiv 0 \bmod p$ gibt es einen Index r mit $1 \leq r \leq \ell < n$ mit
$$c_r \not\equiv 0 \bmod p, \quad c_{r-1} \equiv c_{r-2} \equiv \cdots \equiv c_1 \equiv c_0 \equiv 0 \bmod p.$$
Dann ist
$$a_r = b_0c_r + b_1c_{r-1} + b_2c_{r-2} + \cdots + b_{r-1}c_1 + b_rc_0 \equiv b_0c_r \bmod p, \quad \text{und damit} \quad a_r \not\equiv 0 \bmod p,$$
was aber wegen $r < n$ der Voraussetzung $p \mid a_r$ widerspricht. Die Annahme ist also falsch, f ist daher irreduzibel. ■

Beispiele:

(1) Ist $a \in \mathbb{Z}$ und gibt es eine Primzahl p mit $p \mid a$, aber $p^2 \nmid a$, so ist für alle $n \in \mathbb{N}$ das Polynom
$$x^n - a$$
irreduzibel über $\mathbb{Q}$.

(2) Das Polynom $3x^5 - 15$ ist irreduzibel über $\mathbb{Q}$, nicht jedoch über $\mathbb{Z}$.

Satz (Reduktionskriterium). *Sei R ein faktorieller Ring mit Quotientenkörper K, $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ vom Grad $n \geq 1$, $p \in R$ ein Primelement mit $p \nmid a_n$. Sei*

$$\overline{f} = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0} \in (R/(p))[x].$$

Ist das modulo p reduzierte Polynom $\overline{f}$ irreduzibel, so ist f über K irreduzibel. Ist zusätzlich primitiv, so ist f irreduzibel über R.

Beweis: Ist f in $K[x]$ reduzibel, so finden wir auch eine Zerlegung $f = gh$ mit $g, h \in R[x]$ mit $\mathrm{grad}(g) \geq 1$ und $\mathrm{grad}(h) \geq 1$. Wegen $p \nmid a_n$ gilt $\mathrm{grad}(f) = \mathrm{grad}(\overline{f})$, und damit auch $\mathrm{grad}(\overline{g}) = \mathrm{grad}(g)$, $\mathrm{grad}(\overline{h}) = \mathrm{grad}(h)$ und

$$\overline{f} = \overline{g} \cdot \overline{h}.$$

Dies widerspricht aber der Voraussetzung. Also ist f irreduzibel über $K[x]$. Dass aus der Irreduzibilität über K und der Primitivität dann die Irreduzibilität über R folgt, wissen wir schon. ■

Beispiel: Das Polynom $x^2 + x + 1$ ist irreduzibel über $\mathbb{F}_2$, da es keine Nullstelle in $\mathbb{F}_2$ hat. Daher ist auch jedes Polynom

$$f = ax^2 + bx + c \in \mathbb{Z}[x] \quad \text{mit } a \equiv b \equiv c \equiv 1 \bmod 2$$

über $\mathbb{Q}$ irreduzibel, wie man durch Reduktion modulo 2 sieht.

Satz (Integral Root Test). *Sei R ein faktorieller Ring mit Quotientenkörper K und*

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x] \setminus \{0\} \text{ vom Grad } n \geq 1.$$

Ist $\alpha \in K$ eine Nullstelle von f, d.h. $f(\alpha) = 0$, so gilt:

(1) *Schreibt man $\alpha = \frac{b}{c}$ mit $b, c \in R$ und $\mathrm{ggT}(b, c) \sim 1$, so gilt*

$$b \mid a_0 \quad \text{und} \quad c \mid a_n.$$

(2) *Ist f normiert, so gilt*

$$\alpha \in R \quad \text{und} \quad \alpha \mid a_0.$$

Beweis: Sei $\alpha = \frac{b}{c} \in K$ mit $b, c \in R$, $\mathrm{ggT}(b, c) \sim 1$ und $f(\frac{b}{c}) = 0$. Dann folgt $c^n f(\frac{b}{c}) = 0$, was die Gleichung

$$a_n b^n + a_{n-1} b^{n-1} c + a_{n-2} b^{n-2} c^2 + \cdots + a_1 b c^{n-1} + a_0 c^n = 0$$

liefert. Hieraus ergibt sich

$$b \mid a_0 c^n \quad \text{und} \quad c \mid a_n b^n.$$

Wegen $\mathrm{ggT}(b, c) \sim 1$ folgt

$$b \mid a_0 \quad \text{und} \quad c \mid a_n.$$

Ist $a_n = 1$, so ist $c \in R^*$ und damit $\frac{b}{c} \in R$. ■

Beispiel: Wir betrachten das Polynom

$$f = x^3 + x + 2 \in \mathbb{Z}[x].$$

Der vorangegangene Satz sagt, dass Nullstellen aus $\mathbb{Q}$ schon in $\mathbb{Z}$ liegen und Teiler von 2 sind. Also kommen nur $\pm 1, \pm 2$ als rationale Nullstellen in Frage. Nun ist

$$f(1) = 4, \quad f(-1) = 0, \quad f(2) = 12, \quad f(-2) = -8.$$

Also ist -1 eine Nullstelle von f und daher spaltet $x + 1$ ab:

$$f = (x + 1)(x^2 - x + 2).$$

Mit der gleichen Vorgehensweise findet man, dass $x^2 - x + 2$ keine Nullstelle in $\mathbb{Q}$ hat, weswegen das Polynom irreduzibel über $\mathbb{Q}$ ist. Daher ist

$$f = (x + 1)(x^2 - x + 2)$$

die Primfaktorzerlegung von f über $\mathbb{Q}$ (und $\mathbb{Z}$).

Bemerkung: Bei den vorangegangenen Überlegungen haben wir benutzt, dass im Falle eines faktoriellen Rings R (mit Quotientenkörper K) und $f \in R[x]$ mit $\operatorname{grad}(f) \geq 1$ folgende Implikation gilt:

$$f \in R[x] \text{ irreduzibel} \quad \Longrightarrow \quad g \in K[x] \text{ irreduzibel.}$$

Das folgende Beispiel zeigt, dass die Aussage für allgemeine Integritätsringe nicht erfüllt sein muss.

Beispiel: Der Integritätsring $R = \mathbb{Z}[\sqrt{-22}]$ hat den Quotientenkörper $K = \mathbb{Q}[\sqrt{-22}]$. Wir wollen zeigen, dass das Polynom

$$f = 2x^2 + 11$$

als Element von $R[x]$ irreduzibel, als Element von $K[x]$ aber reduzibel ist.

- Die Normform von $R = \mathbb{Z}[\sqrt{-22}]$ ist $\mathrm{N}(x + y\sqrt{-22}) = x^2 + 22y^2$. Die einzigen Einheiten sind ± 1. Da 2 und 11 nicht als Norm auftreten, sieht man, dass die Elemente 2 (mit Norm 2^2) und 11 (mit Norm 11^2) in R irreduzibel sind.
- Seien $g, h \in R[x]$ mit $f = gh$ und $\operatorname{grad}(g) \leq \operatorname{grad}(h)$. Aus $2 = \operatorname{grad}(f) = \operatorname{grad}(g) + \operatorname{grad}(h)$ folgt dann
$$(\operatorname{grad}(g), \operatorname{grad}(h)) \in \{(0,2), (1,1)\}.$$
Im Fall $(\operatorname{grad}(g), \operatorname{grad}(h)) = (0,2)$ gilt dann $g \in R^*$, da 2 und 11 irreduzibel in R sind. Im Fall $(\operatorname{grad}(g), \operatorname{grad}(h)) = (1,1)$ setzen wir an
$$g = ax + b \quad \text{und} \quad h = cx + d \quad \text{mit} \quad a, b, c, d \in R.$$
Aus
$$2x^2 + 11 = f = gh = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$$
erhält man durch Koeffizientenvergleich
$$ac = 2, \quad ad + bc = 0, \quad bd = 11.$$
Da 2 irreduzibel ist, muss a oder c eine Einheit sein. Nach eventueller Abänderung um eine Einheit, können wir $a = 1$, und damit $c = 2$ annehmen. Es bleiben die Gleichungen
$$d + 2b = 0, \quad bd = 11,$$
also
$$d = -2b \quad \text{und} \quad -2b^2 = 11.$$
Normbildung liefert aus $-2b^2 = 11$
$$4\mathrm{N}(b)^2 = 121.$$
Wegen $\mathrm{N}(b) \in \mathbb{N}_0$ ist aber die letzte Gleichung nicht lösbar. Daher ist $2x^2 + 11$ nicht in der Form gh zerlegbar. Dies beweist, dass $2x^2 + 11$ in $R[x]$ irreduzibel ist.
- Es gilt aber in $K[x]$:
$$\begin{aligned} 2x^2 + 11 &= \frac{1}{2}(4x^2 + 22) = \frac{1}{2}(4x^2 - \sqrt{-22}^2) = \frac{1}{2}(2x - \sqrt{-22})(2x + \sqrt{-22}) = \\ &= (x - \frac{1}{2}\sqrt{-22})(2x + \sqrt{-22}). \end{aligned}$$
$2x^2 + 11$ ist also reduzibel in $K[x]$.

9. Anhang: Ein Lemma zum Faktorring $\mathbb{Z}[\sqrt{d}]/(\alpha)$

Lemma. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$ und $\alpha \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}$. Wir schreiben*

$$\alpha = ma + mb\sqrt{d} \text{ mit } m \in \mathbb{N},\ a, b \in \mathbb{Z} \text{ und } \operatorname{ggT}(a,b) = 1.$$

Dann gilt:

(1) *Es gibt $u, v \in \mathbb{Z}$ mit*
$$ub + va(a^2 - db^2) = 1.$$
(2) *Das Hauptideal $(\alpha) = \mathbb{Z}[\sqrt{d}] \cdot \alpha$ lässt sich so schreiben:*
$$(\alpha) = \mathbb{Z}[\sqrt{d}] \cdot \alpha = \mathbb{Z} \cdot m(a^2 - db^2) + \mathbb{Z} \cdot (mau + m\sqrt{d}).$$

(3) *Die Menge*

$$R = \{r + s\sqrt{d} : 0 \le r \le |m(a^2 - db^2)| - 1,\ 0 \le s \le m - 1\}$$

bildet ein Repräsentantensystem von $\mathbb{Z}[\sqrt{d}]/(\alpha)$*, insbesondere gilt*

$$|\mathbb{Z}[\sqrt{d}]/(\alpha)| = |R| = |\mathrm{N}(\alpha)| = |m^2(a^2 - db^2)|.$$

(4) *Die Abbildung* $\rho : \mathbb{Z}[\sqrt{d}] \to R$ *mit*

$$\rho(x + y\sqrt{d}) = \big((x - \left\lfloor \frac{y}{m} \right\rfloor mau) \bmod |m(a^2 - db^2)|\big) + (y \bmod m)\sqrt{d}$$

ordnet jedem Element aus $\mathbb{Z}[\sqrt{d}]$ *seinen Repräsentanten aus* R *zu.*

Beweis:

(1) Aus $\mathrm{ggT}(a, b) = 1$ folgt $\mathrm{ggT}(b, a(a^2 - db^2)) = 1$. Mit dem erweiterten euklidischen Algorithmus findet man $u, v \in \mathbb{Z}$ mit

$$ub + va(a^2 - db^2) = 1.$$

(2) (a) Zunächst gilt

$$\begin{aligned}(\alpha) &= (ma + mb\sqrt{d}) = \{(m(a + b\sqrt{d})(x + y\sqrt{d}) : x, y \in \mathbb{Z}\} = \\ &= \{xm(a + b\sqrt{d}) + ym(db + a\sqrt{d}) : x, y \in \mathbb{Z}\} = \\ &= \mathbb{Z} \cdot m(a + b\sqrt{d}) + \mathbb{Z} \cdot m(db + a\sqrt{d}).\end{aligned}$$

(b) Wir betrachten die Matrix

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} = \begin{pmatrix} a & -b \\ u - vabd & va^2 \end{pmatrix}.$$

Es gilt

$$\det(T) = a \cdot va^2 + b \cdot (u - vabd) = ub + va(a^2 - db^2) = 1.$$

Nun ist

$$\begin{aligned}T\begin{pmatrix} a + b\sqrt{d} \\ db + a\sqrt{d} \end{pmatrix} &= \begin{pmatrix} a & -b \\ u - vabd & va^2 \end{pmatrix}\begin{pmatrix} a + b\sqrt{d} \\ bd + a\sqrt{d} \end{pmatrix} = \\ &= \begin{pmatrix} a(a + b\sqrt{d}) - b(bd + a\sqrt{d}) \\ (u - vabd)(a + b\sqrt{d}) + va^2(bd + a\sqrt{d}) \end{pmatrix} = \\ &= \begin{pmatrix} a^2 - db^2 \\ au + (ub - vab^2d + vaa^2)\sqrt{d} \end{pmatrix} = \\ &= \begin{pmatrix} a^2 - db^2 \\ au + (ub + va(a^2 - db^2))\sqrt{d} \end{pmatrix} = \\ &= \begin{pmatrix} a^2 - db^2 \\ au + \sqrt{d} \end{pmatrix}.\end{aligned}$$

Also gilt

$$a^2 - db^2 = t_{11}(a + b\sqrt{d}) + t_{12}(bd + a\sqrt{d})$$

und

$$au + \sqrt{d} = t_{21}(a + b\sqrt{d}) + t_{22}(bd + a\sqrt{d}).$$

Daher folgt

$$\mathbb{Z} \cdot (a^2 - db^2) + \mathbb{Z} \cdot (au + \sqrt{d}) \subseteq \mathbb{Z} \cdot (a + b\sqrt{d}) + \mathbb{Z} \cdot (bd + a\sqrt{d}).$$

Nun ist aber wegen $\det(T) = 1$

$$T^{-1} = \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix},$$

also folgt

$$a + b\sqrt{d} = t_{22}(a^2 - db^2) - t_{12}(au + \sqrt{d})$$

und
$$bd + a\sqrt{d} = -t_{21}(a^2 - db^2) + t_{11}(au + \sqrt{d}).$$
Dies impliziert
$$\mathbb{Z} \cdot (a + b\sqrt{d}) + \mathbb{Z} \cdot (bd + a\sqrt{d}) \subseteq \mathbb{Z} \cdot (a^2 - db^2) + \mathbb{Z} \cdot (au + \sqrt{d}).$$
Insgesamt erhalten wir
$$\mathbb{Z} \cdot (a + b\sqrt{d}) + \mathbb{Z} \cdot (bd + a\sqrt{d}) = \mathbb{Z} \cdot (a^2 - db^2) + \mathbb{Z} \cdot (au + \sqrt{d}).$$

(c) Multiplizieren wir die letzte Gleichung in (b) mit m, so ergibt sich
$$(\alpha) = \mathbb{Z} \cdot m(a^2 - db^2) + \mathbb{Z} \cdot (mau + m\sqrt{d}).$$
Dies beweist die in (2) behauptete Aussage.

(3) (a) Wie reduziert man modulo (α)? Wir starten mit $x + y\sqrt{d}$ mit $x, y \in \mathbb{Z}$. Wir dividieren y durch m und erhalten eine Zerlegung
$$y = qm + s \text{ mit } q, s \in \mathbb{Z} \text{ und } 0 \leq s \leq m - 1.$$
Dann ist
$$\begin{aligned} x + y\sqrt{d} &= x + (qm + s)\sqrt{d} = x + qm\sqrt{d} + s\sqrt{d} = \\ &= x + q(mau + m\sqrt{d}) - qmau + s\sqrt{d} = \\ &= (x - qmau) + s\sqrt{d} + q(mau + m\sqrt{d}). \end{aligned}$$
Nun dividieren wir $x - qmau$ durch $m(a^2 - db^2)$ und erhalten eine Zerlegung
$$x - qmau = tm(a^2 - db^2) + r \text{ mit } t, r \in \mathbb{Z} \text{ und } 0 \leq r \leq |m(a^2 - db^2)| - 1.$$
Damit folgt
$$\begin{aligned} x + y\sqrt{d} &= tm(a^2 - db^2) + r + s\sqrt{d} + q(mau + m\sqrt{d}) = \\ &= (r + s\sqrt{d}) + tm(a^2 - db^2) + q(mau + m\sqrt{d}), \end{aligned}$$
woraus sofort
$$x + y\sqrt{d} \equiv r + s\sqrt{d} \bmod (\alpha)$$
folgt mit
$$0 \leq r \leq |m(a^2 - db^2)| \text{ und } 0 \leq s \leq m - 1.$$
Dies zeigt, dass die angegebene Menge R ein Repräsentantensystem von $\mathbb{Z}[\sqrt{d}]$ modulo (α) enthält.

(b) Wir müssen noch zeigen, dass zwei Elemente der angegebenen Menge R genau dann kongruent modulo (α) sind, wenn sie gleich sind. Seien also $r + s\sqrt{d}, r' + s'\sqrt{d}$ Elemente der Menge mit
$$r + s\sqrt{d} \equiv r' + s'\sqrt{d} \bmod (\alpha).$$
Insbesondere gilt dann
$$0 \leq r, r' \leq |m(a^2 - db^2)| - 1 \text{ und } 0 \leq s, s' \leq m - 1.$$
Dann gibt es $x, y \in \mathbb{Z}$ mit
$$r' + s'\sqrt{d} = r + s\sqrt{d} + x \cdot m(a^2 - db^2) + y \cdot (mau + m\sqrt{d}).$$
Vergleich der Koeffizienten bei $\sqrt{d}$ liefert
$$s' = s + ym.$$
Wegen $0 \leq s, s' \leq m - 1$ folgt $y = 0$, und damit $s' = s$. Es bleibt:
$$r' = r + xm(a^2 - db^2).$$
Wegen $0 \leq r, r' \leq |m(a^2 - db^2)| - 1$ folgt $x = 0$ und $r = r'$. Dies beweist die Behauptung.

(4) Dies ist nur eine Zusammenfassung von dem, was bereits unter (3) gezeigt wurde. ■

Beispiele: Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$.

(1) Für $\alpha = a + b\sqrt{d}$ mit $\mathrm{ggT}(a,b) = 1$ ist
$$\{r \in \mathbb{Z} : 0 \leq r \leq |a^2 - db^2| - 1\}$$
ein Repräsentantensystem von $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$.

(2) Für $\alpha = m$ mit $m \in \mathbb{N}$ ist
$$\{r + s\sqrt{d} : 0 \leq r, s \leq m - 1\}$$
ein Repräsentantensystem von $\mathbb{Z}[\sqrt{d}]/(m)$.

10. Anhang: Wann ist ein faktorieller Ring ein Hauptidealring?

Bemerkungen:

(1) Wir wissen, dass jeder Hauptidealring ein faktorieller Ring ist. Allerdings muss nicht jeder faktorielle Ring ein Hauptidealring sein, wie das Beispiel in (2) zeigt.
(2) Der Ring $\mathbb{Z}[x]$ ist faktoriell (als Polynomring über dem faktoriellen Ring $\mathbb{Z}$), aber kein Hauptidealring, da beispielsweise das Ideal $(2, x)$ kein Hauptideal ist.
(3) Wir haben im Abschnitt über Hauptidealringe gesehen, dass in einem Hauptidealring R für jedes Primelement π das Hauptideal (π) sogar ein maximales Ideal ist. Wir werden zeigen, dass sich die Hauptidealringe dadurch auch unter den faktoriellen Ringen charakterisieren lassen.

SATZ. *Sei R ein faktorieller Ring. Genau dann ist R ein Hauptidealring, wenn für jedes Primelement π das Hauptideal (π) ein maximales Ideal ist.*

Beweis:

- $\Longrightarrow$ Ist R ein Hauptidealring, so haben wir bereits früher gezeigt, dass für jedes Primelement π das Hauptideal (π) maximal ist.
- $\Longleftarrow$ Sei nun R ein faktorieller Ring mit der Eigenschaft, dass für jedes Primelement π das Hauptideal (π) maximal ist. Besitzt R keine Primelemente, so ist R ein Körper, $\{0\} = (0)$ und $R = (1)$ sind die einzigen Ideale von R und wir sind fertig. Wir können also annehmen, dass Primelemente in R existieren.
  (1) *Behauptung:* Jedes maximale Ideal $\mathfrak{m}$ wird von einem Primelement π erzeugt, d.h. $\mathfrak{m} = (\pi)$.
  Beweis: Sei $\alpha \in \mathfrak{m} \setminus \{0\}$. Wir schreiben α als Produkt von Primelementen: $\alpha = \pi_1 \dots \pi_r$. Dann ist $\pi_1 \dots \pi_r \in \mathfrak{m}$. Da $\mathfrak{m}$ insbesondere ein Primideal ist, gibt es einen Index i mit $\pi_i \in \mathfrak{m}$, also $(\pi_i) \subseteq \mathfrak{m}$. Da nach Voraussetzung (π_i) maximal ist, folgt $\mathfrak{m} = (\pi_i)$, und damit die Behauptung.
  (2) Sei nun $\mathfrak{a}$ ein beliebiges, von (0) verschiedenes Ideal. Wir wählen ein Element $\alpha \in \mathfrak{a} \setminus \{0\}$. Wir konstruieren eine Folge π_i von Primelementen und Idealen $\mathfrak{a}_i$ wie folgt:
    - Wir beginnen mit $\mathfrak{a}_0 = \mathfrak{a}$.
    - Sei nun $\mathfrak{a}_i$ (mit $i \geq 0$) bereits konstruiert.
      * Ist $\mathfrak{a}_i = (1) = R$, so hören wir auf.
      * Ist $\mathfrak{a}_i \subsetneq R$, so ist $\mathfrak{a}_i$ in einem maximalen Ideal enthalten, es gibt also ein Primelement π_{i+1} mit $\mathfrak{a}_i \subseteq (\pi_{i+1})$. Wir definieren
      $$\mathfrak{a}_{i+1} = \{x \in R : \pi_{i+1}x \in \mathfrak{a}_i\}.$$
      Dann ist $\mathfrak{a}_{i+1}$ ein Ideal mit $\mathfrak{a}_i = \pi_{i+1}\mathfrak{a}_{i+1}$.

  Ist $i \geq 1$ und $\mathfrak{a}_i$ definiert, so gilt also
  $$\mathfrak{a} = \pi_1\pi_2 \dots \pi_i\mathfrak{a}_i.$$
  Wegen $\alpha \in \mathfrak{a}$ gilt $\alpha \in (\pi_1 \dots \pi_i)$, also
  $$\pi_1 \dots \pi_i \mid \alpha.$$
  Hat α genau s Primteiler, so gilt also $i \leq s$. Es gibt also einen Index $r \leq s$ mit $\mathfrak{a}_r = R$. Dann ist
  $$\mathfrak{a} = (\pi_1 \dots \pi_r),$$

$\mathfrak{a}$ ist also ein Hauptideal. Da $\mathfrak{a}$ ein beliebiges Ideal $\neq (0)$ sein konnte, folgt, dass R ein Hauptidealring ist. ■

Folgerung. *Ist R ein faktorieller Ring, mit der Eigenschaft, dass für jedes Primelement π der Restklassenring $R/(\pi)$ endlich ist, so ist R ein Hauptidealring.*

Beweis: Ist π ein Primelement, so ist (π) ein Primideal, also $R/(\pi)$ ein Integritätsring. Nach Voraussetzung ist $R/(\pi)$ endlich. Als endlicher Integritätsring ist dann $R/(\pi)$ bereits ein Körper, also (π) ein maximales Ideal. Die Behauptung folgt nun aus dem vorangegangenen Satz. ■

Folgerung. *Sei $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$. Dann gilt für den Ring $\mathbb{Z}[\sqrt{d}]$:*

$$\mathbb{Z}[\sqrt{d}] \text{ ist Hauptidealring} \quad \Longleftrightarrow \quad \mathbb{Z}[\sqrt{d}] \text{ ist faktoriell.}$$

Beweis:

- $\Longrightarrow$ Dies ist klar, da jeder Hauptidealring ein faktorieller Ring ist.
- $\Longrightarrow$ Sei $\mathbb{Z}[\sqrt{d}]$ faktoriell. Ist $\alpha \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}$, so gilt für den Restklassenring $\mathbb{Z}[\sqrt{d}]/(\alpha)$
$$|\mathbb{Z}[\sqrt{d}]/(\alpha)| = |\mathrm{N}(\alpha)|.$$
Der Restklassenring ist also endlich. Nach der vorangegangenen Folgerung ist daher $\mathbb{Z}[\sqrt{d}]$ ein Hauptidealring. ■

11. Anhang: Für $d \leq -3$ ist $\mathbb{Z}[\sqrt{d}]$ nicht faktoriell

Die Ringe $\mathbb{Z}[\sqrt{-1}]$ und $\mathbb{Z}[\sqrt{-2}]$ sind euklidisch, insbesondere also faktoriell.

Satz. *Für $d \leq -3$ ist das Element 2 in $\mathbb{Z}[\sqrt{d}]$ irreduzibel, aber nicht prim. Insbesondere ist der Ring $\mathbb{Z}[\sqrt{d}]$ nicht faktoriell.*

Beweis: Wir betrachten den Ring $\mathbb{Z}[\sqrt{d}]$ mit $d \leq -3$.

(1) Die Norm ist $\mathrm{N}(x + y\sqrt{d}) = x^2 - dy^2 = x^2 + |d|y^2$. Die Norm ist also immer ≥ 0. Da sich die Einheiten ε durch $\mathrm{N}(\varepsilon) = \pm 1$ charakterisieren lassen, folgt sofort
$$\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\}.$$
Wegen $|d| \geq 3$ und $\mathrm{N}(x + y\sqrt{d}) = x^2 + |d|y^2$ sieht man auch sofort, dass es keine Elemente mit Norm ± 2 gibt.

(2) Warum ist 2 irreduzibel? Wir setzen an $2 = \alpha\beta$ mit $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. Normbildung liefert
$$4 = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$
Da es keine Elemente mit Norm 2 gibt, folgt $\mathrm{N}(\alpha) = 1$ oder $\mathrm{N}(\beta) = 1$, d.h. $\alpha = \pm 1$ oder $\beta = \pm 1$. Die 2 lässt sich also nur trivial in $\mathbb{Z}[\sqrt{d}]$ zerlegen, was beweist, dass 2 irreduzibel in $\mathbb{Z}[\sqrt{d}]$ ist.

(3) Warum ist 2 kein Primelement in $\mathbb{Z}[\sqrt{d}]$?
- Im Fall $d \equiv 0 \bmod 2$ gilt wegen $2 \mid d$
$$2 \nmid \sqrt{d}, \quad \text{aber} \quad 2 \mid \sqrt{d} \cdot \sqrt{d},$$
also ist 2 kein Primelement.
- Im Fall $d \equiv 1 \bmod 2$ ist $(1 + \sqrt{d})(1 - \sqrt{d}) = 1 - d$, also gilt
$$2 \nmid 1 + \sqrt{d}, \quad 2 \nmid 1 - \sqrt{d}, \quad \text{aber} \quad 2 \mid (1 + \sqrt{d}) \cdot (1 - \sqrt{d}),$$
was zeigt, dass 2 kein Primelement ist.

(4) Da in einem faktoriellen Ring irreduzible Elemente auch Primelemente sind, kann $\mathbb{Z}[\sqrt{d}]$ für $d \leq -3$ nicht faktoriell sein. ■