4. Teil: Ringe II

18. Faktorisierungen in kommutativen Ringen

Definition: Es sei R ein kommutativer Ring und $a, b \in R$. Man sagt, a teilt b (und schreibt dafür kurz $a \mid b$) wenn $\exists x \in R : ax = b$.

Definition: Es sei R ein kommutativer Ring und $a, b \in R$. Man sagt, a und b seien assoziiert wenn $a \mid b$ und $b \mid a$.

Bemerkung: Auf der Menge $\mathbb{N} \setminus \{0\}$ (die mit der üblichen Addition und Multiplikation keinen Ring bildet) hat die Teilerrelation alle Eigenschaften einer Ordnungsrelation, d.h. sie ist reflexiv (da $a \mid a \; \forall a \in \mathbb{N} \setminus \{0\}$), antisymmetrisch (da $a \mid b \; \wedge \; b \mid a \Rightarrow a = b$) und transitiv (da $a \mid b \; \wedge \; b \mid c \Rightarrow a \mid c$). Auf dem kommutativen Ring der ganzen Zahlen $\mathbb{Z}$ ist die Teilerrelation noch immer reflexiv und transitiv, aber nicht mehr antisymmetrisch (da nur mehr $a \mid b \; \wedge b \mid a \Rightarrow |a| = |b|$ gilt).

Lemma 130: (i) In einem beliebigen kommutativen Ring R braucht ein $a \in R$ keine Teiler zu besitzen. Insbesondere ist die Teilerrelation im Allgemeinen nicht reflexiv.
(ii) Ist R ein kommutativer Ring mit Eins, so gelten $u \mid a$ und $ua \mid a$ für alle $a \in R$ und alle $u \in R^*$.
(iii) Ist R ein kommutativer Ring mit Eins, so gelten $1 \mid a$ und $a \mid a$ für alle $a \in R$, d.h. die Teilerrelation ist reflexiv.
(iv) Ist R ein kommutativer Ring und für $a, b, c \in R$ gelten $a \mid b$ und $b \mid c$, so folgt $a \mid c$, d.h. die Teilerrelation ist transitiv.

Beweis: (i) Es sei $R = 2\mathbb{Z}$ der kommutative Ring der geraden ganzen Zahlen. Dann besitzt $2 \in R$ keine Teiler in R. (Es seien $a, b \in R$. Ist $a = 0$ oder $b = 0$, so ist $ab = 0 \neq 2$. Ist $a \neq 0$ und $b \neq 0$, so ist $|ab| \geq 4$ und daher $ab \neq 2$.)
(ii) Für $a \in R$ und $u \in R^*$ ist $a = u \cdot (u^{-1}a)$ und $a = u^{-1}(ua)$.
(iii) Erhält man sofort aus (ii), indem man $u = 1$ setzt.
(iv) Da $a \mid b$ und $b \mid c$, existieren $k, \ell \in R$, sodass $b = ak$ und $c = b\ell$ und somit $c = a(k\ell)$.

Satz 131: Es sei R ein kommutativer Ring mit Eins und $a, b, u \in R$. Dann gelten:

(i) $a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$ (wobei $(a) = aR = Ra$ das von a erzeugte Ideal bezeichnet),
(ii) a und b sind assoziiert $\Leftrightarrow (a) = (b)$,
(iii) $u \in R^* \Leftrightarrow u \mid x \; \forall x \in R \Leftrightarrow u \mid 1$,
(iv) $u \in R^* \Leftrightarrow (u) = R$,
(v) Assoziiert zu sein ist eine Äquivalenzrelation auf R,

(vi) Wenn $\exists v \in R^* : a = bv$, so sind a und b assoziiert,
(vii) Ist R ein Integritätsbereich und a und b sind assoziiert, so $\exists v \in R^* : a = bv$,
(viii) Ist R ein Integritätsbereich, so gilt: a und b sind assoziiert $\Leftrightarrow \exists v \in R^* : a = bv$.

Beweis: (i) $a \mid b \Leftrightarrow \exists x \in R : b = ax \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$,
(ii) a und b sind assoziiert $\Leftrightarrow a \mid b$ und $b \mid a \overset{\text{(i)}}{\Leftrightarrow} (a) \subseteq (b)$ und $(b) \subseteq (a) \Leftrightarrow (a) = (b)$,
(iii) Ist $u \in R^*$, so ist $x = u\big(u^{-1}x\big)$ $\forall x \in R$ und daher $u \mid x$ $\forall x \in R$.
Gilt $u \mid x$ $\forall x \in R$, so gilt insbesondere $u \mid 1$.
Aus $u \mid 1$ folgt $\exists x \in R : ux = 1$ und daher $u \in R^*$.
(iv) ($\Rightarrow$) $u \in R^* \Rightarrow \exists x \in R : ux = 1 \Rightarrow 1 \in uR = (u) \Rightarrow y = y \cdot 1 \in (u)$ $\forall y \in R \Rightarrow R \subseteq (u)$,
($\Leftarrow$) $(u) = R \Rightarrow 1 \in (u) = uR \Rightarrow \exists x \in R : ux = 1 \Rightarrow u \in R^*$.
(v) Reflexivität folgt aus Lemma 130 (iii). Symmetrie folgt aus der Definition. Sind a und b assoziiert und b und c assoziiert, so gelten $a \mid b$ und $b \mid a$ sowie $b \mid c$ und $c \mid b$. Daraus folgt $a \mid c$ und $c \mid a$ wegen Lemma 130 (iv), d.h. a und c sind assoziiert.
(vi) Aus $a = bv$ folgt $b \mid a$. Da daraus sofort $b = av^{-1}$ folgt, gilt auch $a \mid b$.
(vii) Sei zunächst $a = 0$. Da $a \mid b$, existiert ein $x \in R$ mit $b = ax = 0 \cdot x = 0$ Also ist $a = b$ und man kann $v = 1 \in R^*$ wählen. Seien also nun $a \neq 0$ und $a \mid b$ und $b \mid a$. Dann gibt es $v, w \in R$, derart dass $a = bv$ und $b = aw$, woraus man sofort $a \cdot 1 = a = avw$ erhält. Wegen Lemma 50 folgt $vw = 1$ und somit $v, w \in R^*$.
(viii) Folgt sofort aus (vi) und (vii).

Beispiel: Im Integritätsbereich $\mathbb{Z}$ sind die zu $a \in \mathbb{Z}$ assoziierten Elemente genau a und $-a$. Das folgt aus Satz 131 (viii) und $\mathbb{Z}^* = \{-1, 1\}$. Zwei Zahlen $a, b \in \mathbb{Z}$ sind offenbar genau dann assoziiert wenn $|a| = |b|$. Die Äquivalenzklassen zueinander assoziierter Elemente sind also in diesem Fall $\{0\}$, $\{-1, 1\}$, $\{-2, 2\}$, $\{-3, 3\}$, ...

Definition: Es sei R ein kommutativer Ring mit Eins.
1) Ein $p \in R$ mit $p \neq 0$ und $p \notin R^*$ heißt irreduzibel, wenn aus $p = ab$ folgt, dass $a \in R^*$ oder $b \in R^*$ (wobei $a, b \in R$).
2) Ein $p \in R$ mit $p \neq 0$ und $p \notin R^*$ heißt prim, wenn aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$ (wobei $a, b \in R$).

Bemerkungen: 1) Ein primes Element eines kommutativen Rings mit Eins braucht nicht irreduzibel zu sein. Z.B. ist die Restklasse $\overline{2} \in \mathbb{Z}_6$ prim aber nicht irreduzibel. Der Verknüpfungstafel der Multiplikation im Restklassenring $\mathbb{Z}_6$ entnimmt man, dass $\overline{2} \mid \overline{0}$, $\overline{2} \mid \overline{2}$ und $\overline{2} \mid \overline{4}$ aber $\overline{2} \nmid \overline{1}$, $\overline{2} \nmid \overline{3}$ und $\overline{2} \nmid \overline{5}$. Dabei tritt $\overline{0}$ folgendermaßen als Produkt auf (wobei die Kommutativität berücksichtigt wurde):

$$\overline{0} = \overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{1} = \overline{0} \cdot \overline{2} = \overline{0} \cdot \overline{3} = \overline{0} \cdot \overline{4} = \overline{0} \cdot \overline{5} = \overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{4},$$

sowie $\overline{2}$ und $\overline{4}$ als

$$\overline{2} = \overline{1} \cdot \overline{2} = \overline{2} \cdot \overline{4} = \overline{4} \cdot \overline{5} \quad \text{und} \quad \overline{4} = \overline{1} \cdot \overline{4} = \overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{5} = \overline{4} \cdot \overline{4}.$$

Da $\overline{2}$ in jedem Fall einen der Faktoren teilt, ist $\overline{2}$ ein primes Element von $\mathbb{Z}_6$. Andererseits ist $\overline{2} = \overline{2} \cdot \overline{4}$ und $\overline{2}, \overline{4} \notin \mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$ und $\overline{2}$ daher nicht irreduzibel.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Wir werden allerdings in Satz 132 (iii) zeigen, dass in einem Integritätsbereich jedes prime Element auch irreduzibel ist.

2) Ein irreduzibles Element eines Integritätsbereichs braucht nicht prim zu sein. Es sei R der Integritätsbereich $R = \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \,|\, a, b \in \mathbb{Z}\}$ (versehen mit der üblichen Addition und Multiplikation komplexer Zahlen). Dann kann man z.B. zeigen, dass $2 \in R$ irreduzibel aber nicht prim ist.

Sind $a, b, c, d \in \mathbb{Z}$, so ist

$$(a + i\sqrt{5}b) - (c + i\sqrt{5}d) = (a - c) + i\sqrt{5}(b - d) \in R$$

und

$$(a + i\sqrt{5}b)(c + i\sqrt{5}d) = (ac - 5bd) + i\sqrt{5}(ad + bc) \in R.$$

Daher ist R ein Unterring (mit Eins) des Körpers $\mathbb{C}$ und damit sogar ein Integritätsbereich. Wir zeigen zuerst, dass $R^* = \{-1, 1\}$. Ist $a + i\sqrt{5}b \in R^*$ (mit $a, b \in \mathbb{Z}$), so ist

$$(a + i\sqrt{5}b)(c + i\sqrt{5}d) = 1 \text{ (für gewisse } c, d \in \mathbb{Z})$$

Durch komplexe Konjugation folgt daraus $(a - i\sqrt{5}b)(c - i\sqrt{5}d) = 1$ und durch Multiplikation der beiden Gleichungen erhält man

$$(a^2 + 5b^2)(c^2 + 5d^2) = (a + i\sqrt{5}b)(c + i\sqrt{5}d)(a - i\sqrt{5}b)(c - i\sqrt{5}d) = 1 \cdot 1 = 1.$$

Daraus folgt sofort $a^2 + 5b^2 = 1$. Für $b \neq 0$ ist $a^2 + 5b^2 \geq 5$ und daher muss $b = 0$ und $a^2 = 1$ gelten. Also ist $a \in \{-1, 1\}$ und folglich auch $a + i\sqrt{5}b \in \{-1, 1\}$. Damit ist $R^* \subseteq \{-1, 1\}$ gezeigt. Aus $1^2 = (-1)^2 = 1$ folgt sofort $\{-1, 1\} \subseteq R^*$.

Wir zeigen nun, dass 2 irreduzibel ist. Offensichtlich ist $2 \neq 0$ und $2 \notin R^*$. Angenommen

$$2 = (a + i\sqrt{5}b)(c + i\sqrt{5}d)$$

für gewisse $a, b, c, d \in \mathbb{Z}$. Wieder folgt durch komplexe Konjugation

$$(a - i\sqrt{5}b)(c - i\sqrt{5}d) = 2$$

und durch Multiplikation der beiden Gleichungen

$$(a^2 + 5b^2)(c^2 + 5d^2) = (a + i\sqrt{5}b)(c + i\sqrt{5}d)(a - i\sqrt{5}b)(c - i\sqrt{5}d) = 4.$$

Nun kann unmöglich $a^2 + 5b^2 = 2$ gelten. (Ist $b \neq 0$, so folgt $a^2 + 5b^2 \geq 5$. Also müsste $b = 0$ und damit $a^2 = 2$ sein.) Daher muss entweder $a^2 + 5b^2 = 1$ und $c^2 + 5d^2 = 4$ oder $a^2 + 5b^2 = 4$ und $c^2 + 5d^2 = 1$ gelten. Im ersten Fall ist $(a + i\sqrt{5}b)(a - i\sqrt{5}b) = a^2 + 5b^2 = 1$ und daher $a + i\sqrt{5}b \in R^*$. Im zweiten Fall folgt analog $c + i\sqrt{5}d \in R^*$.
Wir zeigen nun, dass 2 nicht prim ist. Da $2 \mid 6$ und $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ gilt

$$2 \mid (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Nun ist aber $2 \nmid (1 + i\sqrt{5})$ und $2 \nmid (1 - i\sqrt{5})$. Würde nämlich $2 \mid (1 \pm i\sqrt{5})$ gelten, so gäbe es $x, y \in \mathbb{Z}$, derart dass $1 \pm i\sqrt{5} = 2(x + i\sqrt{5}y)$ und daher $1 = 2x$, ein Widerspruch.

Satz 132: Es sei R ein Integritätsbereich und $p \in R$. Dann gelten:

(i) p ist prim $\Leftrightarrow (p) \neq (0)$ und (p) ist ein Primideal von R,
(ii) p ist irreduzibel $\Leftrightarrow (p) \neq (0)$ und (p) ist maximal (bezüglich der Mengeninklusion) in der Menge $\{(a) \mid a \in R, (a) \neq R\} = \{(a) \mid a \in R \setminus R^*\}$ aller Hauptideale $\neq R$,
(iii) Ist p prim, so ist p irreduzibel,
(iv) Ist R ein Hauptidealbereich, so gilt: p ist prim $\Leftrightarrow p$ ist irreduzibel,
(v) Ist R ein Hauptidealbereich und $P \neq (0)$ ein Primideal von R, so ist P ein maximales Ideal von R,
(vi) Ist p irreduzibel und $a \in R$ ist zu p assoziiert, so ist a ebenfalls irreduzibel,
(vii) Ist p prim und $a \in R$ ist zu p assoziiert, so ist a ebenfalls prim,
(viii) Ist p irreduzibel und $a \mid p$ (mit $a \in R$), so ist a zu p assoziiert oder $a \in R^*$,
(ix) Assoziiert zu sein ist eine Äquivalenzrelation auf der Menge der irreduziblen Elemente von R,
(x) Assoziiert zu sein ist eine Äquivalenzrelation auf der Menge der primen Elemente von R.

Beweis: (i) ($\Rightarrow$) Es gelten $p \neq 0 \Rightarrow (p) \neq (0)$, $p \notin R^* \Rightarrow (p) \neq R$ (wegen Satz 131 (iv)) und $ab \in (p)$ (mit $a, b \in R$) $\Rightarrow p \mid ab \Rightarrow p \mid a$ oder $p \mid b \Rightarrow a \in (p)$ oder $b \in (p)$.
($\Leftarrow$) Es gelten $(p) \neq (0) \Rightarrow p \neq 0$, $(p) \neq R \Rightarrow p \notin R^*$ (wegen Satz 131 (iv)) und $p \mid ab$ (mit $a, b \in R$) $\Rightarrow ab \in (p) \Rightarrow a \in (p)$ oder $b \in (p) \Rightarrow p \mid a$ oder $p \mid b$.

(ii) ($\Rightarrow$) Es gelten $p \neq 0 \Rightarrow (p) \neq (0)$, $p \notin R^* \Rightarrow (p) \neq R$ und
$(p) \subseteq (a)$ (mit $a \in R$) $\Rightarrow a \mid p$ (wegen Satz 131 (i)) $\Rightarrow \exists x \in R : p = ax$
$\Rightarrow a \in R^*$ oder $x \in R^*$. Falls $a \in R^*$, so $(a) = R$ nach Satz 131 (iv). Falls $x \in R^*$, so sind a und p assoziiert (nach Satz 131 (vi)) und $(a) = (p)$ (nach Satz 131 (ii)).
($\Leftarrow$) Es gelten $(p) \neq (0) \Rightarrow p \neq 0$, $(p) \neq R \Rightarrow p \notin R^*$ (wegen Satz 131 (iv)) und
$p = ab$ (mit $a, b \in R$) $\Rightarrow a \mid p \Rightarrow (p) \subseteq (a)$ (wegen Satz 131 (i)) $\Rightarrow (p) = (a)$ oder $(a) = R$.
Falls $(a) = R$, so ist $a \in R^*$ nach Satz 131 (iv). Falls $(a) = (p)$, so $p \mid a \Rightarrow \exists x \in R : a = px$
$\Rightarrow p = ab = pxb \Rightarrow xb = 1$ (wegen Lemma 50) $\Rightarrow b \in R^*$.
(iii) Es gilt $p = ab$ (mit $a, b \in R$) $\Rightarrow p \mid ab \Rightarrow p \mid a$ oder $p \mid b$. Wenn $p \mid a \Rightarrow \exists x \in R : a = px$
$\Rightarrow p = ab = pxb \Rightarrow xb = 1 \Rightarrow b \in R^*$. Wenn $p \mid b$ zeigt man analog $a \in R^*$.
(iv) ($\Rightarrow$) Gilt allgemein und wurde in (iii) bewiesen.
($\Leftarrow$) Da R ein Hauptidealbereich ist, ist (p) nach (ii) ein maximales Ideal und daher (nach Korollar 78) ein Primideal $\neq (0)$. Nach (i) ist p prim.
(v) Da R ein Hauptidealbereich ist $\exists p \in R \setminus \{0\} : P = (p)$. Nach (i) ist p prim und daher ist p irreduzibel (nach (iii)). Wegen (ii) ist $P = (p)$ daher ein maximales Ideal.
(vi) und (vii) Ist a zu p assoziiert, so $\exists u \in R^* : p = au$ nach Satz 131 (vii). Daher ist $a = 0$ unmöglich, da daraus $p = 0$ folgen würde. Ebenso ist $a \in R^*$ unmöglich, da daraus $p \in R^*$ folgen würde.
Sei p nun irreduzibel. Dann gilt $a = bc$ (für $b, c \in R$) $\Rightarrow p = au = bcu$
$\Rightarrow b \in R^*$ oder $cu \in R^*$ (und daher $c \in R^*$). Also ist a ebenfalls irreduzibel.
Sei p nun prim. Dann gilt $a \mid bc$ (für $b, c \in R$) $\Rightarrow p \mid bc$ (wegen Lemma 130 (iv))
$\Rightarrow p \mid b$ oder $p \mid c \Rightarrow a \mid b$ oder $a \mid c$ (wegen Lemma 130 (iv)). Daher ist a ebenfalls prim.
(viii) Es gilt $a \mid p \Rightarrow (p) \subseteq (a)$ (nach Satz 131 (i)) $\Rightarrow (p) = (a)$ oder $(a) = R$ (wegen (ii))
$\Rightarrow a$ ist zu p assoziiert oder $a \in R^*$ (wegen Satz 131 (ii) bzw. Satz 131 (iv)).
(ix) Folgt sofort aus Satz 131 (v) und (vi).
(x) Folgt sofort aus Satz 131 (v) und (vii).

Korollar 133: Für ein $p \in \mathbb{Z}$ sind äquivalent:

(i) p ist prim,
(ii) p ist irreduzibel,
(iii) $|p|$ ist eine Primzahl.

Beweis: (i) $\Leftrightarrow$ (ii) Folgt sofort aus Satz 132 (iv), da $\mathbb{Z}$ ein Hauptidealbereich ist.
(ii) $\Rightarrow$ (iii) Da p irreduzibel und $\mathbb{Z}^* = \{-1, 1\}$ ist, ist $p \notin \{-1, 0, 1\}$ und daher $|p| \geq 2$. Es sei $m \in \mathbb{Z}$ und $m \,\big|\, |p|$. Wir wollen zeigen, dass $m \in \{-1, 1, -p, p\}$ ist. Zunächst $\exists n \in \mathbb{Z} : |p| = mn$. Ist $\varepsilon = \operatorname{sgn} p \in \{-1, 1\}$, so ist $p = \varepsilon mn$ und daher (da p irreduzibel ist) $\varepsilon m \in \{-1, 1\}$ (und folglich $m \in \{-1, 1\}$) oder $n \in \{-1, 1\}$ (woraus $\varepsilon m \in \{-p, p\}$ und

daher $m \in \{-p, p\}$ folgt).
(iii) $\Rightarrow$ (ii) Da $|p| \geq 2$ ist $p \notin \{-1, 0, 1\}$. Ist $p = mn$ (mit $m, n \in \mathbb{Z}$), so folgt sofort $|p| = |m| \cdot |n|$. Da $|p|$ eine Primzahl ist, muss entweder $|m| = 1$ (und daher $m \in \{-1, 1\}$) oder $|n| = 1$ (und daher $n \in \{-1, 1\}$) gelten.

Bemerkung: Die Menge der primen bzw. irreduziblen Elemente von $\mathbb{Z}$ ist also

$$\{p \mid p \text{ ist Primzahl}\} \cup \{-p \mid p \text{ ist Primzahl}\} = \{2, 3, 5, 7, \dots\} \cup \{-2, -3, -5, -7, \dots\}$$

und die Äquivalenzklassen zueinander assoziierter primer bzw. irreduzibler Elemente sind

$$\{-2, 2\},\ \{-3, 3\},\ \{-5, 5\},\ \{-7, 7\},\ \{-11, 11\},\ \dots$$

Definition: Ein Integritätsbereich R heißt faktorieller Ring (oder ZPE – Ring) wenn die folgenden beiden Bedingungen erfüllt sind:
1) Für jedes $a \in R$ mit $a \neq 0$ und $a \notin R^*$ existiert eine Produktdarstellung $a = p_1 \cdots p_n$ für gewisse irreduzible $p_1, \dots, p_n \in R$.
2) Die in Bedingung 1) beschrieben Produktdarstellung ist eindeutig im folgenden Sinn: Ist $a \in R$ mit $a \neq 0$ und $a \notin R^*$ und $a = p_1 \cdots p_n = q_1 \cdots q_m$ zwei Produktdarstellungen für irreduzible $p_1, \dots, p_n, q_1, \dots, q_m \in R$, so ist $m = n$ und es gibt eine Permutation $\sigma \in S_n$, derart dass p_i und $q_{\sigma(i)}$ assoziiert sind für $1 \leq i \leq n$.

Beispiele: 1) Die ganzen Zahlen $\mathbb{Z}$ sind ein faktorieller Ring. Da $\mathbb{Z}^* = \{-1, 1\}$, muss jedes $a \in \mathbb{Z}$ mit $|a| \geq 2$ als Produkt irreduzibler Elemente dargestellt werden können. Besitzt $|a| \geq 2$ die Primfaktorzerlegung $|a| = p_1 \cdots p_n$ (für gewisse Primzahlen $p_1, \dots, p_n$) und ist $\varepsilon = \operatorname{sgn} a \in \{-1, 1\}$, so ist $a = (\varepsilon p_1) p_2 \cdots p_n$ nach Korollar 133 eine solche Produktdarstellung und Bedingung 1) ist daher erfüllt. Es sei nun $|a| \geq 2$ und $a = p_1 \cdots p_n = q_1 \cdots q_m$ zwei Produktdarstellungen von a mit irreduziblen $p_1, \dots, p_n, q_1, \dots, q_m \in \mathbb{Z}$. Dann folgt sofort $|a| = |p_1| \cdots |p_n| = |q_1| \cdots |q_m|$, wobei $|p_1|, \dots, |p_n|, |q_1|, \dots, |q_m|$ Primzahlen sind (wieder wegen Korollar 133). Wegen der Eindeutigkeit der Primfaktorzerlegung ist $m = n$ und es gibt eine Permutation $\sigma \in S_n$, derart dass $|p_i| = |q_{\sigma(i)}|$ für $1 \leq i \leq n$. Das bedeutet aber gerade, dass p_i und $q_{\sigma(i)}$ assoziiert sind.
2) Jeder Körper K ist trivialerweise ein faktorieller Ring, der außer dem Nullelement allerdings nur die Einheiten $K^* = K \setminus \{0\}$ (und daher keine irreduziblen Elemente) enthält.
3) Der Integritätsbereich $R = \mathbb{Z}\big[i\sqrt{5}\big] = \big\{a + i\sqrt{5}b \,\big|\, a, b \in \mathbb{Z}\big\}$ (versehen mit der üblichen Addition und Multiplikation komplexer Zahlen) ist kein faktorieller Ring. Um das zu beweisen, betrachten wir die Faktorisierungen $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Wir haben bereits oben gezeigt, dass $2 \in R$ irreduzibel ist. Man kann nun ganz ähnlich beweisen, dass $3, 1 + i\sqrt{5}, 1 - i\sqrt{5} \in R$ alle irreduzibel sind. Offensichtlich sind diese drei Zahlen $\neq 0$ und nicht in $R^* = \{-1, 1\}$.

Ist $3 = (a + i\sqrt{5}b)(c + i\sqrt{5}d)$ (mit $a, b, c, d \in \mathbb{Z}$), so würde analog zu oben

$$(a^2 + 5b^2)(c^2 + 5d^2) = (a + i\sqrt{5}b)(c + i\sqrt{5}d)(a - i\sqrt{5}b)(c - i\sqrt{5}d) = 9$$

folgen. Ähnlich wie dort ist $a^2+5b^2 = 3$ unmöglich. Daher muss entweder $a^2+5b^2 = 1$ (und daher $(a + i\sqrt{5}b)(a - i\sqrt{5}b) = 1$) oder $c^2 + 5d^2 = 1$ (und daher $(c + i\sqrt{5}d)(c - i\sqrt{5}d) = 1$) gelten und $3 \in R$ ist somit irreduzibel.
Ist $1 \pm i\sqrt{5} = (a + i\sqrt{5}b)(c + i\sqrt{5}d)$, so erhält man völlig analog

$$(a^2 + 5b^2)(c^2 + 5d^2) = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 6.$$

Wie oben ist $a^2 + 5b^2 \in \{2, 3\}$ unmöglich und daher entweder $(a + i\sqrt{5}b)(a - i\sqrt{5}b) = 1$ oder $(c + i\sqrt{5}d)(c - i\sqrt{5}d) = 1$ und $1 + i\sqrt{5}, 1 - i\sqrt{5} \in R$ sind irreduzibel.
Wäre R faktoriell, so müsste 2 entweder zu $1 + i\sqrt{5}$ oder zu $1 - i\sqrt{5}$ assoziiert sein, was wegen $R^* = \{-1, 1\}$ und Satz 131 (viii) unmöglich ist.

Satz 134: Es sei R ein faktorieller Ring und $p \in R$. Dann gilt

$$p \text{ ist prim} \Leftrightarrow p \text{ ist irreduzibel.}$$

Beweis: ($\Rightarrow$) Gilt allgemein, siehe Satz 132 (iii).
($\Leftarrow$) Ist $p \mid ab$ (für $a, b \in R$), so $\exists x \in R : ab = px$. Falls $a = 0$, so $p \mid a$ (da $a = 0 = p \cdot 0$). Ebenso folgt aus $b = 0$, dass $p \mid b$. Es gelte darum ab jetzt $a, b \in R \setminus \{0\}$.
Es ist nicht möglich, dass $a, b \in R^*$, da dann auch $ab \in R^*$, woraus $px(ab)^{-1} = 1$ und daher $p \in R^*$ folgen würde, ein Widerspruch.
Wenn $a, b \in R \setminus R^*$, gibt es irreduzible $p_1, \dots, p_n, q_1, \dots, q_m \in R$, derart dass $a = p_1 \cdots p_n$ und $b = q_1 \cdots q_m$ und somit

$$px = ab = p_1 \cdots p_n q_1 \cdots q_m.$$

Da R faktoriell ist, gibt es entweder ein $i \in \{1, \dots, n\}$, derart dass p zu p_i assoziiert ist oder ein $j \in \{1, \dots, m\}$, derart dass p zu q_j assoziiert ist. Im ersten Fall gilt $p \mid p_i$ und daher $p \mid a$. Im zweiten Fall gilt $p \mid q_j$ und daher $p \mid b$.
Ist $a \in R^*$, so muss $b \in R \setminus R^*$ gelten und daher $b = q_1 \cdots q_m$ für gewisse irreduzible $q_1, \dots, q_m \in R$. Es folgt $p(xa^{-1}) = q_1 \cdots q_m$ und p muss zu einem der irreduziblen Elemente $q_1, \dots, q_m$ assoziiert sein. Daher gibt es wieder ein $j \in \{1, \dots, m\}$, für das $p \mid q_j$ und daher $p \mid b$ gilt. Ist $b \in R^*$, so muss $a \in R \setminus R^*$ gelten und man zeigt analog $p \mid a$.

Satz 135: Es sei R ein kommutativer Ring mit Eins. Dann sind äquivalent:

(i) Jede aufsteigende Kette von Idealen in R wird stationär. D.h. sind

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Ideale von R, so gibt es ein $n \in \mathbb{N} \setminus \{0\}$ mit der Eigenschaft $I_n = I_k$ für alle $k \geq n$.

(ii) Jede Menge $\mathcal{M} \neq \varnothing$ von Idealen von R besitzt ein maximales Element (bezüglich der Mengeninklusion).
(iii) Jedes Ideal I von R ist endlich erzeugt, d.h. $\exists a_1, \dots, a_n \in R : I = (a_1, \dots, a_n)$.

Beweis: (i) $\Rightarrow$ (ii) Es sei $\mathcal{M}$ eine nichtleere Menge von Idealen von R, die kein maximales Element besitzt. Da $\mathcal{M} \neq \varnothing$, gibt es ein Ideal $I_1 \in \mathcal{M}$. Da I_1 nicht maximal ist (in $\mathcal{M}$), gibt es ein Ideal $I_2 \in \mathcal{M}$ mit der Eigenschaft $I_1 \subsetneqq I_2$.
Verfahre weiter so: Ist das Ideal $I_k \in \mathcal{M}$ schon gefunden, so ist es ebenfalls nicht maximal (in $\mathcal{M}$) und es gibt ein Ideal $I_{k+1} \in \mathcal{M}$ mit der Eigenschaft $I_k \subsetneqq I_{k+1}$. Auf diese Weise erhält man eine aufsteigende Kette

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

von Idealen von R, die nicht stationär wird.
(ii) $\Rightarrow$ (iii) Es sei I ein Ideal von R. Wir definieren

$$\mathcal{M} = \{J \mid J \text{ ist Ideal von } R,\ J \subseteq I \text{ und } J \text{ ist endlich erzeugt}\}.$$

Dann ist $\mathcal{M} \neq \varnothing$, da $(0) \in \mathcal{M}$ und $\mathcal{M}$ enthält ein maximales Element J_0. Wir behaupten, dass $J_0 = I$ gelten muss. Angenommen, es wäre $J_0 \subsetneqq I$. Dann existiert ein $a_0 \in I \setminus J_0$. Da J_0 endlich erzeugt ist, ist $J_0 = (a_1, \dots, a_n)$ für gewisse $a_1, \dots, a_n \in I$. Betrachte nun das Ideal $J_1 := (a_0, a_1, \dots, a_n)$. Dann ist $J_1 \subseteq I$ (da $a_0, a_1, \dots, a_n \in I$) und J_1 ist offenbar endlich erzugt. Also ist $J_1 \in \mathcal{M}$ und $J_0 \subsetneqq J_1$, was der Maximalität von J_0 widerspricht.
(iii) $\Rightarrow$ (i) Ist die aufsteigende Kette $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ von Idealen von R gegeben, so setze $J := \bigcup_{k=1}^{\infty} I_k$. Wir behaupten, dass J ebenfalls ein Ideal von R ist. Sind $a, b \in J$, so gibt es $k, \ell \geq 1$, für die $a \in I_k$ und $b \in I_\ell$ gelten. Ist $m = \max\{k, \ell\}$, so ist $a, b \in I_m$ und daher $a - b \in I_m \subseteq J$. Ist $x \in R$, so ist $xa \in I_k \subseteq J$. Da J endlich erzeugt ist, gibt es $a_1, \dots, a_n \in R$, derart dass $J = (a_1, \dots, a_n)$. Für jedes $i \in \{1, \dots, n\}$ gibt es nun ein Ideal I_{k_i} in der Kette mit der Eigenschaft $a_i \in I_{k_i}$. Ist $m = \max\{k_1, \dots, k_n\}$, so sind $a_1, \dots, a_n \in I_m$ und daher

$$J = (a_1, \dots, a_n) \subseteq I_m \subseteq J,$$

also $J = I_m$ und aus $I_m \subseteq I_k \subseteq J = I_m$ folgt $I_k = I_m$ für $k \geq m$.

Definition: Ein kommutativer Ring mit Eins R, der eine (und damit alle) der drei Eigenschaften aus Satz 135 besitzt, wird noetherscher Ring genannt.

Korollar 136: Jeder Hauptidealbereich ist ein noetherscher Ring.

Beweis: In einem Hauptidealbereich ist offenbar jedes Ideal endlich erzeugt.

Satz 137: Jeder Hauptidealbereich R ist ein faktorieller Ring.

Beweis: Angenommen, es gibt ein $a \in R$ mit der Eigenschaften $a \neq 0$ und $a \notin R^*$, das sich nicht als Produkt irreduzibler Elemente schreiben lässt. Nach Satz 79 gibt es ein maximales Ideal (p) von R, derart dass $(a) \subseteq (p)$. Dabei ist $p \in R$ irreduzibel wegen Satz 132 (ii). Wegen Satz 131 (i) folgt $p \mid a$, d.h. $\exists a_1 \in R : a = pa_1$. Dabei ist $a_1 \neq 0$ (da sonst $a = 0$ gelten würde) und $a_1 \notin R^*$ (da sonst nach a und p nach Satz 131 (viii) assoziiert wären und daher a irreduzibel nach Satz 132 (vi)). Weiters kann a_1 nicht als Produkt irreduzibler Elemente darstellbar sein, da sonst a als Produkt irreduzibler Elemente geschrieben werden könnte. Wegen $a_1 \mid a$ gilt $(a) \subseteq (a_1)$. Tatsächlich muss sogar $(a) \subsetneq (a_1)$ gelten. Wäre nämlich $(a) = (a_1)$, so wären a und a_1 assoziiert. Dann würde auch $a \mid a_1$ gelten, d.h. $\exists x \in R : a_1 = ax$. Dann wäre $a = a_1 p = axp$, woraus man $px = 1$ erhält, d.h. es wäre $p \in R^*$, ein Widerspruch.
Verfährt man weiter so, erhält man eine Folge $a, a_1, a_2, \ldots$ von Elementen aus R (mit $a_i \neq 0$ und $a_i \notin R^*$ für $i \geq 1$), von denen sich keines als Produkt irreduzibler Elemente darstellen lässt und die die Eigenschaft

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

besitzen. Das widerspricht aber Satz 135 bzw. Korollar 136. D.h. ein derartiges $a \in R$ kann nicht existieren und Eigenschaft 1) aus der Definition eines faktoriellen Rings ist erfüllt.
Angenommen ein $a \in R$ mit $a \neq 0$ und $a \notin R^*$ besitzt die Darstellungen

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

mit irreduziblen $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$. Dabei setzen wir o.B.d.A. voraus, dass $m \leq n$ und verwenden Induktion nach m.
Es sei zunächst $m = 1$, d.h. $p_1 \cdots p_n = q_1$ $(*)$. Wegen Satz 132 (iv) ist q_1 prim und daher $\exists i \in \{1, \ldots, n\} : q_1 \mid p_i$. Da auch $p_i \mid q_1$ sind q_1 und p_i assoziiert. Nach Satz 131 (viii) $\exists u \in R^* : p_i = uq_1$. Kürzt man in $(*)$ den Faktor q_1, so erhält man

$$up_1 \cdots p_{i-1} p_{i+1} \cdots p_n = 1.$$

Wäre nun $n > 1$, so wären $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n \in R^*$, ein Widerspruch. Also ist $n = i = 1$ (und q_1 und p_1 sind assoziiert).
Ist $m > 1$, so kann man analog vorgehen: Wieder ist q_m prim und aus $q_m \mid p_1 \cdots p_n$ folgt, dass $\exists i \in \{1, \ldots, n\} : q_m \mid p_i$. O.B.d.A. sei $i = n$ (ansonsten ändert man die Indizes von $p_1, \ldots, p_n$ entsprechend). Wegen Satz 132 (viii) sind q_m und p_n assoziiert und $\exists u \in R^* : p_n = uq_m$. Kürzt man, so erhält man $(up_1)p_2 \cdots p_{n-1} = q_1 \cdots q_{m-1}$. Da up_1 ebenfalls irreduzibel (wegen Satz 132 (vi)) und zu p_1 assoziiert ist, folgt die Behauptung aus der Induktionsvoraussetzung. Damit ist auch Eigenschaft 2) in der Definition eines

faktoriellen Rings gezeigt.

Bemerkungen: 1) Die Umkehrung von Satz 137 gilt nicht. Man kann z.B. zeigen, dass $\mathbb{Z}[X]$ (d.h. der Ring aller Polynome mit Koeffizienten aus $\mathbb{Z}$ und der üblichen Addition und Multiplikation von Polynomen) ein faktorieller Ring, aber kein Hauptidealbereich ist.
2) Aus Satz 137 folgt nochmals, dass $\mathbb{Z}$ ein faktorieller Ring ist. Dass $\mathbb{Z}$ ein noetherscher Ring ist, entspricht der Tatsache, dass man von einer ganzen Zahl $n \in \mathbb{Z}$ mit $|n| \geq 2$ nur endlich viele Primfaktoren abspalten kann. Z.B. entspricht $60 = 2 \cdot 30 = 2^2 \cdot 15 = 2^2 \cdot 3 \cdot 5$ der aufsteigenden Kette $(60) \subsetneqq (30) \subsetneqq (15) \subsetneqq (5)$, die beim maximalen Ideal (5) endet.

Definition: Ein Integritätsbereich R heißt euklidischer Ring, wenn es eine Abbildung $\varphi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ mit der folgenden Eigenschaft gibt:

$$\forall a, b \in R,\ b \neq 0\ \exists q, r \in R, \text{ sodass } a = bq + r \text{ und entweder } r = 0 \text{ oder } r \neq 0 \text{ and } \varphi(r) < \varphi(b)$$

Satz 138: Jeder euklidische Ring R ist ein Hauptidealbereich.

Beweis: Es sei I ein Ideal von R. Falls $I = (0)$ ist nichts zu zeigen. Sei also nun $I \neq (0)$. Dann wähle ein $a \in I \setminus \{0\}$ mit der Eigenschaft $\varphi(a) = \min\{\varphi(x) \,|\, x \in I \setminus \{0\}\}$. Dann ist offenbar $(a) \subseteq I$. Zu $b \in I$ gibt es nun $q, r \in R$, derart dass $b = qa + r$ und entweder $r = 0$ oder $\varphi(r) < \varphi(a)$. Wäre $r \neq 0$, so wäre $r = b - qa \in I$ (da $a, b \in I$) und $\varphi(r) < \varphi(a)$, was der Minimalität von $\varphi(a)$ widerspricht. Also ist $r = 0$ und $b = qa \in (a)$, d.h. es gilt auch $I \subseteq (a)$ und daher $I = (a)$.

Beispiele: 1) Der Ring $\mathbb{Z}$ der ganzen Zahlen wird durch die Abbildung $\varphi(x) = |x|$ zu einem euklidischer Ring. Wir verwenden für den Beweis Division mit absolut kleinstem Rest. Es seien $a, b \in \mathbb{Z}$ und zunächst $b > 0$. Wähle $q \in \mathbb{Z}$ mit der Eigenschaft

$$q < \tfrac{a}{b} + \tfrac{1}{2} \leq q + 1,$$

woraus sofort

$$bq < a + \tfrac{b}{2} \leq bq + b$$

und daher

$$-\tfrac{b}{2} < a - bq \leq \tfrac{b}{2}$$

folgt. Setzt man $r := a - bq$, so ist $a = bq + r$ und (für $r \neq 0$)

$$\varphi(r) = |r| \leq \tfrac{b}{2} < b = |b| = \varphi(b).$$

Ist $b < 0$, so wenden wir das bisher Gezeigte auf $-a$ und $-b(> 0)$ an. Daraus erhalten wir die Existenz von $q, r \in \mathbb{Z}$, derart dass $-a = -bq + r$ und daher $a = bq - r$ und (für $r \neq 0$)

$$\varphi(-r) = |-r| = |r| < |-b| = |b| = \varphi(b).$$

2) Das vorangegangene Beispiel zeigt, dass in einem euklidischen Ring R die Elemente $q, r \in R$ zu gegebenem $a, b \in R$ nicht eindeutig bestimmt sein müssen. Z.B. ist (für $a = 7$ und $b = 4$)

$$7 = 1 \cdot 4 + 3 = 2 \cdot 4 - 1,$$

wobei sowohl $|3| < |4|$ als auch $|-1| < |4|$.

3) Jeder Köper K wird durch die Abbildung $\varphi : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$, $\varphi(x) = 1$ zu einem euklidischen Ring. (Für $a, b \in K$ mit $b \neq 0$ ist $a = \big(ab^{-1}\big)b$, d.h. man kann $q = ab^{-1}$ und $r = 0$ wählen.)

4) Der Ring $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$ (mit der üblichen Addition und Multiplikation komplexer Zahlen) wird durch die Abbildung $\varphi : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \cup \{0\}$,

$$\varphi(x + iy) = x^2 + y^2 = |x + iy|^2 = (x + iy)(x - iy) \text{ (mit } x, y \in \mathbb{Z})$$

zu einem euklidischen Ring (und ist daher ein faktorieller Ring). Es seien $a = x + iy$ und $b = u + iv$ mit $x, y, u, v \in \mathbb{Z}$ und $b \neq 0$ (und daher $|b|^2 = u^2 + v^2 > 0$). Ist

$$\frac{a}{b} = \frac{x + iy}{u + iv} = \frac{(x + iy)(u - iv)}{(u + iv)(u - iv)} = s + it$$

mit

$$s = \frac{xu + yv}{u^2 + v^2} \in \mathbb{Q} \quad \text{und} \quad t = \frac{yu - xv}{u^2 + v^2} \in \mathbb{Q},$$

so wähle $m, n \in \mathbb{Z}$, derart dass $|s - m| \leq 1/2$ und $|t - n| \leq 1/2$. Setze $q = m + in$ und $r = a - bq$. Ist $r \neq 0$, so gilt

$$\begin{aligned}
\varphi(r) = |r|^2 = |a - bq|^2 &= |b|^2 \cdot \left|\frac{a}{b} - q\right|^2 = |b|^2 \cdot |(s + it) - (m + in)|^2 \\
&= |b|^2 \cdot |(s - m) + i(t - n)|^2 = |b|^2 \cdot \big((s - m)^2 + (t - n)^2\big) \\
&\leq |b|^2 \cdot \big(\tfrac{1}{4} + \tfrac{1}{4}\big) = \tfrac{1}{2} \cdot |b|^2 < |b|^2 = \varphi(b)
\end{aligned}$$

5) Der Ring $\mathbb{Z}\big[\sqrt{2}\big] = \big\{x + \sqrt{2}y \,\big|\, x, y \in \mathbb{Z}\big\}$ (mit der üblichen Addition und Multiplikation reeller Zahlen) wird durch die Abbildung $\varphi : \mathbb{Z}\big[\sqrt{2}\big] \setminus \{0\} \to \mathbb{N} \cup \{0\}$,

$$\varphi\big(x + \sqrt{2}y\big) = \big|x^2 - 2y^2\big| = \big|(x + \sqrt{2}y)(x - \sqrt{2}y)\big| \text{ (mit } x, y \in \mathbb{Z})$$

zu einem euklidischen Ring (und ist daher ein faktorieller Ring). Der Beweis kann weitgehend analog zum vorangegangenen Beispiel geführt werden, allerdings müssen wir zuerst Ersatz für die komplexe Konjugation schaffen, die uns dort gute Dienste geleistet hat. Versieht man die Menge $\mathbb{Q}\big(\sqrt{2}\big) = \big\{a + \sqrt{2}b \,\big|\, a, b \in \mathbb{Q}\big\}$ mit der üblichen Addition und Multiplikation reeller Zahlen, so wird sie zu einem Körper.

Zunächst folgt (für $a,b,c,d \in \mathbb{Q}$) aus

$$\big(a+\sqrt{2}b\big)-\big(c+\sqrt{2}d\big)=(a-c)+\sqrt{2}(b-d)\in\mathbb{Q}\big(\sqrt{2}\big)$$

und

$$\big(a+\sqrt{2}b\big)\big(c+\sqrt{2}d\big)=(ac+2bd)+\sqrt{2}(ad+bc)\in\mathbb{Q}\big(\sqrt{2}\big),$$

dass es sich bei $\mathbb{Q}\big(\sqrt{2}\big)$ um einen Unterring (mit Eins) des Körpers $\mathbb{R}$ handelt.
Ist $a+\sqrt{2}b\in\mathbb{Q}\big(\sqrt{2}\big)$ und $a+\sqrt{2}b\neq 0$, so ist $a^2-2b^2\neq 0$ (da $\sqrt{2}\notin\mathbb{Q}$) und daher

$$\big(a+\sqrt{2}b\big)^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in\mathbb{Q}\big(\sqrt{2}\big).$$

Damit ist bewiesen, dass es sich bei $\mathbb{Q}\big(\sqrt{2}\big)$ tatsächlich um einen Körper handelt. Klarerweise ist $\mathbb{Z}\big[\sqrt{2}\big]$ ein Unterring von $\mathbb{Q}\big(\sqrt{2}\big)$. Wir beweisen nun, dass die Abbildung

$$\sigma:\mathbb{Q}\big(\sqrt{2}\big)\to\mathbb{Q}\big(\sqrt{2}\big),\ \sigma\big(a+\sqrt{2}b\big)=a-\sqrt{2}b$$

ein Ringautomorphismus ist. Wegen

$$\begin{aligned}\sigma\big(\big(a+\sqrt{2}b\big)+\big(c+\sqrt{2}d\big)\big)&=\sigma\big((a+c)+\sqrt{2}(b+d)\big)=(a+c)-\sqrt{2}(b+d)\\&=\big(a-\sqrt{2}b\big)+\big(c-\sqrt{2}d\big)=\sigma\big(a+\sqrt{2}b\big)+\sigma\big(c+\sqrt{2}d\big)\end{aligned}$$

und

$$\begin{aligned}\sigma\big(\big(a+\sqrt{2}b\big)\big(c+\sqrt{2}d\big)\big)&=\sigma\big((ac+2bd)+\sqrt{2}(ad+bc)\big)=(ac+2bd)-\sqrt{2}(ad+bc)\\&=\big(a-\sqrt{2}b\big)\big(c-\sqrt{2}d\big)=\sigma\big(a+\sqrt{2}b\big)\sigma\big(c+\sqrt{2}d\big)\end{aligned}$$

handelt es sich um einen Ringhomomorphismus, der offensichtlich surjektiv ist und wegen

$$\sigma\big(a+\sqrt{2}b\big)=0\Leftrightarrow a-\sqrt{2}b=0\Leftrightarrow a=b=0\Leftrightarrow a+\sqrt{2}b=0\ (\text{wegen }\sqrt{2}\notin\mathbb{Q})$$

auch injektiv ist. Wendet man die obigen Rechnungen auf die Einschränkung von σ auf $\mathbb{Z}\big[\sqrt{2}\big]$ (die wir ebenfalls mit σ bezeichnen) an, so erkennt man, dass es sich bei

$$\sigma:\mathbb{Z}\big(\sqrt{2}\big)\to\mathbb{Z}\big(\sqrt{2}\big),\ \sigma\big(a+\sqrt{2}b\big)=a-\sqrt{2}b$$

ebenfalls um einen Ringautomorphismus handelt. Wegen $\varphi(a)=|a\cdot\sigma(a)|$ (mit $a\in\mathbb{Z}\big[\sqrt{2}\big]$) können wir die Abbildung σ nun als Ersatz für die komplexe Konjugation verwenden. Es seien $a=x+\sqrt{2}y$ und $b=u+\sqrt{2}v$ mit $x,y,u,v\in\mathbb{Z}$ und $b\neq 0$ (und daher $u^2-2v^2\neq 0$ und $\varphi(b)=\big|u^2-2v^2\big|>0$). Ist

$$\frac{a}{b}=\frac{x+\sqrt{2}y}{u+\sqrt{2}v}=\frac{\big(x+\sqrt{2}y\big)\big(u-\sqrt{2}v\big)}{\big(u+\sqrt{2}v\big)\big(u-\sqrt{2}v\big)}=s+\sqrt{2}t\in\mathbb{Q}\big(\sqrt{2}\big)$$

mit

$$s=\frac{xu-2yv}{u^2-2v^2}\in\mathbb{Q}\quad\text{und}\quad t=\frac{yu-xv}{u^2-2v^2}\in\mathbb{Q},$$

so wähle $m, n \in \mathbb{Z}$, derart dass $|s-m| \leq 1/2$ und $|t-n| \leq 1/2$. Setze $q = m + \sqrt{2}n$ und $r = a - bq$. Ist $r \neq 0$, so gilt

$$\begin{aligned}
\varphi(r) = |r \cdot \sigma(r)| &= |(a-bq)\sigma(a-bq)| = |b \cdot \sigma(b)| \cdot \Big|\Big(\frac{a}{b} - q\Big) \cdot \sigma\Big(\frac{a}{b} - q\Big)\Big| \\
&= |b \cdot \sigma(b)| \cdot \big|\big((s+\sqrt{2}t) - (m+\sqrt{2}n)\big) \cdot \sigma\big((s+\sqrt{2}t) - (m+\sqrt{2}n)\big)\big| \\
&= |b \cdot \sigma(b)\big| \cdot |\big((s-m) + \sqrt{2}(t-n)\big)\big((s-m) - \sqrt{2}(t-n)\big)\big| \\
&= |b \cdot \sigma(b)| \cdot \big|(s-m)^2 - 2(t-n)^2\big| \\
&\leq |b \cdot \sigma(b)| \cdot \max\big\{(s-m)^2, 2(t-n)^2\big\} \\
&\leq |b \cdot \sigma(b)| \cdot \max\big\{\tfrac{1}{4}, \tfrac{2}{4}\big\} = \tfrac{1}{2}\varphi(b) < \varphi(b).
\end{aligned}$$

6) Ein wichtiges Beispiel euklidischer Ringe, mit dem wir uns später ausführlicher beschäftigen werden, sind Polynomringe $K[X]$ mit Koeffizienten in einem Körper K. Ist $p \in K[X] \setminus \{0\}$ ein Polynom, so wählt man für $\varphi(p)$ den Grad des Polynoms p. Die Polynomdivision mit Rest zeigt, dass es sich um einen euklidischen Ring handelt.
7) Der Ring $\mathbb{Z}\big[i\sqrt{5}\big] = \{x + i\sqrt{5}y \mid x, y \in \mathbb{Z}\}$ (mit der üblichen Addition und Multiplikation komplexer Zahlen) ist kein euklidischer Ring, da er nicht faktoriell ist.
8) Die Umkehrung von Satz 138 gilt nicht. In der algebraischen Zahlentheorie zeigt man z.B., dass der Integritätsbereich

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + \frac{1+i\sqrt{19}}{2}b \,\middle|\, a, b \in \mathbb{Z}\right\}$$

(mit der üblichen Addition und Multiplikation komplexer Zahlen) ein Hauptidealbereich, aber kein euklidischer Ring ist.

Satz 139: Es sei R ein faktorieller Ring. Die Menge $\{\pi_i \mid i \in I\}$ enthalte aus jeder Äquivalenzklasse zueinander assoziierter irreduzibler Elemente von R genau einen Repräsentanten. (D.h. ist $p \in R$ irreduzibel, so $\exists! i \in I$, sodass p und π_i assoziiert sind.) Dann besitzt jedes $a \in R \setminus \{0\}$ eine Darstellung

$$a = u \prod_{i \in I} \pi_i^{\alpha_i}, \quad (*)$$

wobei $u \in R^*$, $\forall i \in I : \alpha_i \in \mathbb{N} \cup \{0\}$ und $\alpha_i = 0$ für alle bis auf endlich viele $i \in I$. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis: Existenz: Ist $a \in R^*$, so ist

$$a = a \prod_{i \in I} \pi_i^0$$

eine Darstellung wie in $(*)$.
Ist $a \notin R^*$, so gibt es nach Voraussetzung irreduzible $p_1, \dots, p_n \in R$, sodass $a = p_1 \cdots p_n$. Nun gilt:

$$\forall j \in \{1, \dots, n\}\ \exists i_j \in I : p_j \text{ ist zu } \pi_{i_j} \text{ assoziiert}$$

und daher

$$\forall j \in \{1, \dots, n\}\ \exists u_j \in R^* : p_j = u_j \pi_{i_j}.$$

Setzt man $u = u_1 \cdots u_n \in R^*$, so ist $a = u\pi_{i_1} \cdots \pi_{i_n}$. Durch Zusammenfassen erhält man nun eine Darstellung

$$a = u \prod_{k \in I} \pi_k^{\alpha_k},$$

wobei $\alpha_k = \big|\{j \in \{1, \dots, n\} \,\big|\, i_j = k\}\big|$.
Eindeutigkeit: Gegeben seien für ein $a \in R \setminus \{0\}$ nun zwei Darstellungen

$$a = u \prod_{i \in I} \pi_i^{\alpha_i} = v \prod_{i \in I} \pi_i^{\beta_i},$$

wie in $(*)$. Wir beweisen die Eindeutigkeit durch Induktion nach $\sum\limits_{i \in I} \alpha_i$. Ist $\sum\limits_{i \in I} \alpha_i = 0$, so muss auch $\sum\limits_{i \in I} \beta_i = 0$ gelten und $u = v$. Wäre nämlich $\sum\limits_{i \in I} \beta_i > 0$, so $\exists k \in I : \beta_k > 0$ und daher $\pi_k \mid a$, d.h. $\pi_k \mid u$. Da $u \mid 1$ folgt daraus $\pi_k \mid 1$ und $\pi_k \in R^*$, ein Widerspruch.
Ist $\sum\limits_{i \in I} \alpha_i > 0$, so $\exists k \in I : \alpha_k > 0$. Dann muss auch $\beta_k > 0$ gelten. Offenbar gilt

$$\pi_k \,\Big|\, v \prod_{i \in I} \pi_i^{\beta_i}.$$

Da π_k nach Satz 134 auch prim ist, folgt $\pi_k \mid v$ (und daher $\pi_k \in R^*$, ein Widerspruch) oder $\exists i \in I : \beta_i > 0$ und $\pi_k \mid \pi_i$. Wäre dabei $i \neq k$, so wären nach Satz 132 (viii) entweder π_k und π_i assoziiert (Widerspruch zur Voraussetzung) oder $\pi_k \in R^*$ (ebenfalls ein Widerspruch). Also ist $k = i$ und Anwendung von Lemma 50 liefert

$$u \prod_{i \in I} \pi_i^{\tilde{\alpha}_i} = v \prod_{i \in I} \pi_i^{\tilde{\beta}_i}$$

mit

$$\tilde{\alpha}_i = \begin{cases} \alpha_i & \text{für } i \neq k, \\ \alpha_k - 1 & \text{für } i = k \end{cases} \quad \text{und} \quad \tilde{\beta}_i = \begin{cases} \beta_i & \text{für } i \neq k, \\ \beta_k - 1 & \text{für } i = k. \end{cases}$$

Dabei ist offensichtlich $\sum\limits_{i \in I} \tilde{\alpha}_i = \sum\limits_{i \in I} \alpha_i - 1$. Nach Induktionsvoraussetzung ist daher $u = v$ und $\tilde{\alpha}_i = \tilde{\beta}_i\ \forall i \in I$, woraus sofort $\alpha_i = \beta_i\ \forall i \in I$ folgt.

Beispiel: Es bezeichne p_n die n-te Primzahl. Für jedes $n \in \mathbb{N} \setminus \{0\}$ wählt man nun ein $\pi_n \in \{-p_n, p_n\}$. Dann lässt sich jede ganze Zahl $k \in \mathbb{Z} \setminus \{0\}$ eindeutig als Produkt

$$k = u \prod_{n \geq 1} \pi_n^{\alpha_n}$$

mit $u \in \mathbb{Z}^* = \{-1, 1\}$ und $\alpha_n \geq 0$ schreiben, wobei $\alpha_n > 0$ nur für endlich viele $n \geq 1$. Die übliche Wahl ist dabei $\pi_n = p_n$ für alle $n \geq 1$, d.h. die normale Primfaktorzerlegung.

Lemma 140: Es sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Die Menge $\{\pi_i \mid i \in I\}$ sei wie in Satz 139. Sind

$$a = u \prod_{i \in I} \pi_i^{\alpha_i} \quad \text{und} \quad b = v \prod_{i \in I} \pi_i^{\beta_i}$$

Darstellungen wie in $(*)$ in Satz 139, so sind äquivalent:

(i) $a \mid b$,
(ii) $\alpha_i \leq \beta_i \ \forall i \in I$.

Beweis: (i) $\Rightarrow$ (ii) Nach Voraussetzung $\exists x \in R \setminus \{0\} : b = ax$. Ist

$$x = w \prod_{i \in I} \pi_i^{\xi_i}$$

die Darstellung wie in $(*)$ in Satz 139, so folgt

$$v \prod_{i \in I} \pi_i^{\beta_i} = b = ax = uw \prod_{i \in I} \pi_i^{\alpha_i + \xi_i}.$$

Aus der Eindeutigkeit der Darstellung erhält man $v = uw$ und $\beta_i = \alpha_i + \xi_i \geq \alpha_i \ \forall i \in I$.
(ii) $\Rightarrow$ (i) Setze

$$x = vu^{-1} \prod_{i \in I} \pi_i^{\beta_i - \alpha_i} \in R \setminus \{0\}.$$

Dann ist $ax = b$ und daher $a \mid b$.

Definition: Es sei R ein kommutativer Ring und $a_1, \ldots, a_n \in R$. Ein $d \in R$ heißt gemeinsamer Teiler von $a_1, \ldots, a_n$ wenn $d \mid a_i$ für $1 \leq i \leq n$.

Lemma 141: (i) In einem beliebigen kommutativen Ring R brauchen $a_1, \ldots, a_n \in R$ keine gemeinsamen Teiler zu besitzen.
(ii) Ist R ein kommutativer Ring mit Eins und $a_1, \ldots, a_n \in R$, so ist jedes $u \in R^*$ gemeinsamer Teiler von $a_1, \ldots, a_n$.

Beweis: (i) Das folgt sofort aus Lemma 130 (i), wo gezeigt wurde, dass bereits ein einziges Element eines beliebigen kommutativen Rings keine Teiler zu besitzen braucht.
(ii) Folgt sofort aus Lemma 130 (ii).

Definition: Es sei R ein kommutativer Ring und $a_1, \dots, a_n \in R$. Ein $d \in R$ heißt größter gemeinsamer Teiler von $a_1, \dots, a_n$ wenn die folgenden beiden Bedingungen erfüllt sind:

1) $d \mid a_i$ für $1 \leq i \leq n$ (d.h. d ist gemeinsamer Teiler von $a_1, \dots, a_n$),
2) Ist $x \in R$ und $x \mid a_i$ für $1 \leq i \leq n$, so folgt $x \mid d$
(d.h. jeder andere gemeinsame Teiler von $a_1, \dots, a_n$ teilt d).

Bemerkungen: 1) Nach dieser Definition ist der größte gemeinsame Teiler der Ringelemente $a_1, \dots, a_n \in R$ nicht eindeutig bestimmt, sondern die größten gemeinsamen Teiler von $a_1, \dots, a_n \in R$ bilden eine Menge.
2) Anders als in der elementaren Zahlentheorie (die den Fall $R = \mathbb{Z}$ behandelt), ist der größte gemeinsame Teiler von 12 und 18 beispielsweise nicht (nur) 6. Vielmehr sind sowohl 6 also auch -6 beides größte gemeinsame Teiler von 12 und 18, da sie beide die Eigenschaften 1) und 2) aus der Definition erfüllen.
3) In der elementaren Zahlentheorie schließt man den Fall $a_1 = \cdots = a_n = 0$ gewöhnlich aus, da man $\mathrm{ggT}(a_1, \dots, a_n) = \max\{d \in \mathbb{Z} \mid d \mid a_i \text{ für } 1 \leq i \leq n\}$ definiert und die Menge $\{d \in \mathbb{Z} \mid d \mid a_i \text{ für } 1 \leq i \leq n\}$ für $a_1 = \cdots = a_n = 0$ nach oben unbeschränkt ist. Dieser Fall ist in der obigen Definition aber nicht ausgeschlossen.

Lemma 142: Es sei R ein kommutativer Ring und $d_1 \in R$.
(i) Ist d_1 ein größter gemeinsamer Teiler von $a_1, \dots, a_n \in R$, so gilt für $d_2 \in R$, dass

d_2 ist ebenfalls größter gemeinsamer Teiler von $a_1, \dots, a_n \Leftrightarrow d_2$ ist zu d_1 assoziiert,

(ii) Ist R ein Integritätsbereich und d_1 ein größter gemeinsamer Teiler von $a_1, \dots, a_n \in R$, so gilt für $d_2 \in R$, dass

$$d_2 \text{ ist ebenfalls größter gemeinsamer Teiler von } a_1, \dots, a_n \Leftrightarrow \exists u \in R^* : d_2 = ud_1,$$

(iii) Haben $a_1, \dots, a_n \in R$ und $b_1, \dots, b_m \in R$ die selben gemeinsamen Teiler, so stimmen auch ihre größten gemeinsamen Teiler überein,
(iv) Sind $a_1, \dots, a_n \in R \setminus \{0\}$ und $a_{n+1} = \cdots = a_{n+k} = 0$, so haben $a_1, \dots, a_n$ und $a_1, \dots, a_{n+k}$ die selben größten gemeinsamen Teiler (d.h. man kann bei der Bestimmung der größten gemeinsamen Teiler von $a_1, \dots, a_\ell$ alle $a_i = 0$ außer Acht lassen),
(v) Sind $a_1 = \cdots = a_n = 0$, so ist 0 der einzige größte gemeinsame Teiler von $a_1, \dots, a_n$.

Beweis: (i) ($\Rightarrow$) Aus der Definition eines größten gemeinsamen Teilers folgt sofort $d_2 \mid d_1$ und $d_1 \mid d_2$, d.h. d_1 und d_2 sind assoziiert.

($\Leftarrow$) Aus $d_2 \mid d_1$ und $d_1 \mid a_i$ folgt $d_2 \mid a_i$ (für $1 \leq i \leq n$), d.h. d_2 ist ebenfalls ein gemeinsamer Teiler von $a_1, \dots, a_n$. Ist $c \in R$ ein gemeinsamer Teiler von $a_1, \dots, a_n$, so gilt $c \mid d_1$ und wegen $d_1 \mid d_2$ auch $c \mid d_2$, d.h. d_2 ist ebenfalls ein größter gemeinsamer Teiler von $a_1, \dots, a_n$.
(ii) Folgt sofort aus (i) und Satz 131 (viii).
(iii) Ist d ein größter gemeinsamer Teiler von $a_1, \dots, a_n$, so ist d nach Voraussetzung ein gemeinsamer Teiler von $b_1, \dots, b_m$. Ist $c \in R$ ein gemeinsamer Teiler von $b_1, \dots, b_m$ so ist c nach Voraussetzung auch gemeinsamer Teiler von $a_1, \dots, a_n$ und daher $c \mid d$, d.h. d ist auch größter gemeinsamer Teiler von $b_1, \dots, b_m$.
(iv) Da $d \mid 0$ für jedes $d \in R$ ist d genau dann gemeinsamer Teiler von $a_1, \dots, a_n$ wenn d gemeinsamer Teiler von $a_1, \dots, a_{n+k}$ ist. Die Behauptung folgt nun aus (iii).
(v) Aus $0 = a \cdot 0 \ \forall a \in R$ folgt sofort $a \mid 0 \ \forall a \in R$ (und insbesondere $0 \mid 0$). Im Fall $a_1 = \cdots = a_n = 0$ ist daher jedes $a \in R$ ein gemeinsamer Teiler von $a_1, \dots, a_n$. (Insbesondere ist 0 ein gemeinsamer Teiler von $a_1, \dots, a_n$.) Da $a \mid 0 \ \forall a \in R$ ist 0 sogar ein größter gemeinsamer Teiler von $a_1, \dots, a_n$. Ist nun $d \in R$ irgendein größter gemeinsamer Teiler von $a_1, \dots, a_n$, so muss nach der Definition auch $0 \mid d$ gelten. Daher $\exists x \in R : d = 0 \cdot x$ und daher $d = 0$. D.h. 0 ist der einzige größte gemeinsame Teiler von $a_1, \dots, a_n$.

Satz 143 (euklidischer Algorithmus): Es sei R ein euklidischer Ring (durch die Funktion $\varphi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$) und $a, b \in R$ mit $b \neq 0$. Man setzt $r_0 := b$ und führt folgendermaßen fortwährend Division mit Rest durch:

$$\begin{aligned}
a &= q_0 b + r_1 && \text{mit } r_1 \neq 0 \text{ und } \varphi(r_1) < \varphi(b), \\
b &= q_1 r_1 + r_2 && \text{mit } r_2 \neq 0 \text{ und } \varphi(r_2) < \varphi(r_1), \\
r_1 &= q_2 r_2 + r_3 && \text{mit } r_3 \neq 0 \text{ und } \varphi(r_3) < \varphi(r_2), \\
&\dots \\
r_k &= q_{k+1} r_{k+1} + r_{k+2} && \text{mit } r_{k+2} \neq 0 \text{ und } \varphi(r_{k+2}) < \varphi(r_{k+1}), \\
&\dots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && \text{mit } r_n \neq 0 \text{ und } \varphi(r_n) < \varphi(r_{n-1}), \\
r_{n-1} &= q_n r_n && \text{d.h. } n \geq 0 \text{ bezeichnet den kleinsten Index mit } r_{n+1} = 0.
\end{aligned}$$

Dann ist r_n ein größter gemeinsamer Teiler von a und b. (Insbesondere existiert in diesem Fall ein größter gemeinsamer Teiler.)

Beweis: Da

$$\varphi(b) = \varphi(r_0) > \varphi(r_1) > \varphi(r_2) > \cdots > \varphi(r_k) > \varphi(r_{k+1}) > \cdots \geq 0$$

und $\varphi(r_i) \in \mathbb{N} \cup \{0\}$ für $i \geq 0$ bricht der Algorithmus wie oben beschrieben ab.

Aus der letzten Gleichung $r_{n-1} = q_n r_n$ folgt $r_n \mid r_{n-1}$. Ist (für ein $k \leq n-2$) $r_n \mid r_{k+2}$ und $r_n \mid r_{k+1}$ schon gezeigt, so folgt aus $r_k = q_{k+1} r_{k+1} + r_{k+2}$ sofort $r_n \mid r_k$. Ist $r_n \mid r_2$ und $r_n \mid r_1$ schon gezeigt, so folgt aus $b = q_1 r_1 + r_2$, dass $r_n \mid b$ und aus $a = q_0 b + r_1$, dass $r_n \mid a$, d.h. r_n ist ein gemeinsamer Teiler von a und b. (Das ist auch für $n = 0$ richtig, da dann $r_1 = 0$ gilt und aus $a = q_0 b$ folgt, dass b ein gemeinsamer Teiler von a und b ist.) Angenommen $d \in R$ ist ein gemeinsamer Teiler von a und b. Aus der ersten Gleichung $r_1 = a - q_0 b$ folgt $d \mid r_1$ und aus $r_2 = b - q_1 r_1$ folgt $d \mid r_2$. Ist $r_n \mid r_k$ und $r_n \mid r_{k+1}$ schon gezeigt, so folgt aus $r_{k+2} = r_k - q_{k+1} r_{k+1}$ sofort $d \mid r_{k+2}$. Insbesondere erhält man zuletzt $d \mid r_n$, d.h. r_n ist ein größter gemeinsamer Teiler von a und b. (Das ist auch für $n = 0$ richtig, da $d \mid r_0$ nicht anderes als $d \mid b$ besagt und b in diesem Fall offensichtlich ein größter gemeinsamer Teiler von a und b ist.)

Satz 144: Es sei R ein faktorieller Ring und $a_1, \ldots, a_n \in R \setminus \{0\}$. Ist (für $1 \leq j \leq n$)

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Produktdarstellung von a_j wie in Satz 139, so sind genau die Elemente der Gestalt

$$u \prod_{i \in I} \pi_i^{\min\{\alpha_{i1}, \ldots, \alpha_{in}\}} \quad \text{mit } u \in R^* \text{ beliebig}$$

die größten gemeinsamen Teiler von $a_1, \ldots, a_n$. (Insbesondere existiert in diesem Fall ein größter gemeinsamer Teiler.)

Beweis: Es bezeichne

$$g = \prod_{i \in I} \pi_i^{\min\{\alpha_{i1}, \ldots, \alpha_{in}\}}.$$

Wir zeigen zunächst, dass g ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist. Aus $\min\{\alpha_{i1}, \ldots, \alpha_{in}\} \leq \alpha_{ij}$ $\forall i \in I$ $\forall j \in \{1, \ldots, n\}$ folgt $g \mid a_j$ für $1 \leq j \leq n$ (wegen Lemma 140), d.h. g ist ein gemeinsamer Teiler von $a_1, \ldots, a_n$. Ist b ein gemeinsamer Teiler von $a_1, \ldots, a_n$ (d.h. $b \mid a_j$ für $1 \leq j \leq n$) mit Darstellung

$$b = v \prod_{i \in I} \pi_i^{\beta_i}$$

wie in Satz 139, so folgt wegen $b \mid a_j$ (für $1 \leq j \leq n$), dass $\beta_i \leq \alpha_{ij}$ $\forall j \in \{1, \ldots, n\}$ $\forall i \in I$ (wegen Lemma 140) und daher $\beta_i \leq \min\{\alpha_{i1}, \ldots, \alpha_{in}\}$ $\forall i \in I$. Daraus folgt (wieder wegen Lemma 140) $b \mid g$, d.h. g ist ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$. Die Behauptung folgt nun aus Lemma 142 (ii).

Satz 145: Es sei R ein Hauptidealbereich und $a_1, \dots, a_n, d \in R$. Dann sind äquivalent:

(i) d ist ein größter gemeinsamer Teiler von $a_1, \dots, a_n$,

(ii) $(d) = (a_1) + \cdots + (a_n) (= Ra_1 + \cdots + Ra_n = (a_1, \dots, a_n))$.

Insbesondere gilt: Ist $d \in R$ ein größter gemeinsamer Teiler von $a_1, \dots, a_n$, so gibt es $x_1, \dots, x_n \in R$ mit der Eigenschaft $a_1x_1 + \cdots + a_nx_n = d$.

Beweis: (i) $\Rightarrow$ (ii) Da $d \mid a_i$ folgt $(a_i) \subseteq (d)$ für $1 \leq i \leq n$ (wegen Satz 131 (i)). Daher ist auch $(a_1) + \cdots + (a_n) \subseteq (d)$. Nach Lemma 71 ist $(a_1) + \cdots + (a_n)$ ein Ideal von R. Da R ein Hauptidealbereich ist, $\exists b \in R : (a_1) + \cdots + (a_n) = (b)$. Da dann $(a_i) \subseteq (b)$ und daher $b \mid a_i$ (wegen Satz 131 (i)) für $1 \leq i \leq n$, folgt nach Voraussetzung $b \mid d$ und daher $(d) \subseteq (b) = (a_1) + \cdots + (a_n)$.
(ii) $\Rightarrow$ (i) Für $1 \leq i \leq n$ ist $(a_i) \subseteq (a_1) + \cdots + (a_n) = (d)$ und daher $d \mid a_i$. Wenn $c \mid a_i$ für $1 \leq i \leq n$ für ein $c \in R$, so gilt auch $(a_i) \subseteq (c)$ für $1 \leq i \leq n$ und daher $(d) = (a_1) + \cdots + (a_n) \subseteq (c)$ und folglich $c \mid d$.

Bemerkung: Als Spezialfall erhält man die Beziehung $a\mathbb{Z} + b\mathbb{Z} = \mathrm{ggT}(a, b)\mathbb{Z}$ (für $a, b \in \mathbb{Z}$) aus der elementaren Zahlentheorie.

Definition: Es sei R ein kommutativer Ring mit Eins und $a_1, \dots, a_n \in R$. Man sagt, $a_1, \dots, a_n$ seien relativ prim (oder teilerfremd), wenn 1 ein größter gemeinsamer Teiler von $a_1, \dots, a_n$ ist.

Korollar 146: Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R \setminus \{0\}$. Ist

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Produktdarstellung von a_j wie in Satz 139 (für $1 \leq j \leq n$), so sind äquivalent:

(i) $a_1, \dots, a_n$ sind relativ prim,

(ii) $\min\{\alpha_{i1}, \dots, \alpha_{in}\} = 0 \ \forall i \in I$,

(iii) Die Menge der gemeinsamen Teiler von $a_1, \dots, a_n$ ist R^*.

Beweis: (i) $\Rightarrow$ (ii) Wenn $\exists i \in I : \min\{\alpha_{i1}, \dots, \alpha_{in}\} > 0$, dann $\alpha_{ij} \geq 1$ für $1 \leq j \leq n$ und daher $\pi_i \mid \alpha_j$ für $1 \leq j \leq n$. Dann kann 1 aber kein größter gemeinsamer Teiler von $a_1, \dots, a_n$ sein, da dann $\pi_i \mid 1$ und daher $\pi_i \in R^*$ gelten würde.
(ii) $\Rightarrow$ (iii) Nach Satz 144 ist die Menge der größten gemeinsamen Teiler von $a_1, \dots, a_n$ gerade R^*, insbesondere ist 1 ein größter gemeinsamer Teiler. Ist $d \in R$ ein gemeinsamer Teiler von $a_1, \dots, a_n$, so muss daher $d \mid 1$ und $d \in R^*$ gelten. Umgekehrt sind alle Elemente von R^* wegen Satz 130 (ii) gemeinsame Teiler von $a_1, \dots, a_n$.
(iii) $\Rightarrow$ (i) Klarerweise ist 1 ein gemeinsamer Teiler von $a_1, \dots, a_n$ und wird wegen der Voraussetzung von jedem anderen gemeinsamen Teiler geteilt.

Korollar 147: Es sei R ein Hauptidealbereich und $a_1, \dots, a_n \in R$. Dann sind äquivalent:

(i) $a_1, \dots, a_n$ sind relativ prim,
(ii) $R = (a_1) + \cdots + (a_n) (= Ra_1 + \cdots + Ra_n = (a_1, \dots, a_n))$,
(iii) $\exists x_1, \dots, x_n \in R : x_1a_1 + \cdots + x_na_n = 1$.

Beweis: (i) $\Rightarrow$ (ii) Aus Satz 145 folgt $(a_1) + \cdots + (a_n) = (1) = R$.
(ii) $\Rightarrow$ (iii) Trivial.
(iii) $\Rightarrow$ (i) Nach Lemma 130 (iii) gilt $1 \mid a_j$ für $1 \leq j \leq n$. Aus $d \mid a_j$ für $1 \leq j \leq n$ folgt $d \mid (x_1a_1 + \cdots + x_na_n)$, d.h. $d \mid 1$.

Korollar 148: Es sei R ein faktorieller Ring, $a, b, c \in R$ und a, c relativ prim. Dann folgt aus $a \mid bc$, dass $a \mid b$.

Beweis: Wäre $a = c = 0$, so wären a, c nicht relativ prim (wegen Lemma 142 (v)). Nach Voraussetzung $\exists x \in R : ax = bc$. Ist $a = 0$, so ist $0 = ax = bc$ und daher $b = 0$ oder $c = 0$. Da $c = 0$ unmöglich ist, gilt $b = 0$ und daher $a \mid b$. Ist $b = 0$, so gilt $a \mid b$ trivialerweise. Ist $c = 0$, so muss $a \neq 0$ sein. In diesem Fall ist a gemeinsamer Teiler von a und c und daher $a \mid 1$, d.h. $a \in R^*$ und daher $a \mid b$ wegen Lemma 130 (ii).
Ist $a \in R^*$, so gilt $b = a(a^{-1}b)$ und daher $a \mid b$. Ist $b \in R^*$, so gilt $bc \mid c$ (da $c = b^{-1}(bc)$) und daher $a \mid c$. D.h. a ist gemeinsamer Teiler von a und c und daher $a \mid 1$. Also ist $a \in R^*$ und wir haben schon gezeigt, dass daraus $a \mid b$ folgt. Ist $c \in R^*$, so folgt $axc^{-1} = b$ und daher $a \mid b$.
Es gelte nun $0 \notin \{a, b, c\}$ und $a, b, c \notin R^*$. Dann gibt es irreduzible

$$p_1, \dots, p_n, q_1, \dots, q_m, r_1, \dots, r_k \in R,$$

derart dass $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$ und $c = r_1 \cdots r_k$. Aus der Voraussetzung folgt sofort

$$p_1 \cdots p_n x = ax = bc = q_1 \cdots q_m r_1 \cdots r_k.$$

Wegen der Definition eines faktoriellen Rings ist jedes p_i (mit $1 \leq i \leq n$) entweder zu einem q_j (mit $1 \leq j \leq m$) oder einem r_ℓ (mit $1 \leq \ell \leq k$) assoziiert. Wäre p_i zu einem r_ℓ assoziiert, würde $p_i \mid a$ und $p_i \mid c$ folgen. Da a und c relativ prim sind, würde sich daraus $p_i \mid 1$ ergeben, ein Widerspruch. Also sind $p_1, \dots, p_n$ zu (jeweils verschiedenen) q_j (mit $1 \leq j \leq m$) assoziiert. Daraus folgt sofort $p_1 \cdots p_n \mid q_1 \cdots q_m$ und somit $a \mid b$.

Definition: Es sei R ein kommutativer Ring und $a_1, \dots, a_n \in R$. Ein $v \in R$ heißt gemeinsames Vielfaches von $a_1, \dots, a_n$ wenn $a_i \mid v$ für $1 \leq i \leq n$.

Bemerkungen: 1) Da $a_i \mid 0$ für $1 \leq i \leq n$, ist 0 stets ein gemeinsames Vielfaches von $a_1, \dots, a_n \in R$. Ebenso ist $a_1 \cdots a_n$ ein gemeinsames Vielfaches von $a_1, \dots, a_n \in R$.

2) Wenn es ein $i \in \{1, \dots, n\}$ gibt, für das $a_i = 0$ ist, ist 0 das einzige gemeinsame Vielfache von $a_1, \dots, a_n$ (denn $a_i \mid v \Rightarrow \exists x \in R : v = a_i x = 0 \cdot x = 0$).

Definition: Es sei R ein kommutativer Ring und $a_1, \dots, a_n \in R$. Ein $k \in R$ heißt kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$ wenn die folgenden beiden Bedingungen erfüllt sind:

1) $a_i \mid k$ für $1 \leq i \leq n$ (d.h. k ist gemeinsames Vielfaches von $a_1, \dots, a_n$),
2) Ist $x \in R$ und $a_i \mid x$ für $1 \leq i \leq n$, so folgt $k \mid x$
(d.h. k teilt jedes andere gemeinsame Vielfache von $a_1, \dots, a_n$).

Bemerkungen: 1) Wie beim größten gemeinsamen Teiler ist auch das kleinste gemeinsame Vielfache nicht eindeutig bestimmt, sondern die kleinsten gemeinsamen Vielfachen der Ringelemente $a_1, \dots, a_n \in R$ bilden eine Menge.
2) Anders als in der elementaren Zahlentheorie ist nicht nur 36 kleinstes gemeinsames Vielfaches von 12 und 18, sondern auch -36.

Lemma 149: Es sei R ein kommutativer Ring und $a_1, \dots, a_n, k_1 \in R$.
(i) Ist k_1 ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n \in R$, so gilt für $k_2 \in R$, dass
k_2 ist ebenfalls kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n \Leftrightarrow k_2$ ist zu k_1 assoziiert,
(ii) Ist R ein Integritätsbereich und k_1 ein kleinstes gemeinsames Vielfaches der Ringelemente $a_1, \dots, a_n \in R$, so gilt für $k_2 \in R$, dass

k_2 ist ebenfalls kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n \Leftrightarrow \exists u \in R^* : k_2 = uk_1$,

(iii) Gibt es ein $i \in \{1, \dots, n\}$, derart dass $a_i = 0$, so ist 0 das einzige kleinste gemeinsame Vielfache von $a_1, \dots, a_n$.

Beweis: (i) ($\Rightarrow$) Aus der Definition eines kleinsten gemeinsamen Vielfachen folgt sofort $k_1 \mid k_2$ und $k_2 \mid k_1$, d.h. k_1 und k_2 sind assoziiert.
($\Leftarrow$) Aus $k_1 \mid k_2$ und $a_i \mid k_1$ folgt $a_i \mid k_2$ (für $1 \leq i \leq n$), d.h. k_2 ist ebenfalls ein gemeinsames Vielfaches von $a_1, \dots, a_n$. Ist $c \in R$ ein gemeinsames Vielfaches von $a_1, \dots, a_n$, so gilt $k_1 \mid c$ und wegen $k_2 \mid k_1$ auch $k_2 \mid c$, d.h. k_2 ist ebenfalls ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$.
(ii) Folgt sofort aus (i) und Satz 131 (viii).
(iii) Wir haben uns schon oben überlegt, dass 0 in diesem Fall das einzige gemeinsame Vielfache von $a_1, \dots, a_n$ ist. Wegen $0 \mid 0$ ist es auch das einzige kleinste gemeinsame Vielfache.

Satz 150: Es sei R ein faktorieller Ring und $a_1, \dots, a_n \in R \setminus \{0\}$. Ist (für $1 \leq j \leq n$)

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Produktdarstellung von a_j wie in Satz 139, so sind genau die Elemente der Gestalt

$$u \prod_{i \in I} \pi_i^{\max\{\alpha_{i1}, \dots, \alpha_{in}\}} \quad \text{mit } u \in R^* \text{ beliebig}$$

die kleinsten gemeinsamen Vielfachen von $a_1, \dots, a_n$.

Beweis: Es bezeichne

$$k = \prod_{i \in I} \pi_i^{\max\{\alpha_{i1}, \dots, \alpha_{in}\}}.$$

Wir zeigen zunächst, dass k ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$ ist. Aus $\alpha_{ij} \leq \max\{\alpha_{i1}, \dots, \alpha_{in}\}\ \forall i \in I\ \forall j \in \{1, \dots, n\}$ folgt $a_j \mid k$ für $1 \leq j \leq n$ (wegen Lemma 140), d.h. k ist ein gemeinsames Vielfaches von $a_1, \dots, a_n$. Ist b ein gemeinsames Vielfaches von $a_1, \dots, a_n$ (d.h. $a_j \mid b$ für $1 \leq j \leq n$) mit Darstellung

$$b = v \prod_{i \in I} \pi_i^{\beta_i}$$

wie in Satz 139, so folgt wegen $a_j \mid b$ (für $1 \leq j \leq n$), dass $\alpha_{ij} \leq \beta_i\ \forall j \in \{1, \dots, n\}\ \forall i \in I$ (wegen Lemma 140) und daher $\max\{\alpha_{i1}, \dots, \alpha_{in}\} \leq \beta_i\ \forall i \in I$. Daraus folgt (wieder wegen Lemma 140) $k \mid b$, d.h. k ist ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$. Die Behauptung folgt nun aus Lemma 149 (ii).

Satz 151: Es sei R ein Hauptidealbereich und $a_1, \dots, a_n, k \in R$. Dann sind äquivalent:

(i) k ist ein kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$,
(ii) $(k) = (a_1) \cap \dots \cap (a_n)$.

Beweis: (i) $\Rightarrow$ (ii) Da $a_i \mid k$ folgt $(k) \subseteq (a_i)$ für $1 \leq i \leq n$ (wegen Satz 131 (i)). Daher ist auch $(k) \subseteq (a_1) \cap \dots \cap (a_n)$. Nach Lemma 55 (ii) ist $(a_1) \cap \dots \cap (a_n)$ ein Ideal von R. Da R ein Hauptidealbereich ist, $\exists b \in R : (a_1) \cap \dots \cap (a_n) = (b)$. Da dann $(b) \subseteq (a_i)$ und daher $a_i \mid b$ (wegen Satz 131 (i)) für $1 \leq i \leq n$, folgt nach Voraussetzung $k \mid b$ und daher $(a_1) \cap \dots \cap (a_n) = (b) \subseteq (k)$.
(ii) $\Rightarrow$ (i) Für $1 \leq i \leq n$ ist $(k) = (a_1) \cap \dots \cap (a_n) \subseteq (a_i)$ und daher $a_i \mid k$. Wenn $a_i \mid c$ für $1 \leq i \leq n$ für ein $c \in R$, so gilt auch $(c) \subseteq (a_i)$ für $1 \leq i \leq n$ und daher $(c) \subseteq (a_1) \cap \dots \cap (a_n) = (k)$ und folglich $k \mid c$.

Bemerkung: Als Spezialfall erhält man die Beziehung $(a\mathbb{Z}) \cap (b\mathbb{Z}) = \mathrm{kgV}(a, b)\mathbb{Z}$ (für $a, b \in \mathbb{Z}$) aus der elementaren Zahlentheorie.