2. Teilbarkeit in Integritätsbereichen

Wir wollen die elementaren Begriffe, die mit Teilbarkeit zu tun haben, vom Ring $\mathbb{Z}$ aller ganzen Zahlen auf allgemeinere Ringe übertragen. Daß dies nur für kommutative Ringe sinnvoll sein wird, ist klar (weil man sonst zwischen Teilbarkeit von links und von rechts unterscheiden müßte); ebenso, daß man die Existenz eines Einselements fordern muß (damit jedes Ringelement durch sich selbst teilbar ist, was wir von einem sinnvollen Teilbarkeitsbegriff sicher erwarten). Auch die Existenz von Nullteilern ist auszuschließen; wir werden also eine Teilbarkeitslehre nur für Integritätsbereiche entwickeln.

(2.1) Definition. *Es sei R ein Integritätsbereich.*

(a) *Es seien $a, b \in R$. Wir schreiben $a \mid b$, wenn es ein Element $r \in R$ gibt mit $b = ra$. Dies drücken wir durch die folgenden (äquivalenten) Sprechweisen aus: a* **teilt** *b bzw. a ist ein* **Teiler** *von b bzw. b ist* **teilbar** *durch a bzw. b ist ein* **Vielfaches** *von a.*

(b) *Ein Element d heißt* **gemeinsamer Teiler** *von $a_1, \ldots, a_n \in R$, wenn $d \mid a_i$ für $1 \leq i \leq n$ gilt.*

(c) *Ein Element g heißt* **größter gemeinsamer Teiler** *(ggT) von $a_1, \ldots, a_n \in R$, wenn g ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist und wenn $d \mid g$ für jeden gemeinsamen Teiler von $a_1, \ldots, a_n$ gilt.*

(d) *Ein Element d heißt* **gemeinsames Vielfaches** *von $a_1, \ldots, a_n \in R$, wenn $a_i \mid d$ für $1 \leq i \leq n$ gilt.*

(e) *Ein Element k heißt* **kleinstes gemeinsames Vielfaches** *(kgV) von $a_1, \ldots, a_n \in R$, wenn k ein gemeinsames Vielfaches von $a_1, \ldots, a_n$ ist und wenn $k \mid d$ für jedes gemeinsame Vielfache d von $a_1, \ldots, a_n$ gilt.*

(f) *Wir nennen $a_1, \ldots, a_n$* **teilerfremd**, *wenn 1 ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist.*

(2.2) Bemerkungen. (a) Das Nullelement spielt eine Sonderrolle. Es ist durch jedes Element teilbar, teilt selbst aber nur sich selbst. Wirklich sinnvolle Aussagen über Teilbarkeit kann man nur für von Null verschiedene Elemente erwarten.

(b) Gilt $a \mid b$ mit $a \neq 0$, so ist das Ringelement r mit $b = ra$ aufgrund der Nullteilerfreiheit von R eindeutig bestimmt; wir schreiben $r = b/a$.

(c) Bei der Definition *größter* gemeinsamer Teiler und *kleinster* gemeinsamer Vielfacher können wir nicht wie im Ring $\mathbb{Z}$ aller ganzen Zahlen eine Ordnungsrelation benutzen (die es in allgemeinen Integritätsbereichen ja gar nicht geben muß). Wir wählen eine Definition, die in allgemeinen Integritätsbereichen möglich ist und im Fall $\mathbb{Z}$ zur üblichen Definition äquivalent ist.

(d) Über die Existenz oder Eindeutigkeit größter gemeinsamer Teiler bzw. kleinster gemeinsamer Vielfacher ist durch die bloße Definition solcher Objekte noch nichts ausgesagt.

(2.3) Definition. *Zwei Elemente $a, b \in R$ eines Integritätsbereich heißen* **assoziiert**, *wenn sie sich nur um eine Einheit unterscheiden, wenn es also eine Einheit $u \in R^\times$ gibt mit $b = ua$. In diesem Fall schreiben wir $b \sim a$. Ein Teiler eines Elements r heißt* **echter Teiler**, *wenn er weder eine Einheit noch zu r assoziiert ist.*

(2.4) Bemerkung. Man prüft schnell nach, daß $\sim$ eine Äquivalenzrelation ist und daß $a \sim b$ genau dann gilt, wenn die Bedingungen $a \mid b$ und $b \mid a$ gelten.

(2.5) Satz. *Es sei R ein Integritätsbereich.*

(a) *Besitzen zwei Elemente $x, y \in R \setminus \{0\}$ ein kleinstes gemeinsames Vielfaches $[x, y]$, so besitzen sie auch einen größten gemeinsamen Teiler (x, y), und es gilt $xy \sim [x, y] \cdot (x, y)$.*

(b) *Besitzen je zwei Elemente in $R \setminus \{0\}$ einen größten gemeinsamen Teiler, dann besitzen auch je zwei Elemente in $R \setminus \{0\}$ ein kleinstes gemeinsames Vielfaches.*

Beweis. (a) Es sei $[x, y]$ ein kgV von x und y. Da xy ein gemeinsames Vielfaches von x und y ist, gibt es dann definitionsgemäß ein Element $d \in R$ mit $xy = d[x, y]$. Wir sind fertig, wenn wir zeigen können, daß d ein ggT von x und y ist. Dazu beweisen wir zunächst, daß d ein gemeinsamer Teiler von x und y ist, und dann, daß jeder andere gemeinsame Teiler von x und y schon d teilt.

• Da $[x, y]$ sowohl ein Vielfaches von x als auch ein Vielfaches von y ist, gibt es $x', y' \in R$ mit $[x, y] = xy' = x'y$. Dann gilt $xy = d[x, y] = dxy' = dx'y$. Durch Kürzen (das aufgrund der Nullteilerfreiheit von R erlaubt ist) erhalten wir dann $y = dy'$ und $x = dx'$. Also ist d ein gemeinsamer Teiler von x und y.

• Nun sei δ irgendein gemeinsamer Teiler von x und y; sagen wir $x = \delta x''$ und $y = \delta y''$. Dann ist $\delta x''y''$ ein gemeinsames Vielfaches von x und y und damit ein Vielfaches von $[x, y]$, sagen wir $\delta x''y'' = \lambda[x, y]$. Hieraus folgt $d[x, y] = xy = \delta^2 x''y'' = \delta\lambda[x, y]$, nach der Kürzungsregel also $d = \delta\lambda$. Also ist δ ein Teiler von d.

(b) Es seien $x, y \in R \setminus \{0\}$ beliebig. Nach Voraussetzung existiert dann ein größter gemeinsamer Teiler g von x und y, sagen wir $x = gx'$ und $y = gy'$, wobei x' und y' teilerfremd sind. Dann ist offensichtlich $gx'y'$ ein gemeinsames Vielfaches von x und y. Wir behaupten, daß $gx'y'$ sogar ein kgV von x und y ist.

Dazu sei m irgendein anderes gemeinsames Vielfaches von x und y. Nach Voraussetzung besitzen m und $gx'y'$ einen größten gemeinsamen Teiler d, sagen wir $gx'y' = \alpha d$ mit $\alpha \in R$. Da x und y gemeinsame Teiler von m und $gx'y'$ sind, sind sie auch Teiler von d, sagen wir $d = rx = sy$. Hieraus erhalten wir $x'y = gx'y' = \alpha d = \alpha sy$ (folglich $x' = \alpha s$) und $xy' = gx'y' = \alpha d = \alpha rx$ (folglich $y' = \alpha r$). Also teilt α sowohl x' als auch y', muß also (da x' und y' teilerfremd sind) eine Einheit sein. Daher ist $gx'y' = \alpha d \sim d$ ein Teiler von m. Jedes gemeinsame Vielfache m von x und y ist also ein Vielfaches von $gx'y'$, und das war zu zeigen. ∎

(2.6) Bemerkung. Es kann sein, daß es in einem Integritätsbereich R zwei Elemente in $R \setminus \{0\}$ gibt, die zwar einen größten gemeinsamen Teiler, aber kein kleinstes gemeinsames Vielfaches besitzen. Ein Beispiel dazu werden wir in den Übungen sehen.

Ein fundamentaler Satz der elementaren Zahlentheorie ist die Aussage, daß jede natürliche Zahl eine bis auf die Reihenfolge der Faktoren eindeutige Primfaktorzerlegung besitzt. Wir fragen nun, ob sich ähnliche Aussagen auch für allgemeinere Ringe gewinnen lassen. Dazu müssen wir zunächst definieren, wie der Begriff der Primzahl verallgemeinert werden soll. Wie die folgende Definition zeigt, gibt es dafür zwei Möglichkeiten.

(2.7) Definition. *Es sei R ein Integritätsbereich. Wir bezeichnen mit $R^\heartsuit$ die Menge derjenigen Elemente von R, die weder Null noch eine Einheit sind.*

(a) *Ein Element $p \in R$ heißt* **irreduzibel**, *wenn es in $R^\heartsuit$ liegt und keine echten Teiler besitzt, sondern nur solche Teiler, die entweder invertierbar oder aber zu p assoziiert sind.*

(b) *Ein Element $p \in R$ heißt* **prim**, *wenn es in $R^\heartsuit$ liegt und die folgende Bedingung erfüllt: gilt $p \mid ab$, dann gilt $p \mid a$ oder $p \mid b$.*

(2.8) Bemerkung. Die Menge $R^\heartsuit$ ist sozusagen das "Herz" des Rings R, weil das Nullelement und die Einheiten unter vielen Gesichtspunkten uninteressant sind, aber weder diese Bezeichnung noch das Symbol $R^\heartsuit$ ist üblich. Daß man Einheiten nicht als irreduzibel oder prim bezeichnet, entspricht der Konvention, die Zahl 1 nicht zu den Primzahlen zu zählen. Im Fall der ganzen Zahlen fallen die Begriffe "irreduzibel" und "prim" zusammen; in allgemeineren Ringen ist das nicht mehr der Fall, wie wir noch sehen werden.

(2.9) Satz. *Es sei R ein Integritätsbereich.*

(a) *Es sei p' assoziiert zu p. Ist p irreduzibel, dann auch p'. Ist p prim, dann auch p'.*

(b) *Ist p prim und gilt $p \mid a_1 \cdots a_n$, so gibt es (mindestens) einen Index $1 \le i \le n$ mit $p \mid a_i$.*

(c) *Gilt $p_1 \cdots p_m = q_1 \ldots q_n$ mit Primelementen p_i und q_j, so gilt $m = n$, und es gibt eine Permutation $\sigma \in \mathrm{Sym}_n$ derart, daß jeweils q_i mit $p_{\sigma(i)}$ assoziiert ist. (Eine Darstellung eines Elements als Produkt von Primelementen ist also immer eindeutig bis auf die Reihenfolge der Faktoren und die Multiplikation mit Einheiten.)*

(d) *Jedes Primelement ist irreduzibel.*

Beweis. Aussage (a) folgt sofort aus den Definitionen, Aussage (b) ergibt sich mit Induktion über n aus der Definition des Begriffs "prim". Aussage (c) kann mit Induktion über $m + n$ bewiesen werden (Übungsaufgabe!). Zum Nachweis von (d) betrachten wir ein Primelement p und eine Faktorisierung $p = ab$; wir müssen zeigen, daß a oder b eine Einheit ist. Aus $p = ab$ folgt $p \mid ab$ und damit $p \mid a$ oder $p \mid b$; o.B.d.A. gelte $p \mid a$. Andererseits gilt auch $a \mid p$; also sind a und p assoziiert. Folglich ist b eine Einheit. ∎

(2.10) Definition. *Ein Integritätsbereich R, in dem jedes Element $x \in R^\heartsuit$ eine Zerlegung in irreduzible Faktoren besitzt, heißt* **Faktorisierungsbereich**. *Ein Faktorisierungsbereich, in dem jede Zerlegung in irreduzible Faktoren im wesentlichen eindeutig ist (also eindeutig bis auf die Reihenfolge der Faktoren und Multiplikation mit Einheiten) heißt ein* **faktorieller Ring**.

(2.11) Bemerkung. Die Bezeichnung "Faktorisierungsbereich" ist eine ad-hoc-Bezeichnung; es scheint keine allgemein übliche Bezeichnung zu geben. (Zuweilen findet sich die Bezeichnung "atomarer Ring".) Der Begriff "faktorieller Ring" ist synonym mit dem Begriff "ZPE-Ring" ("Zerlegung in Primfaktoren ist eindeutig"); im Englischen ist die Bezeichnung "unique factorization domain" (UFD) üblich.

(2.12) Satz. *Für einen Faktorisierungsbereich R sind die folgenden Bedingungen äquivalent:*

(1) *R ist faktoriell;*

(2) *je n Elemente $a_1, \ldots, a_n \in R$ besitzen einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches;*

(3) *je n Elemente $a_1, \ldots, a_n \in R$ besitzen einen größten gemeinsamen Teiler;*

(4) *immer dann, wenn $a_1, \ldots, a_n \in R$ einen größten gemeinsamen Teiler g besitzen und $b \in R$ beliebig ist, ist gb ein größter gemeinsamer Teiler von $a_1 b, \ldots, a_n b$;*

(5) *jedes irreduzible Element in R ist prim;*

(6) *jedes Element von $R^\heartsuit$ ist als Produkt von Primelementen darstellbar.*

Beweis. (1)⇒(2): Es seien $a_1, \ldots, a_n$ beliebig. Gilt $a_i = 0$ für alle i, so ist 0 sowohl ein ggT als auch ein kgV von $a_1, \ldots, a_n$. Ansonsten dürfen wir bei Bildung von ggT und kgV die von Null verschiedenen Elemente a_i weglassen. Wir dürfen daher $a_i \neq 0$ für alle i annehmen. Nach Voraussetzung gibt es Einheiten $u_i \in R$, irreduzible Elemente $p_i \in R$ und Exponenten $\nu_{ij} \ge 0$ mit

$$\begin{aligned} a_1 &= u_1 p_1^{\nu_{11}} p_2^{\nu_{12}} \cdots p_k^{\nu_{1k}}, \\ a_2 &= u_2 p_1^{\nu_{21}} p_2^{\nu_{22}} \cdots p_k^{\nu_{2k}}, \\ &\vdots \\ a_n &= u_n p_1^{\nu_{n1}} p_2^{\nu_{n2}} \cdots p_k^{\nu_{nk}}. \end{aligned}$$

Wir setzen jetzt $m_i := \min(\nu_{1i}, \nu_{2i}, \ldots, \nu_{ni})$ und $M_i := \max(\nu_{1i}, \nu_{2i}, \ldots, \nu_{ni})$; es ist dann leicht nachzuprüfen, daß $g := p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ ein ggT und $k := p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k}$ ein kgV der Elemente $a_1, \ldots, a_n$ ist.

(2)⇒(3): Diese Aussage gilt trivialerweise.

(3)⇒(4): Es seien g ein ggT von $a_1, \ldots, a_n$ und $b \in R$ beliebig. Für $b = 0$ gilt die Behauptung trivialerweise; wir dürfen also $b \neq 0$ voraussetzen. Nach Voraussetzung besitzen $a_1 b, \ldots, a_n b$ einen ggT, sagen wir g'. Da gb alle Elemente ga_i teilt, ist gb ein Teiler von g', sagen wir $g' = xgb$ mit $x \in R$. Da g' die Elemente $a_1 b, \ldots, a_n b$ teilt, teilt xg die Elemente $a_1, \ldots, a_n$ und damit auch deren größten gemeinsamen Teiler g, sagen wir $g = (xg)y = xyg$ mit $y \in R$. Hieraus folgt $xy = 1$, so daß x eine Einheit ist. Also unterscheiden sich g' und gb nur um eine Einheit; da g' ein größter gemeinsamer Teiler von $a_1 b, \ldots, a_n b$ ist, ist also auch gb ein solcher.

(4)⇒(5): Es sei p irreduzibel. Um p als prim nachzuweisen, müssen wir zeigen, daß aus $p \mid ab$ und $p \nmid a$ schon $p \mid b$ folgt. Wir setzen also $p \mid ab$ und $p \nmid a$ voraus. Die Elemente p und a sind teilerfremd. (Besäßen sie einen gemeinsamen Teiler, der keine Einheit ist, so müßte dieser wegen der Irreduzibilität von p zu p assoziiert sein; dann müßte aber auch $p \mid a$ gelten.) Also ist 1 ein ggT von p und a. Wegen (4) ist dann b ein ggT von pb und ab. Als gemeinsamer Teiler von pb und ab teilt dann p diesen ggT; also gilt $p \mid b$, was zu zeigen war.

(5)⇒(6): Da R als Faktorisierungsbereich vorausgesetzt wurde, ist die Existenz einer Zerlegung eines Elements in irreduzible Elemente von vornherein gegeben. Da nach Voraussetzung jedes irreduzible Element prim ist, folgt die Behauptung.

(6)⇒(1): Diese Implikation gilt, weil nach (2.9)(d) jedes Primelement irreduzibel ist und weil eine Faktorisierung in Primelemente gemäß (2.9)(c) im wesentlichen eindeutig ist. ∎

(2.13) Satz. *Ein Integritätsbereich, in dem es keine nichtabbrechende und strikt aufsteigende Folge*

$$\langle\langle x_1 \rangle\rangle \subsetneqq \langle\langle x_2 \rangle\rangle \subsetneqq \langle\langle x_3 \rangle\rangle \subsetneqq \cdots$$

von Hauptidealen gibt, ist zwangsläufig ein Faktorisierungsbereich.

Beweis. Wir nehmen an, R sei kein Faktorisierungsbereich. Es gibt dann ein Element $x \in R^\heartsuit$ ohne Zerlegung in irreduzible Faktoren. Insbesondere ist dann $x_1 := x$ nicht selbst irreduzibel, besitzt also eine Zerlegung in zwei echte Faktoren. Besäßen beide Faktoren eine Zerlegung in irreduzible Faktoren, so würde auch x_1 eine solche Zerlegung besitzen; also muß mindestens ein echter Teiler x_2 von x_1 existieren, der keine Zerlegung in irreduzible Faktoren besitzt. Das gleiche Argument können wir nun auf x_2 statt auf x_1 anwenden. Iteration des Arguments liefert dann eine Idealkette $\langle\langle x_1 \rangle\rangle \subsetneqq \langle\langle x_2 \rangle\rangle \subsetneqq \langle\langle x_3 \rangle\rangle \subsetneqq \cdots$. ∎

(2.14) Bemerkung. Die Umkehrung von Satz (2.13) ist falsch: Es gibt Faktorisierungsbereiche, in denen es unbegrenzt wachsende Ketten von Hauptidealen gibt. (Siehe Anne Grams, *Atomic rings and the ascending chain condition for principal ideals*, Proceedings of the Cambridge Philosophical Society **75** (3), Mai 1974, S. 321-320.)

Wir kennen jetzt einige Charakterisierungen faktorieller Ringe, aber noch kein handliches Kriterium, mit dem wir nachweisen könnten, daß ein gegebener Ring faktoriell ist. Der nächste Satz liefert ein solches Kriterium.

(2.15) Satz. *Der Ring R sei ein Integritätsbereich und gleichzeitig ein Hauptidealring (d.h., jedes Ideal von R sei ein Hauptideal). Dann gelten die folgenden Aussagen.*

(a) *Je n Elemente $a_1, \ldots, a_n \in R$ besitzen einen größten gemeinsamen Teiler, und g ist ein solcher größter gemeinsamer Teiler genau dann, wenn gilt*

$$\langle\langle g \rangle\rangle \;=\; \langle\langle a_1, \ldots, a_n \rangle\rangle.$$

(b) *Der Ring R ist faktoriell.*

Beweis. (a) Es seien $a_1, \ldots, a_n \in R$ beliebig. Nach Voraussetzung ist das Ideal $\langle\langle a_1, \ldots, a_n \rangle\rangle$ ein Hauptideal, sagen wir $\langle\langle a_1, \ldots, a_n \rangle\rangle = \langle\langle g \rangle\rangle$. Dann gilt insbesondere $a_i \in \langle\langle g \rangle\rangle = Rg$ für alle i, so daß g ein gemeinsamer Teiler der Elemente a_i ist. Ist d irgendein anderer gemeinsamer Teiler der Elemente a_i, so liegt jedes der Elemente a_i in Rd, folglich gilt $\langle\langle a_1, \ldots, a_n \rangle\rangle \subseteq Rd$, also $\langle\langle g \rangle\rangle \subseteq Rd$ und damit $g \in Rd$, so daß d ein Teiler von g ist. Damit ist g als größter gemeinsamer Teiler von $a_1, \ldots, a_n$ nachgewiesen. Da je zwei größte gemeinsame Teiler von $a_1, \ldots, a_n$ assoziiert sind und assoziierte Elemente das gleiche Ideal erzeugen, charakterisiert die Bedingung $\langle\langle x \rangle\rangle = \langle\langle a_1, \ldots, a_n \rangle\rangle$ schon die größten gemeinsamen Teiler x von $a_1, \ldots, a_n$.

(b) Es sei $Rx_1 \subseteq Rx_2 \subseteq Rx_3 \subseteq$ eine aufsteigende Familie von Hauptidealen. Dann ist $I := \bigcup_{k=1}^{\infty} Rx_k$ wieder ein Ideal (warum?), nach Voraussetzung also ein Hauptideal, sagen wir $I = Rx$. Dann gilt aber $x \in Rx_N$ für ein $N \in \mathbb{N}$, folglich $x \in Rx_n$ für alle $n \geq N$ und damit $Rx_n = Rx$ für alle $n \geq N$. Jede aufsteigende Kette von Hauptidealen in R wird also stationär; nach (2.13) ist daher R ein Faktorisierungsbereich. Wegen Satz (2.12) und Teil (a) ist dann R sogar ein faktorieller Ring. ∎

(2.16) Bemerkung. Es sei g ein ggT von $a_1, \ldots, a_n$. Die Tatsache, daß g in $\langle\langle a_1, \ldots, a_n \rangle\rangle = Ra_1 + \cdots + Ra_n$ liegt, bedeutet, daß sich g in der Form $g = r_1 a_1 + \cdots + r_n a_n$ mit Ringelementen r_i darstellen läßt. Jede solche Darstellung bezeichnet man als **lineare Darstellung des ggT**.

Beispielsweise sind der Ring $\mathbb{Z}$ aller ganzen Zahlen und der Polynomring $K[X]$ über einem Körper K Hauptidealringe (und damit faktoriell), wie man schnell mit dem Euklidischen Algorithmus sieht. Der Euklidische Algorithmus stellt sich dabei als so wichtig heraus, daß es sich lohnt, ihn auf allgemeinere Ringe zu übertragen.

(2.17) Definition. *Ein Integritätsbereich R heißt ein* **Euklidischer Ring**, *wenn es eine Funktion $d : R \setminus \{0\} \to \mathbb{N}$ derart gibt, daß für alle $a, b \in R \setminus \{0\}$ die folgenden Bedingungen gelten:*

(1) *gilt $a \mid b$, so gilt $d(a) \leq d(b)$;*

(2) *gilt $a \nmid b$, so gibt es Elemente $q \in R$ und $r \in R \setminus \{0\}$ mit $b = qa + r$ und $d(r) < d(a)$ (Division mit Rest).*

Jede solche Funktion heißt eine **Gradfunktion** *für R.*

(2.18) Beispiele. (a) Ist $R = \mathbb{Z}$, so kann man $d(a) = |a|$ wählen.

(b) Ist $R = K$ ein beliebiger Körper, so ist $d \equiv 1$ eine Gradfunktion für R.

(c) Ist $R = K[X]$ der Polynomring über einem Körper K, so ist durch $d(p) :=$ Grad von p eine Gradfunktion gegeben.

(d) Es sei $R = \mathbb{Z}[i]$ der Ring aller Gaußschen ganzen Zahlen. Dann ist durch $d(z) := |z|^2$ eine Gradfunktion auf R gegeben.

(2.19) Bemerkung. Wir wollen in (2.18)(d) nachweisen, daß die angegebene Funktion d eine Gradfunktion ist. Es seien $a, b \in R \setminus \{0\}$ gegeben. Gilt $b = qa$ mit $q \neq 0$, so folgt $d(b) = d(qa) = d(q)d(a) \geq d(a)$, so daß (2.17)(1) erfüllt ist. Zum Nachweis von (2.17)(2) seien $a, b \in \mathbb{Z} + i\mathbb{Z}$ mit $a \nmid b$ gegeben. Wir müssen q und r wie in (2.17)(2) finden.

Erster Fall: $a = n \in \mathbb{N}$. Wir schreiben $b = b_1 + ib_2$ mit ganzen Zahlen $b_i \in \mathbb{Z}$. Es gibt dann ganze Zahlen q_i und r_i mit $b_i = q_i n + r_i$ mit $|r_i| \leq n/2$. Mit $q := q_1 + iq_2$ und $r := r_1 + ir_2$ haben wir dann $b = qn + r = qa + r$ mit $d(r) = r_1^2 + r_2^2 \leq (n/2)^2 + (n/2)^2 < n^2 = d(a)$.

Zweiter Fall: $a \neq 0$ beliebig. Setze $n := a\overline{a}$. Nach dem gerade behandelten Spezialfall, angewandt auf $b\overline{a}$ statt auf b, gibt es $q, \rho \in \mathbb{Z}[i]$ mit $b\overline{a} = q \cdot a\overline{a} + \rho$ mit $d(\rho) < d(a\overline{a})$. Dann gilt $\rho = b\overline{a} - qa\overline{a} = (b - qa)\overline{a}$, folglich

$$d(b - qa)d(\overline{a}) \;=\; d(\rho) \;<\; d(a\overline{a}) \;=\; d(a)d(\overline{a})$$

und damit $d(b - qa) < d(a)$. Setzen wir also $r := b - qa$, so haben wir $b = qa + r$ mit $d(r) < d(a)$. ∎

(2.20) Satz. *Jeder Euklidische Ring ist ein Hauptidealring (und damit faktoriell).*

Beweis. Es sei $I \neq \{0\}$ ein Ideal in einem Euklidischen Ring R. Wähle in I ein Element $x \neq 0$ mit minimalem Wert $d(x)$. Wir wollen zeigen, daß dann $I = \langle\langle x \rangle\rangle$ gilt. Dazu sei $y \in I$ beliebig. Wäre y nicht durch x teilbar, so gäbe es $q, r \in R$ mit $y = qx + r$, $r \neq 0$ und $d(r) < d(x)$. Wegen $r = y - qx \in I - I = I$ widerspräche dies aber der Minimalität von $d(x)$. Also ist y durch x teilbar; es gilt daher $y \in Rx = \langle\langle x \rangle\rangle$. ∎

Um den Nutzen der entwickelten Theorie zu demonstrieren, wollen wir nun die auf Pascal zurückgehende Behauptung beweisen, daß sich eine Primzahl der Form $4n+1$ stets als Summe zweier Quadrate darstellen läßt. Zur Vorbereitung benötigen wir das folgende Ergebnis.

(2.21) Satz von Wilson. *Für jede Primzahl p gilt $(p-1)! \equiv -1$ modulo p; d.h., $(p-1)!+1$ ist durch p teilbar.*

Beweis. In $\mathbb{Z}_p$ ist $x^2 = 1$ äquivalent zu $0 = x^2 - 1 = (x-1)(x+1)$ und damit zu $x = \pm 1$. Kein Element von $\mathbb{Z}_p^\times$ außer ± 1 ist also invers zu sich selbst. Die Elemente von $Z_p^\times \setminus \{\pm 1\}$ treten also in Paaren (ξ, ξ^{-1}) auf. Bezeichnen wir mit $[a]$ die Restklasse einer Zahl $a \in \mathbb{Z}$ modulo p, so gilt also

$$[(p-1)!] \;=\; \prod_{\xi \in \mathbb{Z}_p^\times} \xi \;=\; [1] \cdot [-1] \;=\; [-1].$$

Dies ist schon die Behauptung. ∎

Der folgende Satz ist ein schönes Beispiel dafür, wie abstrakte mathematische Strukturen eingesetzt werden, um elementar formulierbare zahlentheoretische Aussagen zu beweisen. Es soll gezeigt werden, daß eine Primzahl p genau dann als Summe zweier Quadrate darstellbar ist, wenn sie von der Form $p = 4n + 1$ ist. Zur Formulierung dieser Aussage benötigt man nur Grundbegriffe der natürlichen Zahlen; der Beweis benutzt aber den Ring der Gaußschen ganzen Zahlen, also eine viel abstraktere mathematische Struktur.

(2.22) Satz. *Für eine ungerade Primzahl p sind die folgenden Aussagen äquivalent:*

(1) *es gibt $a, b \in \mathbb{N}$ mit $p = a^2 + b^2$;*
(2) *es gilt $p \equiv 1$ modulo 4;*
(3) *es gibt eine Zahl $x \in \mathbb{N}$ mit $x^2 \equiv -1$ modulo p.*

Beweis. (1)⇒(2): Für eine beliebige Zahl $x \in \mathbb{N}$ gilt $x^2 \equiv 0$ oder $x^2 \equiv 1$ modulo 4. Für je zwei Zahlen $a, b \in \mathbb{N}$ gilt daher $a^2 + b^2 \equiv 0, 1, 2$ modulo 4, jedenfalls nicht $a^2 + b^2 \equiv 3$ modulo 4. Primzahlen p mit $p \equiv 3$ modulo 4 sind also nicht in der Form $p = a^2 + b^2$ darstellbar.

(2)⇒(3): Nach Voraussetzung hat p die Form $p = 4n + 1$ mit $n \in \mathbb{N}$. Daher ist

$$(p-1)! \;=\; 1 \cdot 2 \cdot \ldots \cdot 2n \cdot (p-2n) \cdot \ldots \cdot (p-2) \cdot (p-1).$$

Modulo p gilt daher

$$\begin{aligned}(p-1)! \;&\equiv\; 1 \cdot 2 \cdot \ldots \cdot 2n \cdot (-2n) \cdot \ldots \cdot (-2) \cdot (-1) \\ &=\; 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot \ldots \cdot (2n) \cdot (-2n) \\ &=\; 1^2 \cdot 2^2 \cdot \ldots \cdot (2n)^2 \;=\; (1 \cdot 2 \cdot \ldots \cdot 2n)^2,\end{aligned}$$

wobei der Übergang von der zweiten zur dritten Zeile gilt, weil die Anzahl der Minuszeichen gleich $2n$ und damit gerade ist. Mit $x := 1 \cdot 2 \cdot \ldots \cdot 2n$ gilt also $(p-1)! \equiv x^2$ modulo p. Nach dem Satz von Wilson gilt andererseits $(p-1)! \equiv -1$ modulo p, damit also $x^2 \equiv -1$ modulo p.

(3)⇒(1): Nach Voraussetzung gibt es eine Zahl $x \in \mathbb{N}$ mit $p \mid x^2 + 1$ in $\mathbb{Z}$. Erst recht gilt also $p \mid x^2 + 1 = (x + i)(x - i)$ im Ring $\mathbb{Z}[i]$ der Gaußschen ganzen Zahlen. Andererseits gilt offensichtlich $p \nmid x + i$ und $p \nmid x - i$ in $\mathbb{Z}[i]$. Also ist p kein Primelement in $\mathbb{Z}[i]$. Da $\mathbb{Z}[i]$ ein faktorieller Ring ist, ist p damit auch nicht irreduzibel in $\mathbb{Z}[i]$. Es gibt also Elemente $\alpha, \beta \in \mathbb{Z}[i]$, die keine Einheiten sind, mit $p = \alpha\beta$. Ist N die Normabbildung von $\mathbb{Z}[i]$, so folgt hieraus $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$ in $\mathbb{N}$. Da α und β keine Einheiten sind, sind $N(\alpha)$ und $N(\beta)$ von 1 verschieden; die Gleichung $p^2 = N(\alpha)N(\beta)$ erzwingt dann $N(\alpha) = N(\beta) = p$. Schreiben wir $\alpha = a + ib$ mit $a, b \in \mathbb{Z}$, so haben wir also $p = N(\alpha) = a^2 + b^2$. Damit ist p als Summe zweier Quadrate dargestellt. ∎