Vorlesung „Algebra und Zahlentheorie“

– Leitfaden –

1 Zahlentheorie in $\mathbb{Z}$

Bezeichnungen: $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ (ganze Zahlen) und $\mathbb{N} := \{1, 2, 3, \ldots\}$ (natürliche Zahlen ohne die Null)

1.1 Teilbarkeit

Definition 1.1.1. Eine Zahl $d \in \mathbb{Z}$ heißt *Teiler von* $a \in \mathbb{Z}$, wenn es eine Zahl $c \in \mathbb{Z}$ gibt mit $a = d \cdot c\,(= c \cdot d)$. Wir sagen auch „*d teilt a*“ oder „*a ist Vielfaches von d*“ und schreiben verkürzt:

$$d \mid a.$$

Ist d *kein* Teiler von a, so schreiben wir auch: $d \nmid a$.

Beispiel 1.1.2.

- $4 \mid 12$ *(da* $12 = 4 \cdot 3$*)*, $-7 \mid 56$ *(da* $56 = (-7) \cdot (-8)$*)*, $7 \mid -56$ *(da* $-56 = 7 \cdot (-8)$*)*, $4 \nmid 9$ *(9 kann keinen geraden Teiler besitzen, da sonst 9 gerade wäre)*, $12 \mid 0$ *(da* $0 = 12 \cdot 0$*) und* $0 \mid 0$ *(da* $0 = 0 \cdot c$ *für jede ganze Zahl c)*

- *Sei* $a \in \mathbb{Z}$ *und* $n \in \mathbb{N}$*. Dann gilt:* $(a-1) \mid (a^n - 1)$*, denn:*

$$a^n - 1 = (a-1) \cdot \underbrace{(a^{n-1} + \ldots + a^2 + a + 1)}_{\in \mathbb{Z}}$$

Lemma 1.1.3 (Rechenregeln für Teilbarkeit)**.** *Seien* $a, b, c, d \in \mathbb{Z}$*.*

1. *Es gilt immer:* $a \mid a$*.*
2. *Gilt* $a \mid b$ *und* $b \mid c$*, so gilt auch* $a \mid c$*.*
3. *Gilt* $a \mid b$ *und* $c \mid d$*, so gilt auch* $a \cdot c \mid b \cdot d$*.*
4. *Gilt* $a \mid b$ *und* $a \mid c$*, so gilt auch* $a \mid (x \cdot b + y \cdot c)$ *für alle* $x, y \in \mathbb{Z}$*.*

Beweis. (Im Prinzip muss man immer nur die Definition der Teilbarkeit ausnutzen (und wenige Rechenregeln in den ganzen Zahlen).)

1. $a = a \cdot 1$

2. $a \mid b$, also gibt es ein $e \in \mathbb{Z}$ mit $b = a \cdot e$.
   $b \mid c$, also gibt es ein $f \in \mathbb{Z}$ mit $c = b \cdot f$.
   Einsetzen der ersten Gleichung in die zweite liefert: $c = a \cdot \underbrace{e \cdot f}_{\in \mathbb{Z}, \text{ da } e,f \in \mathbb{Z}}$.
   Also gilt: $a \mid c$.

3. $a \mid b$, also gibt es ein $e \in \mathbb{Z}$ mit $b = a \cdot e$.
   $c \mid d$, also gibt es ein $f \in \mathbb{Z}$ mit $d = c \cdot f$.
   Also ist $b \cdot d = a \cdot e \cdot c \cdot f = a \cdot c \cdot \underbrace{e \cdot f}_{\in \mathbb{Z}, \text{ da } e,f \in \mathbb{Z}}$. (Bei der zweiten Gleichung haben wir benutzt, dass die Multiplikation in den ganzen Zahlen kommutativ ist.)
   Also gilt: $a \cdot c \mid b \cdot d$.

4. $a \mid b$, also gibt es ein $e \in \mathbb{Z}$ mit $b = a \cdot e$.
   $a \mid c$, also gibt es ein $f \in \mathbb{Z}$ mit $c = a \cdot f$.
   Dann ist $x \cdot b + y \cdot c = x \cdot a \cdot e + y \cdot a \cdot f = a \cdot x \cdot e + a \cdot y \cdot f = a \cdot \Big(\underbrace{\underbrace{\underbrace{x}_{\in \mathbb{Z}} \cdot \underbrace{e}_{\in \mathbb{Z}}}_{\in \mathbb{Z}} + \underbrace{\underbrace{y}_{\in \mathbb{Z}} \cdot \underbrace{f}_{\in \mathbb{Z}}}_{\in \mathbb{Z}}}_{\in \mathbb{Z}} \Big)$.
   (Bei der zweiten Gleichung haben wir benutzt, dass die Multiplikation in den ganzen Zahlen kommutativ ist, in der dritten das Distributivitätsgesetz (also a ausgeklammert).)
   Also ist $a \mid x \cdot b + y \cdot c$ für alle $x, y \in \mathbb{Z}$.

□

Bemerkung 1.1.4. *<u>Alle</u> $d \in \mathbb{Z}$ sind Teiler von 0, denn:*

$$0 = d \cdot 0$$

für alle $d \in \mathbb{Z}$.

Die 0 hat also unendlich viele Teiler. Alle anderen ganzen Zahlen haben jedoch nur endlich viele Teiler. Das ist der Inhalt des folgenden Satzes.
Zunächst müssen wir jedoch noch Folgendes bemerken:

Bemerkung 1.1.5. *Sind $a, b \in \mathbb{Z}$, so gilt: $|a \cdot b| = |a| \cdot |b|$, wobei für $x \in \mathbb{Z}$ mit $|x|$ der Betrag von x bezeichnet wird, also*

$$|x| = \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}$$

Beweis. Fallunterscheidung: Die beiden Zahlen a und b können jeweils positiv, Null oder negativ sein.
Anschließend alle Fälle durchrechnen – *siehe auch meine Rechnung in der Vorlesung vom*

5.4.2011 (oder Mini-Hausaufgabe) – und die Definition des Betrages anwenden (unter Beachtung, dass das Produkt zweier positiver Zahlen bzw. zweier negativer Zahlen positiv ist und das Produkt einer positiven mit einer negativen Zahl bzw. einer negativen mit einer positiven Zahl negativ). □

Satz 1.1.6. *Seien $a, d \in \mathbb{Z}$, sei $a \neq 0$ und $d \mid a$. Dann gilt:*

$$|d| \leq |a|.$$

Insbesondere hat jedes von Null verschiedene $a \in \mathbb{Z}$ nur endlich viele Teiler.

Beweis. Sei $d \mid a$. Das heißt, es gibt ein $c \in \mathbb{Z}$ mit $a = d \cdot c$.
Nach dem vorangegangenen Lemma gilt dann: $|a| = |d \cdot c| = |d| \cdot |c|$.
Da $a \neq 0$, folgt auch $c \neq 0$ (und $d \neq 0$), also auch schon $|c| \geq 1$ (und $|d| \geq 1$), da es keine ganze Zahl zwischen 0 und 1 gibt.
Da aber $|c| \geq 1$, gilt auch $|a| = |d| \cdot |c| \geq |d| \cdot 1 = |d|$. Also gilt die zu zeigende Ungleichung.

Die Teiler können also nur im Intervall $[-a, a]$ liegen, falls $a > 0$ ist, bzw. im Intervall $[a, -a]$, falls $a < 0$ ist.
Es gibt in beiden Fällen genau $2 \cdot |a| + 1$ verschiedene ganze Zahlen in den Intervallen, also hat $a \neq 0$ höchstens $2 \cdot |a| + 1$ Teiler. Nun ist aber 0 mit Sicherheit *kein* Teiler von a, falls $a \neq 0$, denn $0 \cdot c = 0$ für alle $c \in \mathbb{Z}$. Somit hat $a \neq 0$ sogar höchstens $2 \cdot |a|$ Teiler. □

Bemerkung 1.1.7. *Die Abschätzung, dass jedes $0 \neq a \in \mathbb{Z}$ höchstens $2 \cdot |a|$ Teiler hat, ist im Allgemeinen nicht* scharf. *(D. h., es gilt* echte *Ungleichheit für die Teileranzahl.)*
Die Teiler von 5 sind beispielsweise: 1, -1, 5 und -5, also vier Stück. Aber $2 \cdot |5| = 10 > 4$.

Folgerung 1.1.8. *Seien $a, d \in \mathbb{Z}$ mit $a > 0$ und $d > 0$. Gilt sowohl $d \mid a$ als auch $a \mid d$, so ist $a = d$.*

Beweis. Da $a > 0$ und $d > 0$, ist $|a| = a$ und $|d| = d$. Nach Satz 1.1.6 gilt nun sowohl $d \leq a$ als auch $a \leq d$, also $a = d$. (Rechenregeln für Kleiner-Gleich-Relation in $\mathbb{Z}$) □

Bemerkung 1.1.9. *Sei $a \in \mathbb{Z}$. Dann gilt nicht nur $a \mid a$, sondern auch $-a \mid a$ sowie $1 \mid a$ und $-1 \mid a$. (Jede ganze Zahl $\neq \pm 1$ hat also mindestens vier Teiler.)*

Beweis. $a = (-a) \cdot (-1)$, $a = 1 \cdot a$ und $a = (-1) \cdot (-a)$ für alle $a \in \mathbb{Z}$. □

Definition 1.1.10. Sei $a \in \mathbb{Z}$. Wir nennen dann a, $-a$, 1 und -1 *die trivialen Teiler von a*, alle übrigen Teiler *echte Teiler von a.*

Bemerkung 1.1.11. *Insbesondere gilt für* echte *Teiler d von a (nach Satz 1.1.6) immer: $1 < |d| < |a|$.*

Bemerkung 1.1.12. *Sei $a \in \mathbb{Z}$. Dann haben a und $-a$ dieselben Teiler.*

Beweis. Sei $d \mid a$. Dann gibt es nach Definition ein $c \in \mathbb{Z}$ mit $a = d \cdot c$. Dann ist aber $-a = -(d \cdot c) = d \cdot (-c)$ mit $-c \in \mathbb{Z}$. Also ist auch $d \mid -a$.
Sei umgekehrt $d' \mid -a$. Dann gibt es nach Definition ein $c' \in \mathbb{Z}$ mit $-a = d' \cdot c'$. Dann ist aber $a = -(-a) = -(d' \cdot c') = d' \cdot (-c')$ mit $-c' \in \mathbb{Z}$. Also ist auch $d' \mid a$. □

(Wir können uns also darauf beschränken, zunächst Teiler von nicht-negativen Zahlen zu bestimmen, da für negative Zahlen die Teiler dieselben sind wie für den (positiven) Betrag der Zahl.)

Bemerkung 1.1.13. *Seien $a, d \in \mathbb{Z}$ und $d \mid a$. Dann gilt auch: $-d \mid a$.*

Beweis. Da $d \mid a$, gibt es ein $c \in \mathbb{Z}$ mit $a = d \cdot c$. Dann ist aber auch $a = (-d) \cdot (-c)$ mit $-c \in \mathbb{Z}$. Also ist auch $-d \mid a$. □

(Wir können uns also auch darauf beschränken, zunächst nicht-negative Teiler zu bestimmen, da diese immer in „Paaren“ auftauchen.)

1.2 Primzahlen

Ziel/Aufgabe: Wir möchten ganze Zahlen in Produkte kleinerer Zahlen zerlegen (und das auch noch möglichst „eindeutig“)...
$1188 = 12 \cdot 9 \cdot 11 = 2^2 \cdot 3^3 \cdot 11$, $3315 = 3 \cdot 5 \cdot 13 \cdot 17$, $512 = 2^9$ etc.

Definition 1.2.1. Sei $p \in \mathbb{N}$. Die Zahl p heißt *Primzahl*, wenn die beiden folgenden Bedingungen erfüllt sind:

1. $p > 1$.
2. Ist $p = a \cdot b$ mit $a, b \in \mathbb{N}$, so ist $a = 1$ oder $b = 1$.

Lemma 1.2.2 (1. Charakterisierung von Primzahlen)**.** *Sei $p \in \mathbb{N}$ mit $p > 1$. Dann sind die folgenden Aussagen äquivalent:*

1. *p ist eine Primzahl.*
2. *1 und p sind die einzigen positiven Teiler von p.*
3. *p hat keine echten Teiler.*

Beweis. Wir zeigen: 1. ⇒ 2., 2. ⇒ 3. und 3. ⇒ 1.

(„1. ⇒ 2.“ ist logisch äquivalent zu „nicht 2. ⇒ nicht 1.“ etc.)

nicht 2. ⇒ nicht 1.: Wenn 2. nicht gilt, gibt es einen weiteren positiven Teiler a von p mit $1 < a < p$.
Es gibt, da a Teiler von p ist, also ein $b \in \mathbb{Z}$ mit $p = a \cdot b$. Es gilt aber sogar $b \in \mathbb{N}$, denn sonst wäre p nicht positiv. Insbesondere ist dann $1 \leq b \leq |p| = p$ (nach Satz 1.1.6).
Auch b ist ein echter Teiler von p, denn wäre $b = 1$ oder $b = p$, so müsste dementsprechend $a = p$ oder $a = 1$ sein. (Dann wäre aber a kein echter Teiler von p).

Also haben wir eine Produktzerlegung $p = a \cdot b$ gefunden, in der weder $a = 1$ noch $b = 1$ gilt, weshalb die Bedingung 1. nicht erfüllt ist.

nicht 3. $\Rightarrow$ nicht 2.: Gilt 3. nicht, so gibt es einen echten Teiler d von p. Dann ist aber auch der Betrag $|d|$ ein echter Teiler von p. Nach Bemerkung 1.1.13 ist ja mit d auch $-d$ ein Teiler von p, also auf jeden Fall auch $|d|$. Und nach Bemerkung 1.1.11 gilt: $1 < |d| < |p| = p$. Also kann *nicht* gelten: $|d| = 1$ oder $|d| = p$. Damit haben wir einen weiteren positiven Teiler von p gefunden, außer den trivialen positiven Teilern 1 und p. Also gilt 2. nicht.

3. $\Rightarrow$ 1.: Sei $p = a \cdot b$ mit $a, b \in \mathbb{N}$. Die Zahl a ist also ein Teiler von p. Da p nach Bedingung 3. nur triviale Teiler hat, gilt $a = 1$ oder $a = p$. Im ersten Fall ist p eine Primzahl, und im zweiten Fall folgt dann $b = 1$, also ist p auch eine Primzahl. □

Bemerkung 1.2.3. *Aufgrund der Eigenschaft 3. in der Charakterisierung nennen wir Primzahlen auch* unzerlegbar.[1]

Satz 1.2.4. *Sei $a \in \mathbb{N}$ mit $a > 1$. Dann besitzt a einen kleinsten (positiven) Teiler $t > 1$. Dieser Teiler ist eine Primzahl.*

Beweis. Wir benutzen folgendes Beweisprinzip: Ist $M \subseteq \mathbb{N}$ mit $M \neq \emptyset$, so besitzt M ein kleinstes Element.

Sei $T := \{d \in \mathbb{N} \mid d > 1 \text{ und } d \mid a\}$, also die Menge der positiven Teiler von a, die echt größer als 1 sind.
Natürlich ist $T \subseteq \mathbb{N}$. Die Menge T ist nicht leer, denn $a \in T$. ($a > 1$ und $a \mid a$.)
Also besitzt die Menge ein kleinstes Element t, und dieses t ist gerade der gesuchte kleinste positive Teiler von a, der > 1 ist.

Wir müssen nun noch zeigen, dass dieses t eine Primzahl ist:
Angenommen, t ist keine Primzahl. Dann gäbe es nach dem vorangegangenen Lemma einen echten Teiler t' von t, für den dann $1 < t' < t$ gilt.
Nun haben wir $t' \mid t$ sowie $t \mid a$, also nach den Rechenregeln für Teilbarkeit auch $t' \mid a$. Damit wäre aber auch $t' \in T$, da t' einerseits Teiler von a und andererseits $t' > 1$ ist. Widerspruch (zur Minimalität von t)! (Dann wäre ja t nicht das kleinste Element in T gewesen, denn $t' < t$.)
Also muss t eine Primzahl sein. □

Satz 1.2.5 (Satz von Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir zeigen folgende Behauptung:

Sind $p_1, \ldots, p_n$ endlich viele Primzahlen, dann ist der kleinste (positive) Teiler $t > 1$ der Zahl $a := p_1 \cdot \ldots \cdot p_n + 1$ eine Primzahl, die von allen Primzahlen $p_1, \ldots, p_n$ verschieden ist.

[1] Im Allgemeinen stimmen die Begriffe „Unzerlegbarkeit“ und „Primelement“ nicht überein, mehr dazu jedoch später – im Algebrateil dieser Vorlesung.

Beweis der Behauptung. Nach Satz 1.2.4 ist t eine Primzahl. Wir müssen also nur noch zeigen, dass sie nicht mit einer der Zahlen $p_1, \ldots, p_n$ übereinstimmen kann.

Angenommen, $t = p_i$ für ein $i \in \{1, \ldots, n\}$, dann würde gelten: $t \mid p_1 \cdot \ldots \cdot p_n$. Außerdem gilt nach Voraussetzung: $t \mid a = p_1 \cdot \ldots \cdot p_n + 1$. Nach den Rechenregeln für Teilbarkeit würde folgen: $t \mid a + (-1) \cdot p_1 \cdot \ldots \cdot p_n = p_1 \cdot \ldots \cdot p_n + 1 - p_1 \cdot \ldots \cdot p_n = 1$. Dann wäre aber $|t| = 1$, insbesondere $t \leq 1$. Widerspruch! □

□

Lemma 1.2.6 (Fundamentallemma)**.** *Seien $a, b \in \mathbb{N}$. Ist p eine Primzahl mit $p \mid a \cdot b$, so gilt: $p \mid a$ oder $p \mid b$.*

Beweis. Wir wenden im Beweis zunächst dasselbe Prinzip an wie im Beweis von Satz 1.2.4.

Sei $E := \{x \in \mathbb{N} \mid p \text{ teilt } a \cdot x\} \subseteq \mathbb{N}$.
Die Menge E ist nicht leer, denn es gilt unter Anderem: $p \in E$ (da ja $p \mid a \cdot p$) und $b \in E$ (da ja nach Voraussetzung $p \mid a \cdot b$).
Also hat die Menge E ein kleinstes Element, sagen wir c.

Folgende Behauptung ist nun wichtig für den Beweis:

Behauptung: $c \mid y$ für alle $y \in E$.
(Das kleinste Element in der Menge E ist also ein Teiler aller Elemente in der Menge.)

Beweis der Behauptung. Wir führen eine Division mit Rest durch *(– wenn der Rest Null ist, dann ist c ein Teiler von y)*:
Jedes $y \in \mathbb{N}$ hat eine (eindeutige) Darstellung:

$$y = q \cdot c + r,$$

wobei $q, r \in \mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$ und $0 \leq r < c$ gilt.
Da $y, c \in E$, gilt $p \mid a \cdot y$ und $p \mid a \cdot c$, also auch $p \mid a \cdot r = a \cdot y - q \cdot (a \cdot c)$ (nach den Rechenregeln für Teilbarkeit).
Wäre nun $r > 0$, so wäre auch $r \in E$. Widerspruch (zur Minimalität von c)! (Es ist ja $r < c$.)
Also ist $r = 0$, und damit $c \mid y$. □

Da insbesondere immer $p \in E$ (s.o.), gilt auch $c \mid p$ (nach der soeben bewiesenen Behauptung). Daher ist mit Lemma 1.2.2 nun $c = 1$ oder $c = p$, da p eine Primzahl ist.
Im ersten Fall ist $p \mid a \cdot c = a \cdot 1 = a$ (denn $c \in E$), im zweiten Fall gilt $p = c \mid b$ (nach der soeben bewiesenen Behauptung), denn es gilt immer $b \in E$ (s.o.). □

Folgerung 1.2.7. *Seien $a_1, \ldots, a_n \in \mathbb{N}$.*
Ist $p \in \mathbb{N}$ eine Primzahl mit $p \mid a_1 \cdot \ldots \cdot a_n$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p \mid a_i$.

Beweis. Übung 1, Teil 1, Übungsblatt 1. □

Satz 1.2.8 (2. Charakterisierung von Primzahlen)**.** *Sei $p \in \mathbb{N}$. Dann sind die folgenden Aussagen äquivalent:*

1. *p ist eine Primzahl.*
2. *Ist $p \mid a \cdot b$ mit $a, b \in \mathbb{Z}$, so gilt: $p \mid a$ oder $p \mid b$.*

Beweis. Übung 3, Übungsblatt 1. □

Beispiel 1.2.9 (Beispiel 1 zum Beweis in Lemma 1.2.6)**.** *Seien $p = 3$, $a = 4$ und $b = 6$. Es gilt $3 \mid 4 \cdot 6 = 24$. Wir wollen herausfinden, ob uns der Beweis des Lemmas korrekt $p \mid b = 6$ voraussagt.*
Wir betrachten die Menge $E = \{x \in \mathbb{N} \mid p \text{ teilt } a \cdot x\} = \{x \in \mathbb{N} \mid 3 \text{ teilt } 4 \cdot x\} = \{3, 6, 9, 12, 15, \ldots\}$. Das kleinste Element in E ist $c = 3$, und wir sehen zumindest für die ersten Zahlen in E, dass 3 diese Zahlen teilt, wie in der Behauptung im Beweis des Lemmas.
Im Lemma treten zwei Fälle auf: $c = 1$ oder $c = p$. Im ersten Fall gilt: $p \mid a$, im zweiten Fall gilt: $p \mid b$. Hier also nun $3 \mid b = 6$.

Beispiel 1.2.10 (Beispiel 2 zum Beweis in Lemma 1.2.6)**.** *Seien $p = 3$, $a = 6$ und $b = 4$. Es gilt $3 \mid 6 \cdot 4 = 24$. Wir wollen herausfinden, ob uns der Beweis des Lemmas korrekt $p \mid a = 6$ voraussagt.*
Wir betrachten die Menge $E = \{x \in \mathbb{N} \mid p \text{ teilt } a \cdot x\} = \{x \in \mathbb{N} \mid 3 \text{ teilt } 4 \cdot x\} = \{1, 2, 3, 4, 5, 6, \ldots\}$. Das kleinste Element in E ist $c = 1$, und wir sehen für alle Zahlen in E, dass 1 diese Zahlen teilt, wie in der Behauptung im Beweis des Lemmas.
Im Lemma treten zwei Fälle auf: $c = 1$ oder $c = p$. Im ersten Fall gilt: $p \mid a$, im zweiten Fall gilt: $p \mid b$. Hier also nun $3 \mid a = 6$.

Nun kommen wir zum ersten größeren Satz in der Vorlesung:

Satz 1.2.11 (Hauptsatz der Elementaren Zahlentheorie)**.** *Jede natürliche Zahl $a \in \mathbb{N}$ mit $a > 1$ hat eine (bis auf Reihenfolge der Faktoren) eindeutige Primfaktorzerlegung.*

Beweis.
Wir haben zu zeigen:

- Existenz der Primfaktorzerlegung
- Eindeutigkeit der Primfaktorzerlegung (bis auf die Reihenfolge der Faktoren)

Existenz

Beweis der Existenz. (Wir führen eine Induktion über $a \in \mathbb{N}$ durch.)
Induktionsanfang: $a = 2$.
In diesem Fall ist a eine Primzahl, also auch ein Produkt von Primzahlen.
Induktionsvoraussetzung:
Es gebe eine Primfaktorzerlegung für alle $1 < a' < a$.

Induktionsschritt:
Nach Satz 1.2.4 gibt es einen kleinsten Primteiler $t > 1$ von a.
Also gibt es eine Zahl $b \in \mathbb{N}$ mit $a = t \cdot b$, wobei $1 \leq b < a$ gelten muss (da ja $t > 1$).
Fall 1: $b > 1$.
Nach Induktionsvoraussetzung gibt es nun eine Primfaktorzerlegung von b:
Es gibt also Primzahlen $p_2, \ldots, p_n \in \mathbb{N}$ mit $b = p_2 \cdot \ldots \cdot p_n$. Dann hat aber a die Primfaktorzerlegung $a = t \cdot b = t \cdot p_2 \cdot \ldots \cdot p_n$, denn auch t ist ja auch Primzahl.
Fall 2: $b = 1$.
Dann ist aber $a = t \cdot b = t$, also a eine Primzahl (und damit auch ein Produkt von Primzahlen). □

Eindeutigkeit

Beweis der Eindeutigkeit. (Wir führen eine Induktion über die Anzahl m der Faktoren in einer(!) Primfaktorzerlegung von a durch.)
Die Zahl a habe zwei Primfaktorzerlegungen mit m bzw. n Faktoren. Wir müssen zeigen, dass dann $m = n$ gilt. Außerdem ist zu zeigen, dass wir die Primzahlen $p_1, \ldots, p_n$ und $q_1, \ldots, q_n$ in zwei Primfaktorzerlegungen $a = p_1 \cdot \ldots \cdot p_n$ und $a = q_1 \cdot \ldots \cdot q_n$ so durchnummerieren können, dass $p_1 = q_1$, …, $p_n = q_n$ gilt.
Induktionsanfang: $m = 1$.
In diesem Fall ist $a = p_1$ eine Primzahl, und damit muss auch $n = 1$ und $p_1 = q_1$ sein.
Induktionsvoraussetzung:
Es gebe eindeutige Primfaktorzerlegungen (bis auf die Reihenfolge der Faktoren) von allen Zahlen, deren Primfaktorzerlegungen $\leq m - 1$ Faktoren haben.
Induktionsschritt:
Sind $a = p_1 \cdot \ldots \cdot p_m$ und $a = q_1 \cdot \ldots \cdot q_n$ zwei Primfaktorzerlegungen von a [wir wissen ja noch nicht, dass dann $m = n$ gilt…], so ist natürlich $p_1 \mid a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$. Nach der Folgerung zum Fundamentallemma gibt es ein $j \in \{1, \ldots, m\}$ mit $p_1 \mid q_j$. Wir können dabei ohne Einschränkung der Allgemeinheit davon ausgehen, dass wir die Zahlen in der zweiten Darstellung $a = q_1 \cdot \ldots \cdot q_n$ schon vorher so angeordnet haben, dass $j = 1$ und damit $p_1 \mid q_1$ gilt. Nach der Charakterisierung von Primzahlen im Lemma 1.2.2 sind aber die einzigen positiven Teiler von q_1 als Primzahl nun 1 und q_1. Damit folgt $p_1 = 1$, was nicht sein kann, da p_1 Primzahl und damit > 1 ist, oder $p_1 = q_1$. Also: $p_1 = q_1$.
(Nun „teilen“ wir a durch p_1.) Wir erhalten die Zahl $a' := p_2 \cdot \ldots \cdot p_m$. Dies ist eine Zahl mit $m - 1$ Primfaktoren, für die wir nach Induktionsvoraussetzung eine (bis auf Reihenfolge der Faktoren) eindeutige Primfaktorzerlegung haben. Ist nun also auch $a = q_2 \cdot \ldots \cdot q_n$ mit Primzahlen $q_2, \ldots, q_n$, so gilt $m - 1 = n - 1$ (und damit natürlich auch $n = m$) gilt. Es gilt also (nach evtl. voheriger Umnummerierung): $m = n$ und $p_2 = q_2$, $p_3 = q_3$, …, $p_m = q_m$.
Nun lässt sich aber $a = p_1 \cdot a' = p_1 \cdot p_2 \cdot \ldots \cdot p_m = p_1 \cdot q_2 \cdot \ldots \cdot q_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ schreiben, wobei $p_1 = q_1$ war, und $p_2 = q_2$, $p_3 = q_3$, …, $p_m = q_m$ (nach Induktionsvoraussetzung).
Damit hat nun auch die Zahl a eine eindeutige Primfaktorzerlegung (bis auf die Reihenfolge der Faktoren). □

□

Bemerkung 1.2.12 (Umformulierung des Hauptsatzes der Elementaren Zahlentheorie)**.** *Sei $a \in \mathbb{N}$ mit $a \neq 1$. Dann gibt es Primzahlen $p_1 < p_2 < \ldots < p_k$ und natürliche Zahlen $m_1, \ldots, m_k \in \mathbb{N}$, so dass a eine* eindeutige Darstellung *(nicht nur bis auf Reihenfolge der Faktoren)*

$$a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$$

hat.
(Dazu sortieren wir die Primfaktoren der Größe nach aufsteigend und fassen gemeinsame Faktoren zu einer Potenz zusammen. Hier soll c^d mit $c, d \in \mathbb{N}$ wie folgt definiert sein:

$$c^d := \underbrace{c \cdot \ldots \cdot c}_{d\text{-mal}}$$

Wir nennen hier m_i auch die Vielfachheit *des Primfaktors p_i, $i = 1, \ldots, k$, in a.)*

Bemerkung 1.2.13. *Der Hauptsatz der Elementaren Zahlentheorie wird im Allgemeinen falsch, wenn wir statt der natürlichen Zahlen nur bestimmte multiplikativ abgeschlossene Teilmengen der natürlichen Zahlen nehmen, etwa $M := \{3n + 1 \mid n \in \mathbb{N}_0\}$, und dort* unzerlegbare Zahlen *entsprechend den Primzahlen (wie in Definition 1.2.1) definieren.*
Ein Beispiel dazu ist bei Übung 1, Übungsblatt 2 zu finden.

1.3 Anwendungen des Hauptsatzes der EZT

1.3.1 Anzahl der positiven Teiler

Satz 1.3.1 (Teilbarkeitskriterium)**.** *Sei $a \in \mathbb{N}$, $a \neq 1$, und sei $a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ eine – und nach der Umformulierung des Hauptsatzes damit* die *– Primfaktorzerlegung mit $p_1 < \ldots < p_k$ und $m_i \in \mathbb{N}$ für alle $i = 1, \ldots, k$. Sei $b \in \mathbb{N}$. $(*)$*
Dann sind die folgenden Aussagen äquivalent:

1. *$b \mid a$*
2. *Es gibt $n_i \in \mathbb{N}$, $i = 1, \ldots, k$, so dass $b = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ mit $0 \leq n_i \leq m_i$ für alle $i = 1, \ldots, k$*

Beweis. 1. $\Rightarrow$ 2.: Sei $b \mid a$. Dann gibt es ein $c \in \mathbb{Z}$ (sogar $c \in \mathbb{N}$), so dass $a = b \cdot c$.
$a = b \cdot c$ hat (nach dem Hauptsatz) eine (bis auf die Reihenfolge der Faktoren) eindeutige Primfaktorzerlegung, und b hat eine ebensolche. Also kann b höchstens Primfaktoren haben, die auch schon in a auftreten, also

$$b = p_1^{n_1} \cdot \ldots \cdot a_k^{n_k}$$

mit $n_i \in \mathbb{N}$ für alle $i = 1, \ldots, k$.
Wir müssen nun noch zeigen, dass $n_i \leq m_i$ für alle $i = 1, \ldots, k$ gilt.
Da $p_i^{n_i} \mid b$ für alle $i = 1, \ldots, k$, folgt: $p_i^{n_i} \mid b \cdot c = a$ für alle $i = 1, \ldots, k$. Also gibt es ein $d \in \mathbb{Z}$, sogar in $\mathbb{N}$, so dass $a = p_i^{n_i} \cdot d$. Da a eine (bis auf die Reihenfolge der Faktoren)

eindeutige Primfaktorzerlegung hat, muss $n_i \leq m_i$ für alle $i = 1, \ldots, k$ gelten; sonst wäre ja $p_i^{m_i}$ nicht die *höchste* Potenz von p_i in a. (Natürlich sind die n_i auch alle nicht-negativ, da wir uns ja in $\mathbb{Z}$ befinden (und sonst echte Brüche erhalten würden).)
2. $\Rightarrow$ 1.: Sei $b = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ mit $0 \leq n_i \leq m_i$ für alle $i = 1, \ldots, k$. Gilt $0 \leq n_i \leq m_i$ für alle $i = 1, \ldots, k$, so ist $m_i - n_i \geq 0$ für alle $i = 1, \ldots, k$. Wir können also

$$c := p_1^{m_1 - n_1} \cdot \ldots \cdot p_k^{m_k - n_k} \in \mathbb{N}$$

bilden, wofür dann $b \cdot c = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k} \cdot p_1^{m_1 - n_1} \cdot \ldots \cdot p_k^{m_k - n_k} = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} = a$ gilt. Also ist $b \mid a$. □

Definition 1.3.2. Sei $a \in \mathbb{N}$. Mit $\tau(a)$ bezeichnen wir die *Anzahl der positiven Teiler von* a.

Der folgende Satz zeigt, dass wir $\tau(a)$ ganz schnell berechnen können, wenn wir nur die Primfaktorzerlegung von a (in dem Sinne wie in $(*)$) kennen. (Da der einzige positive Teiler von 1 die 1 ist, gilt $\tau(1) = 1$. Wir beschränken uns im folgenden Satz daher auf Zahlen $a \neq 1$.)

Satz 1.3.3. *Sei $a \in \mathbb{N}$, $a \neq 1$. Sei $a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ die Primfaktorzerlegung von a mit $p_1 < \ldots < p_k$ und $m_i \in \mathbb{N}$ für alle $i = 1, \ldots, k$.*
Dann gilt:

$$\tau(a) = (m_1 + 1) \cdot \ldots \cdot (m_k + 1).$$

Insbesondere ist dann

$$\tau(p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = \tau(p_1^{m_1}) \cdot \ldots \cdot \tau(p_k^{m_k}).$$

Beweis. (Induktion nach der Anzahl k der verschiedenen Primteiler von a)
Induktionsanfang: $k = 1$.
Dann ist $a = p_1^{m_1}$, und a hat genau die $m_1 + 1$ positiven Teiler $1, p_1, p_1^2, \ldots, p_1^{m_1}$. Also $\tau(a) = m_1 + 1$.
Induktionsvoraussetzung: Die Behauptung gelte für alle Zahlen mit höchstens $k - 1$ verschiedenen Primteilern.
Induktionsschritt: Sei $a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$. Dann hat $b := p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$ genau $k-1$ verschiedene Primteiler, und es gilt nach Induktionsvoraussetzung: $\tau(b) = (m_2 + 1) \cdot \ldots \cdot (m_k + 1)$.
Alle positiven Teiler von $a = p_1^{m_1} \cdot b$ erhalten wir, indem wir die positiven Teiler von $p_1^{m_1}$ und die positiven Teiler von b miteinander kombinieren. Wir erhalten also insgesamt $\tau(p_1^{m_1}) \cdot \tau(b) = (m_1 + 1) \cdot \ldots \cdot (m_k + 1)$ positive Teiler von a, also:

$$\tau(a) = \underbrace{(m_1 + 1)}_{=\tau(p_1^{m_1})} \cdot \ldots \cdot \underbrace{(m_k + 1)}_{=\tau(p_k^{m_k})}.$$

□

Beispiel 1.3.4. • $5 = 5^1$ *(Primfaktorzerlegung), also* $\tau(5) = 1 + 1 = 2$

- $120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$ *(Primfaktorzerlegung), also* $\tau(120) = (3+1)\cdot(1+1)\cdot(1+1) = 4 \cdot 2 \cdot 2 = 16$
- $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, *also* $\tau(5040) = 5 \cdot 3 \cdot 2 \cdot 2 = 60$
- $123 = 3 \cdot 41$, *also* $\tau(123) = 2 \cdot 2 = 4$

1.3.2 Produkt aller positiven Teiler

Definition 1.3.5. Sei $a \in \mathbb{N}$. Mit $P(a)$ bezeichnen wir *das Produkt aller positiven Teiler von* a.

Es kann relativ mühsam sein, alle positiven Teiler einer Zahl hinzuschreiben und davon dann auch noch das Produkt zu berechnen. Der folgende Satz zeigt, dass es nicht so schwer ist, vorausgesetzt, wir wissen, wie wir Zahlen schnell potenzieren können. (Dafür gibt es relativ schnelle Rechenverfahren, die man auf Computern implementieren kann.)
Zunächst zeigen wir aber noch Folgendes:

Lemma 1.3.6. *Sei* $a \in \mathbb{N}$. *Dann ist* a *eine Quadratzahl, d. h., es gibt ein* $b \in \mathbb{N}$ *mit* $a = b^2$, *genau dann, wenn* $\tau(a)$ *ungerade ist.*

Beweis. Falls $a = 1 = 1 \cdot 1$, so hat a genau einen Teiler.

Sei nun $a \neq 1$ und $a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ die Primfaktorzerlegung von a mit $p_1 < \ldots < p_k$ und $m_1, \ldots, m_k \in \mathbb{N}$.

Ist a eine Quadratzahl, so sind alle Exponenten m_i, $i = 1, \ldots, k$, gerade, es gibt also $n_i \in \mathbb{N}$ mit $m_i = 2 \cdot n_i$ für alle $i = 1, \ldots, k$.
Dann ist

$$\tau(a) = (m_1 + 1) \cdot \ldots \cdot (m_k + 1) = (2n_1 + 1) \cdot \ldots \cdot (2n_k + 1)$$

als Produkt von ungeraden Zahlen ungerade.

Ist a dagegen keine Quadratzahl, so gibt es (mindestens) einen Exponenten m_i, $i \in \{1, \ldots, k\}$, der ungerade ist, für den es also ein $n_i \in \mathbb{N}_0$ gibt mit $m_i = 2n_i + 1$. (Sonst könnten wir ja $b := p_1^{m_1/2} \cdot \ldots \cdot p_k^{m_k/2}$ setzen, für das dann $b^2 = a$ wäre.)
Dann ist aber

$$\tau(a) = (m_1+1)\cdot\ldots\cdot(m_k+1) = (m_1+1)\cdot\ldots\cdot(m_{i-1}+1)\cdot\underbrace{(2n_i+2)}_{\text{gerade}}\cdot(m_{i+1}+1)\cdot\ldots\cdot(m_k+1)$$

als Produkt einer geraden Zahl mit weiteren Zahlen gerade. □

Hier nun der Satz, wie man das Produkt aller positiven Teiler einer Zahl berechnen kann:

Satz 1.3.7. *Sei* $a \in \mathbb{N}$. *Dann gilt:*

$$P(a) = a^{\tau(a)/2}$$

Beweis. Wir ordnen die Teiler positiven Teiler d_i von a der Größe nach an:

$$1 =: d_1 < d_2 < d_3 < \ldots < d_{\tau(a)-2} < d_{\tau(a)-1} < d_{\tau(a)} := a$$

Dann gilt:

$$d_1 \cdot d_{\tau(a)} = a,$$
$$d_2 \cdot d_{\tau(a)-1} = a,$$
$$d_3 \cdot d_{\tau(a)-2} = a$$
$$\vdots$$

Es können zwei Fälle auftreten:
Fall 1: $\tau(a)$ ist gerade, etwa $\tau(a) = 2 \cdot s$ mit $s \in \mathbb{N}$.
(Dann ist $s = \frac{\tau(a)}{2}$.)
Wir „enden“ dann bei

$$\vdots$$
$$d_s \cdot d_{s+1} = a.$$

Das Produkt aller positiven Teiler von a ist also das Produkt der einzelnen Zeilen, und wir haben s Stück. Daher ist

$$P(a) = d_1 \cdot d_{\tau(a)} \cdot d_2 \cdot d_{\tau(a)-1} \cdot \ldots \cdot d_s \cdot d_{s+1} = a^s = a^{\tau(a)/2}.$$

Fall 2: $\tau(a)$ ist ungerade, etwa $\tau(a) = 2 \cdot s + 1$ mit $s \in \mathbb{N}_0$.
(Dann ist $s = \frac{\tau(a)-1}{2}$.)
Wir „enden“ dann bei

$$\vdots$$
$$d_s \cdot d_{s+2} = a,$$
$$d_{s+1} \cdot d_{s+1} = a.$$

Das Produkt aller positiven Teiler von a besteht also aus dem Produkt der einzelnen Zeilen – bis auf die letzte –, und wir haben davon s Stück. Multiplizieren müssen wir das Ganze aber noch mit d_{s+1}. (Die letzte Gleichung zeigt aber auch, dass $a^{1/2} (= d_{s+1})$ in dem Fall immer existiert.)
Daher ist

$$P(a) = d_1 \cdot d_{\tau(a)} \cdot d_2 \cdot d_{\tau(a)-1} \cdot \ldots \cdot d_s \cdot d_{s+2} \cdot d_{s+1} = a^s \cdot a^{1/2} = a^{\tau(a)/2}.$$

(Es ist ja $s + \frac{1}{2} = \frac{\tau(a)-1}{2} + \frac{1}{2} = \frac{\tau(a)}{2}$.) □

Beispiel 1.3.8.

- $12 = 2^2 \cdot 3$, *also* $\tau(12) = 3 \cdot 2 = 6$, *also* $P(12) = 12^{6/2} = 12^3 = 1728$
- $9 = 3^2$, *also* $\tau(9) = 3$, *also* $P(9) = 9^{3/2} = 9 \cdot 9^{1/2} = 9 \cdot 3 = 27$

- $a := p^3$ *mit* p *Primzahl, also* $\tau(p^3) = 4$*, also* $P(p^3) = (p^3)^{4/2} = (p^3)^2 = p^6$
- $a := p \cdot q$ *mit zwei verschiedenen Primzahlen* p *und* q*, also* $\tau(p \cdot q) = 2 \cdot 2 = 4$*, also* $P(p \cdot q) = (p \cdot q)^{4/2} = p^2 \cdot q^2$
- $a := p^2$ *mit* p *Primzahl, also* $\tau(p^2) = 3$*, also* $P(p^2) = (p^2)^{3/2} = p^3$

1.3.3 Summe der positiven Teiler

Auch die Summe der positiven Teiler einer natürlichen Zahl $a \in \mathbb{N}$ lässt sich leicht berechnen, wenn man die Primfaktorzerlegung der Zahl a kennt.

Definition 1.3.9. Sei $a \in \mathbb{N}$. Mit $\sigma(a)$ bezeichnen wir die *Summe aller positiven Teiler von* a.

Zur Vorbereitung müssen wir noch eine kleine Formel zeigen, die geometrische Summenformel.

Lemma 1.3.10 (Geometrische Summenformel)**.** *Sei* $q \in \mathbb{R}$ *mit* $q \neq 1$*. Dann gilt:*

$$1 + q + q^2 + \ldots + q^n = \frac{q^{n+1} - 1}{q - 1}$$

Beweis. Wir multiplizieren die linke Seite zunächst mit $q - 1$ und erhalten dann:

$$(q-1) \cdot (1 + q + q^2 + \ldots + q^n) = (q + q^2 + q^3 + \ldots + q^{n+1}) - (1 + q + q^2 + \ldots + q^n) = q^{n+1} - 1$$

Dann können wir, da $q \neq 1$, beide Seiten durch $q - 1$ teilen, woraus wir sofort die Formel erhalten. □

Nun können wir die Summe aller positiven Teiler einer natürlichen Zahl berechnen, wobei wir uns wieder auf den Fall beschränken, dass $a \neq 1$ ist. (Denn $\sigma(1) = 1$, da 1 der einzige positive Teiler von 1 ist.)

Satz 1.3.11. *Sei* $a \in \mathbb{N}$ *und* $a \neq 1$*. Sei* $a = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ *die Primfaktorzerlegung von* a *mit* $p_1 < \ldots < p_k$ *und* $m_i \in \mathbb{N}$ *für alle* $i = 1, \ldots, k$*. Dann gilt:*

$$\sigma(a) = \frac{p_1^{m_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{m_k+1} - 1}{p_k - 1}.$$

Insbesondere gilt:

$$\sigma(p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = \sigma(p_1^{m_1}) \cdot \ldots \cdot \sigma(p_k^{m_k}).$$

Beweis. (Induktion nach der Anzahl k der verschiedenen Primteiler von a)
Induktionsanfang: $k = 1$.

Dann ist $a = p_1^{m_1}$ mit einem $m_1 \in \mathbb{N}$. Die positiven Teiler von a sind also genau die Zahlen $1, p_1, p_1^2, \ldots, p_1^{m_1}$. Damit ist deren Summe $\sigma(a) = 1 + p_1 + p_2 + \ldots + p_1^{m_1}$, und nach der geometrischen Summenformel:

$$\sigma(a) = \frac{p_1^{m_1+1} - 1}{p_1 - 1}.$$

Induktionsvoraussetzung:
Die Formel gelte für alle Zahlen mit bis zu $k-1$ verschiedenen Primteilern.
Induktionsschritt:
Nach Satz 1.3.1 sind die Teiler von a genau die Zahlen

$$p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

mit $0 \leq n_i \leq m_i$ für alle $i = 1, \ldots, k$.
Wir bilden also für $\sigma(a)$ die Summe all dieser Zahlen.
Dazu können wir diese nach der Vielfachheit sortieren, mit der p_1 auftritt, also

$$p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \quad p_1 \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \quad p_1^2 \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \quad \ldots, \quad p_1^{m_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k},$$

wobei jeweils alle Zahlen n_i mit $0 \leq n_i \leq m_i$ für alle $i = 2, \ldots, k$ auftreten.
Aus der Summe der erstgenannten Zahlen können wir keine Potenzen von p_1 ausklammern. Aus der Summe der zweitgenannten Zahlen können wir p_1 ausklammern. Aus der Summe der drittgenannten Zahlen können wir p_1^2 ausklammern usw. Aus der Summe der letztgenannten Zahlen können wir $p_1^{m_1}$ ausklammern.
Haben wir die Potenzen von p_1 jeweils ausgeklammert, bleibt als zweiter Faktor noch die Summe über alle $p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ mit $0 \leq n_i \leq m_i$ für alle $i = 2, \ldots, k$ stehen.
Schreiben wir zur Abkürzung $b := p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$, so ist der zweite Faktor gerade die Summe über alle positiven Teiler der Zahl b, also $\sigma(b)$.
Wir erhalten also für die Gesamtsumme $\sigma(a)$ also

$$\begin{aligned}\sigma(a) &= (1 + p_1 + p_1^2 + \ldots + p_1^{m_1}) \cdot \sigma(b) \\ &= \frac{p_1^{m_1+1} - 1}{p_1 - 1} \cdot \sigma(b).\end{aligned}$$

Da b aber nur $k-1$ verschiedene Primfaktoren hat, gilt nach Induktionsvoraussetzung:

$$\sigma(b) = \frac{p_2^{m_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{m_k+1} - 1}{p_k - 1}.$$

Daraus folgt unmittelbar:

$$\sigma(a) = \frac{p_1^{m_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{m_k+1} - 1}{p_k - 1}.$$

□

Beispiel 1.3.12.

- $72 = 2^3 \cdot 3^2$, *also* $\sigma(72) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} = \frac{16-1}{1} \cdot \frac{27-1}{2} = 15 \cdot 13 = 195$
- $19 = 19^1$, *also* $\sigma(19) = \frac{19^2-1}{19-1} = \frac{360}{18} = 20$
- $a := p^m$, *dann ist* $\sigma(a) = \frac{p^{m+1}-1}{p-1} = \frac{p^{m+1}-p^m+p^m-1}{p-1} = p^m + \frac{p^m-1}{p-1}$

1.3.4 Vollkommene Zahlen

Definition 1.3.13. Sei $a \in \mathbb{N}$. Wir nennen a *vollkommen*, wenn $\sigma(a) = 2a$ gilt.

Während sich die Suche nach ungeraden vollkommenen Zahlen als ziemlich schwierig herausgestellt hat – tatsächlich weiß man zurzeit noch nicht einmal, ob es überhaupt ungerade vollkommene Zahlen gibt. . . –, können die geraden vollkommenen Zahlen leicht charakterisiert werden.

Satz 1.3.14. *Sei $a \in \mathbb{N}$, so dass es $s, b \in \mathbb{N}$ mit $s \geq 2$ und b ungerade gibt mit: $a = 2^{s-1}b$. Dann sind die folgenden Aussagen äquivalent:*

1. *a ist vollkommen.*

2. *b ist eine Primzahl und $b = 2^s - 1$.*

Beweis. 2. $\Rightarrow$ 1.: Wir müssen zeigen, dass für eine Zahl a mit den angegebenen Bedingungen immer $\sigma(a) = 2a$ gilt. Da b nach Voraussetzung eine Primzahl ist, ist $a = 2^{s-1} \cdot b$ die Primfaktorzerlegung von a. Nach Satz 1.3.11 gilt dann:

$$\sigma(a) = \frac{2^s - 1}{2 - 1} \cdot \frac{b^2 - 1}{b - 1} = (2^s - 1) \cdot (b + 1) = (2^s - 1) \cdot 2^s = 2 \cdot 2^{s-1} \cdot (2^s - 1) = 2a.$$

1. $\Rightarrow$ 2.: Sei nun a vollkommen. Wir müssen nun zeigen, dass b eine Primzahl ist und sich als $b = 2^s - 1$ mit dem vorgegebenen s schreiben lässt.
Als erstes berechnen wir die Summe $\sigma(b)$ aller positiven Teiler von b aus der Summe $\sigma(a)$ aller positiven Teiler von a:
Da b ungerade ist, kommen in der Primfaktorzerlegung von b keine Primfaktoren $= 2$ vor. Daher gilt nach Satz 1.3.11:

$$2^s b = 2a = \sigma(a) = \sigma(2^{s-1}) \cdot \sigma(b) = (2^s - 1) \cdot \sigma(b),$$

also:

$$\sigma(b) = \frac{2^s}{2^s - 1} b = b + c,$$

wenn wir $c := \frac{b}{2^s - 1} > 0$ setzen.
Da $\sigma(b) \in \mathbb{N}$ und $b \in \mathbb{N}$, muss $c \in \mathbb{Z}$ gelten. Also insgesamt $c \in \mathbb{N}$.
Da $b = c \cdot (2^s - 1)$, ist c ein positiver Teiler von b. Da aber $\sigma(b) = b + c$, sind b und c die *einzigen* positiven Teiler von b, und daher $c = 1$. (Gäbe es einen weiteren Teiler, so wäre $\sigma(b) \geq b + c + 1 > b + c = \sigma(b)$. Widerspruch!) Nach der Charakterisierung aus Lemma 1.2.2 erhalten wir, dass b eine Primzahl ist. Insbesondere ist wegen $c = 1$ dann $b = c \cdot (2^s - 1) = 2^s - 1$. □

Bemerkung 1.3.15. *Die vielleicht ein wenig komisch aussehende Darstellung der Zahl a in der Voraussetzung des vorangegangenen Satzes ist wie folgt zu „erklären“:*

- $s \geq 2 \Rightarrow s-1 \geq 1$, *also taucht der Primfaktor* 2 *in der Primfaktorzerlegung von* a *wirklich auf.* a *ist also gerade.*
  Umgekehrt hat auch jede gerade Zahl a *so eine Darstellung.*

- b *ist ungerade.* $\Rightarrow$ b *enthält keine* 2 *als Primfaktor.* $\Rightarrow$ *Der Primfaktor* 2 *taucht in der Primfaktorzerlegung von* a *genau mit der Vielfachheit* $s-1$ *auf.*
  Umgekehrt gilt auch: Hat a *so eine Darstellung, wobei* 2 *genau mit Vielfachheit* $s-1$ *in der Primfaktorzerlegung von* a *auftaucht, so muss* b *ungerade sein.*

Um herauszufinden, ob eine gerade Zahl a eine vollkommene Zahl ist, müssen wir also testen, ob sie als $a = 2^{s-1} \cdot (2^s - 1)$ mit $s \in \mathbb{N}$ und $s \geq 2$ dargestellt werden kann und dabei $2^s - 1$ eine Primzahl ist. Der folgende Satz gibt ein (hinreichendes) Kriterium an, wann Letzteres *nicht* der Fall ist.

Satz 1.3.16. *Sei* $s \in \mathbb{N}$. *Ist* s *keine Primzahl, so ist auch* $2^s - 1$ *keine Primzahl.*

Beweis. Ist s keine Primzahl, so lässt es sich schreiben als $s = m \cdot n$ mit $m, n \in \mathbb{N}$, wobei $1 < m, n < s$ gilt.
Wir wenden nun einen Spezialfall der geometischen Summenformel an, um einen echten Teiler von $2^s - 1$ zu finden:

$$q^{k+1} - 1 = (q-1) \cdot (q^k + \cdots + q^2 + q + 1)$$

für alle $q \in \mathbb{R}$ und alle $k \in \mathbb{N}$, wobei wir hier $k := n - 1$ und $q := 2^m$ setzen.
Wir erhalten:

$$2^s - 1 = 2^{mn} - 1 = (2^m)^n - 1 = (2^m - 1) \cdot ((2^m)^{n-1} + \cdots + (2^m)^2 + 2^m + 1),$$

wobei $3 \leq 2^2 - 1 \leq 2^m - 1 < 2^s - 1$ ist, da nach Voraussetzung $1 < m < s$ ist.
Also haben wir mit $2^m - 1$ einen echten Teiler von $2^s - 1$ gefunden, weshalb $2^s - 1$ nach Lemma 1.2.2 keine Primzahl sein kann. □

Definition 1.3.17. Zahlen der Form $2^s - 1$ mit $s \in \mathbb{N}$, die Primzahlen sind, nennt man auch *Mersennesche Primzahlen.*

Bemerkung 1.3.18. *Achtung! Nicht alle Zahlen der Form* $2^s - 1$ *mit* $s \in \mathbb{N}$, *wobei* s *Primzahl ist, sind wiederum Primzahlen. Ein Gegenbeispiel ist u. a. bei Übungsaufgabe 3 auf Übungsblatt 3 zu finden:*
$2^{11} - 1$ *ist z. B. keine Primzahl, obwohl* 11 *eine Primzahl ist.*
Bisher (Stand: 6.5.2011) kennt man nur 47 Mersennesche Primzahlen, und es ist ein ungelöstes Problem, ob es unendlich (oder nur endlich) viele Mersennesche Primzahlen gibt.

Im Folgenden betrachten wir weitere Primzahlen, die eine spezielle Form haben.

Definition 1.3.19. Wir nennen die Zahlen der Form $2^s + 1$ mit $s \in \mathbb{N}$, die Primzahlen sind, *Fermatsche Primzahlen.*

Satz 1.3.20. *Sei $s \in \mathbb{N}$. Ist $2^s + 1$ eine Primzahl, so gibt es ein $t \in \mathbb{N}_0$ mit $s = 2^t$.*
(Mit anderen Worten: Ist s keine Zweierpotenz, so ist $2^s + 1$ definitiv keine *Primzahl.)*

Beweis. Wir können $s = m \cdot n$ schreiben, wobei $m = 2^t$ für ein $t \in \mathbb{N}_0$ gilt und n ungerade ist.[2] Wir müssen nun zeigen, dass die Zahl $2^s + 1 = 2^{mn} + 1$ für $n > 1$ keine Primzahl sein kann.

Da n ungerade ist, gilt: $(-1)^n = -1$ und somit

$$2^s + 1 = 1 + (2^m)^n = 1 - (-1) \cdot (2^m)^n = 1 - (-1)^n \cdot (2^m)^n = 1 - (-2^m)^n.$$

Durch Umstellen der geometrischen Summenformel erhalten wir:

$$1 - q^{k+1} = (1 - q) \cdot (1 + q + q^2 + \cdots + q^k)$$

für alle $k \in \mathbb{N}$ und alle $q \in \mathbb{R}$.

Setzen wir dort nun $q := -2^m$ ein und $k := n - 1$, so erhalten wir:

$$2^s + 1 = 1 - (-2^m)^n = (1 + 2^m) \cdot (1 - 2^m + 2^{2m} - 2^{3m} \pm \ldots + 2^{(n-1)m}),$$

wobei $2 = 1 + 2^0 \leq 1 + 2^m < 1 + (2^m)^n = 1 + 2^{mn} = 1 + 2^s$, falls $n > 1$ ist.
Also haben wir mit $1 + 2^m$ einen echten Teiler von $2^s + 1$ gefunden, weshalb $2^s + 1$ nach Lemma 1.2.2 keine Primzahl sein kann.
Also kann, falls $2^s + 1$ eine Primzahl ist, nur $n = 1$ und somit $s = m = 2^t$ mit $t \in \mathbb{N}_0$ sein. □

Bemerkung 1.3.21. *Achtung! Nicht alle Zahlen der Form $2^s + 1$ mit $s \in \mathbb{N}$, wobei s eine 2er-Potenz ist, sind wiederum Primzahlen. Ein Gegenbeispiel ist u. a. bei Übungsaufgabe 3 auf Übungsblatt 4 zu finden:*
$2^{2^5} + 1$ *ist z. B. keine Primzahl.*
Bisher (Stand: 6.5.2011) kennt man nur fünf Fermatsche Primzahlen – nämlich die mit $s \in \{2^0, 2^1, 2^2, 2^3, 2^4\}$ –, und es ist ein ungelöstes Problem, ob es unendlich (oder nur endlich) viele Fermatsche Primzahlen gibt.

1.4 Die Theorie des größten gemeinsamen Teilers

1.4.1 Existenz und Eindeutigkeit

Definition 1.4.1. Seien $a, b \in \mathbb{Z}$. Wir nennen jede Zahl t, für die sowohl $t \mid a$ als auch $t \mid b$ gilt, einen *gemeinsamen Teiler von a und b.*

Eine Zahl $d \in \mathbb{Z}$ heißt *größter gemeinsamer Teiler von a und b*, falls

1. $d \geq 0$, $d \mid a$ und $d \mid b$, und

[2] t ist also gerade die Vielfachheit von 2 in s.

2. für jeden gemeinsamen Teiler t von a und b gilt: $t \mid d$.

Die Frage, die sich nun stellt, ist, ob zu zwei Zahlen a und b jeweils so ein größter gemeinsamer Teiler existiert und ob er eindeutig ist.

Satz 1.4.2. *Seien $a, b \in \mathbb{Z}$. Dann gibt es höchstens einen größten gemeinsamen Teiler von a und b.*

Beweis. Seien d und d' größte gemeinsame Teiler von a und b. Dann gilt insbesondere $d \mid d'$ und $d' \mid d$.

Ist $d = 0$, so muss auch $d' = 0$ sein, denn $0 \mid d'$, da d' ja ein größter gemeinsamer Teiler von a und b ist. Das heißt aber gerade, dass es ein $c \in \mathbb{Z}$ gibt mit $0 \cdot c = d'$. Also ist auch $d' = 0 \cdot c = 0$.

Ist nun $d > 0$, so folgt wegen $d' \mid d$, dass $d' \neq 0$, also $d' > 0$. Dann können wir Korollar 1.1.8 anwenden und erhalten ebenfalls $d = d'$. □

Definition 1.4.3. Wir bezeichnen mit $\mathrm{ggT}(a, b)$ den größten gemeinsamen Teiler von a und b, falls ein solcher existiert.

Satz 1.4.4. *Seien $a, b \in \mathbb{Z}$. Dann haben a und b einen größten gemeinsamen Teiler.*

Beweis. Wir unterscheiden drei wesentlich verschiedene Fälle, in denen wir einen Kandidaten für den größten gemeinsamen Teiler direkt angeben.

Fall 1: $a = 0$ (bzw. $b = 0$)

Behauptung: Dann ist $\mathrm{ggT}(0, b) = |b|$ (bzw. $\mathrm{ggT}(a, 0) = |a|$).

Beweis (der Behauptung):

- $|b| \geq 0$
- $|b| \mid 0$, da ja $|b| \cdot 0 = 0$ für alle $b \in \mathbb{Z}$ ist
- $|b| \mid b$, da ja $b = |b| \cdot 1$, falls $b \geq 0$, und $b = |b| \cdot (-1)$, falls $b < 0$.
- Weiterhin gilt $t \mid |b|$ für jeden Teiler t von b, also erst recht für jeden gemeinsamen Teiler t von 0 und b.

Den zweiten Unterfall zeigt man ganz analog. □

Fall 2: $|a| = 1$ (bzw. $|b| = 1$)

Behauptung: Dann ist $\mathrm{ggT}(a, b) = 1$.

Beweis der (Behauptung):

- $1 \geq 0$
- $1 \mid a$ für alle $a \in \mathbb{Z}$

- $1 \mid b$ für alle $b \in \mathbb{Z}$
- Jeder gemeinsame Teiler t von $a = \pm 1$ und einer beliebigen Zahl $b \in \mathbb{Z}$ ist insbesondere ein Teiler von ± 1. Die einzigen Teiler von ± 1 sind aber 1 und -1. Diese beiden sind aber auch Teiler von jedem $b \in \mathbb{Z}$: $1 \mid b$ für alle $b \in \mathbb{Z}$, da ja $b = 1 \cdot b$ für alle $b \in \mathbb{Z}$ gilt, sowie $-1 \mid b$ für alle $b \in \mathbb{Z}$, da ja $b = (-1) \cdot (-b)$ für alle $b \in \mathbb{Z}$ gilt.

Den zweiten Unterfall zeigt man ganz analog. □

Fall 3: $a, b \in \mathbb{Z}$ mit $|a| > 1$ und $|b| > 1$.

Wir wissen nach dem Hauptsatz der EZT, dass $|a|$ und $|b|$ bis auf die Reihenfolge der Faktoren eindeutige Primfaktorzerlegungen in $\mathbb{N}$ besitzen (mit insgesamt endlich vielen Primfaktoren). Sei $\{p_1, \ldots, p_k\}$ die Menge der *verschiedenen* Primfaktoren p_i, die in $|a|$ oder $|b|$ vorkommen. (Das „verschieden“ soll heißen, dass $p_i \neq p_j$ für alle $i \neq j$ gelten soll.)

Dann können wir $a = \varepsilon(a) \cdot p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ und $b = \varepsilon(b) \cdot p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ mit $m_i, n_i \in \mathbb{N}_0$, $i = 1, \ldots, k$, schreiben, wobei für $c \in \mathbb{Z}$ das Vorzeichen $\varepsilon(c)$ durch

$$\varepsilon(c) := \begin{cases} 1, & \text{falls } c \geq 0 \\ -1, & \text{falls } c < 0 \end{cases}$$

definiert ist. (Bei negativen Zahlen a bzw. b schreiben wir also gerade eine -1 vor die Zahl $|a|$ bzw. $|b|$ und nutzen die Primfaktorzerlegungen von $|a| = -a$ bzw. $|b| = -b$.)

Behauptung: Dann ist

$$\mathrm{ggT}(a, b) = p_1^{\min(m_1, n_1)} \cdot \ldots \cdot p_k^{\min(m_k, n_k)}.$$

Beweis (der Behauptung):

- Natürlich gilt: $p_1^{\min(m_1, n_1)} \cdot \ldots \cdot p_k^{\min(m_k, n_k)} \geq 0$, da ja alle $p_i \geq 0$, $i = 1, \ldots, k$.
- Die Zahl $p_1^{\min(m_1, n_1)} \cdot \ldots \cdot p_k^{\min(m_k, n_k)}$ ist nach der Charakterisierung der Teiler aus Satz 1.3.1 ein Teiler von a, da $\min(m_i, n_i) \leq m_i$ für alle $i = 1, \ldots, k$ ist.
- Die Zahl $p_1^{\min(m_1, n_1)} \cdot \ldots \cdot p_k^{\min(m_k, n_k)}$ ist nach der Charakterisierung der Teiler aus Satz 1.3.1 ein Teiler von b, da $\min(m_i, n_i) \leq n_i$ für alle $i = 1, \ldots, k$ ist.
- Jeder gemeinsame Teiler t von a und b ist nach der Charakterisierung der Teiler aus Satz 1.3.1 von der Form $t = \varepsilon(t) \cdot p_1^{\ell_1} \cdot \ldots \cdot p_k^{\ell_k}$ mit $0 \leq \ell_i \leq m_i$ und $0 \leq \ell_i \leq n_i$ für alle $i = 1, \ldots, k$, also $0 \leq \ell_i \leq \min(m_i, n_i)$ für alle $i = 1, \ldots, k$. Dann ist t (wiederum nach der Charakterisierung der Teiler aus Satz 1.3.1) aber auch ein Teiler von $p_1^{\min(m_1, n_1)} \cdot \ldots \cdot p_k^{\min(m_k, n_k)}$

□
□

1.4.2 Der Euklidische Algorithmus

Zur Existenz und Eindeutigkeit des größten gemeinsamen Teilers zweier Zahlen $a, b \in \mathbb{Z}$ haben wir die Eindeutigkeit der Primfaktorzerlegung in den natürlichen Zahlen benutzt. Es gibt aber (noch) keine effektiven Verfahren, um die Primfaktorzerlegung einer Zahl zu berechnen. Daher hier nun eine andere Möglichkeit, den größten gemeinsamen Teiler zweier ganzer Zahlen zu berechnen: der Euklidische Algorithmus.
Das Verfahren beruht auf der *Division mit Rest*:

Lemma 1.4.5 (Division mit Rest)**.** *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit $b \leq |a|$. Dann gibt es $q, r \in \mathbb{Z}$, $0 \leq r < b$, mit*

$$a = qb + r.$$

Die beiden Zahlen q und r sind durch a und b eindeutig bestimmt.

Die Division mit Rest wenden wir nun wie folgt an:

Satz 1.4.6 (Euklidischer Algorithmus)**.** *Seien $a, b \in \mathbb{N}$ mit $a \geq b$. Wir setzen $a_0 := a$ und $a_1 := b$ und führen sukzessive folgende Divisionen mit Rest durch:*

- $a_0 = q_1 a_1 + a_2$ *mit* $0 \leq a_2 < a_1$,
- $a_1 = q_2 a_2 + a_3$ *mit* $0 \leq a_3 < a_2$,
- $\ldots$
- $a_{k-1} = q_k a_k + a_{k+1}$ *mit* $0 \leq a_{k+1} < a_k$,
- $\ldots$,

solange $a_k \neq 0$ gilt.
Dann gibt es einen Index $n \in \mathbb{N}$ mit $a_n > 0$ und $a_{n+1} = 0$.
Die Zahl a_n ist dann der größte gemeinsame Teiler von a und b.

Beweis. Der Index n existiert, weil die Reste a_k immer (in jedem Schritt um mindestens 1) kleiner werden, aber nicht-negativ sind:

$$b = a_1 > a_2 > a_3 > \ldots \geq 0,$$

wobei alle $a_k \in \mathbb{N}_0$ sind. (Also gilt nach spätestens b Schritten: $a_{b+1} = 0$.)

Im $(n+1)$-ten Schritt haben wir dann $a_{n-1} = q_n a_n$, da ja $a_{n+1} = 0$ ist. Daher ist $a_n \mid a_{n-1}$.
In dem vorangegangenen Schritt ist $a_{n-2} = q_{n-1} a_{n-1} + a_n$, also, da $a_n \mid a_n$ und $a_n \mid a_{n-1}$, nach Lemma 1.1.3, Teil 4, auch $a_n \mid a_{n-2} = q_{n-1} a_{n-1} + a_n$.
Per Induktion erhalten wir nun $a_n \mid a_{n-1}$, $a_n \mid a_{n-2}$, $\ldots$, $a_n \mid a_2$, $a_n \mid a_1 = b$ und $a_n \mid a_0 = a$.
Damit ist a_n ein (nach Konstruktion nicht-negativer) gemeinsamer Teiler von a und b.

Wir müssen nun noch zeigen, dass a_n der größte gemeinsame Teiler von a und b ist, dass also jeder andere gemeinsame Teiler t von a und b auch die Zahl a_n teilt.
Sei t ein gemeinsamer Teiler von $a = a_0$ und $b = a_1$. Dann ist nach Lemma 1.1.3, Teil 4, $t \mid a_2 = a_0 - q_1 a_1$, und per Induktion und mit dem Lemma 1.1.3, Teil 4, erhalten wir $t \mid a_n = a_{n-2} - q_{n-1} a_{n-1}$. □

Bemerkung 1.4.7. *Wir können nun beliebige größte gemeinsame Teiler zweier ganzer Zahlen berechnen. Ist $a = 0$ (bzw. $b = 0$), so haben wir schon gesehen, dass dann $\mathrm{ggT}(a, b) = |b|$ (bzw. $\mathrm{ggT}(a, b) = |a|$) ist. Ansonsten berechnen wir den größten gemeinsamen Teiler d von $|a|$ und $|b|$ mit Hilfe des Euklidischen Algorithmus. Dieses d ist dann auch der größte gemeinsame Teiler von a und b, da die Menge aller Teiler von $|c|$ und die Menge aller Teiler von c ja für jedes (fest gewählte) $c \in \mathbb{Z}$ übereinstimmen.*

Beispiel 1.4.8. *Wir bestimmen den größten gemeinsamen Teiler von 48 und 26 mit Hilfe des euklidischen Algorithmus.*

$$48 = 1 \cdot 26 + 22,$$
$$26 = 1 \cdot 22 + 4,$$
$$22 = 5 \cdot 4 + 2,$$
$$4 = 2 \cdot 2 + 0$$

Also ist $\mathrm{ggT}(48, 26) = 2$.

Bemerkung 1.4.9. *Alternativ hätten wir bei Beispiel 1.4.8 auch die Primfaktorzerlegungen von 48 und 26 benutzen können:*

$$48 = 2^4 \cdot 3 = 2^4 \cdot 3^1 \cdot 13^0, \quad 26 = 2 \cdot 13 = 2^1 \cdot 3^0 \cdot 13^1,$$

also

$$\mathrm{ggT}(48, 26) = 2^{\min(4,1)} \cdot 3^{\min(1,0)} \cdot 13^{\min(0,1)} = 2^1 \cdot 3^0 \cdot 13^0 = 2$$

(nach Satz 1.4.4).

Sind die Zahlen jedoch größer, so ist es i. a. schwierig, die Primfaktorzerlegungen (oder auch nur eine der beiden Primfaktorzerlegungen) auszurechnen.

1.4.3 Das kleinste gemeinsame Vielfache

Definition 1.4.10. Seien $a, b \in \mathbb{Z}$. Wir nennen jede Zahl u, für die sowohl $a \mid u$ als auch $b \mid u$ gilt, ein *gemeinsames Vielfaches von a und b.*

Eine Zahl $v \in \mathbb{Z}$ heißt *kleinstes gemeinsames Vielfaches von a und b*, falls

1. $v \geq 0$, $a \mid v$ und $b \mid v$, und
2. für jedes gemeinsame Vielfache u von a und b gilt: $v \mid u$.

Wie beim größten gemeinsamen Teiler zweier Zahlen a und b kann man nun zeigen – die Beweise verlaufen (fast) vollkommen analog:

Satz 1.4.11. *Seien $a, b \in \mathbb{Z}$. Dann gibt es höchstens ein kleinstes gemeinsames Vielfaches von a und b.*

Definition 1.4.12. Wir bezeichnen mit $\mathrm{kgV}(a, b)$ das kleinste gemeinsame Vielfache von a und b, falls ein solches existiert.

Satz 1.4.13. *Seien $a, b \in \mathbb{Z}$. Dann haben a und b ein kleinstes gemeinsames Vielfaches.*

1.4.4 Hauptsatz über den größten gemeinsamen Teiler

In diesem Abschnitt zeigen wir, dass sich der größte gemeinsame Teiler d zweier ganzer Zahlen a und b immer als *ganzzahlige Linearkombination von a und b* schreiben lässt. Das heißt, dass es zwei ganze Zahlen x und y gibt mit

$$d = x \cdot a + y \cdot b.$$

Satz 1.4.14. *Sei $n \in \mathbb{N}$ und seien $a_1, \ldots, a_n \in \mathbb{Z}$. Wir betrachten die Menge*

$$I := I(a_1, \ldots, a_n) := \{z \in \mathbb{Z} \mid \text{es gibt } x_1, \ldots, x_n \in \mathbb{Z} \text{ mit } z = x_1 \cdot a_1 + \ldots + x_n \cdot a_n\}$$

. Es gilt:

- *Sind $z, z' \in I$, so ist auch $z - z' \in I$.*
- *Ist $z \in I$ und $x \in \mathbb{Z}$, so ist auch $x \cdot z \in I$.*

Beweis. Übung 1, Übungsblatt 6. □

Lemma 1.4.15. *Seien $a, b \in \mathbb{Z}$, so dass es ein $d \in \mathbb{N}_0$ gibt mit $I(a, b) = I(d)$, so ist d der größte gemeinsame Teiler von a und b. Insbesondere gibt es dann $x, y \in \mathbb{Z}$ mit*

$$x \cdot a + y \cdot b = d.$$

Beweis. Wir rechnen nach, dass d wirklich der größte gemeinsame Teiler von a und b ist:

- Nach Voraussetzung ist $d \geq 0$.
- Da $a = 1 \cdot a + 0 \cdot b \in I(a, b) = I(d)$, gibt es also ein $r \in \mathbb{Z}$ mit $a = r \cdot d$. Daher gilt: $d \mid a$.
- Da $b = 0 \cdot a + 1 \cdot b \in I(a, b) = I(d)$, gibt es also ein $s \in \mathbb{Z}$ mit $b = s \cdot d$. Daher gilt: $d \mid b$.
- Ist t ein gemeinsamer Teiler von a und b, also $t \mid a$ und $t \mid b$, so gilt nach Lemma 1.1.3, Teil 4, auch: $t \mid x \cdot a + y \cdot b$ für alle $x, y \in \mathbb{Z}$. Da aber $d \in I(d) = I(a, b)$ nach Voraussetzung von der Form $d = \tilde{x} \cdot a + \tilde{y} \cdot b$ mit $\tilde{x}, \tilde{y} \in \mathbb{Z}$ ist, gilt insbesondere auch $t \mid d$.

□

Lemma 1.4.16. *Sei $\{0\} \neq M \subseteq \mathbb{Z}$ eine Menge, für die die folgenden Eigenschaften gelten:*

- *Sind $z, z' \in M$, so ist auch $z - z' \in M$.*
- *Ist $z \in M$ und $x \in \mathbb{Z}$, so ist auch $x \cdot z \in M$.*

Sei d die kleinste positive Zahl mit $d \in M$.
Dann ist $M = I(d)$, die Menge aller ganzzahligen Vielfachen von d.

Beweis. $\underline{M \subseteq I(d)}$:
Sei $c \in M$. Dann gilt auch $-c \in M$. Da $M \neq \{0\}$, können wir auch $c \neq 0$ wählen. Es gibt also positive Zahlen in M, da $M \neq \{0\}$, und damit auch eine kleinste, die wir d nennen.

Sei nun $z \in M$ beliebig. Durch Division mit Rest erhalten wir eine Darstellung

$$z = q_z \cdot d + r_z,$$

wobei $q_z, r_z \in \mathbb{Z}$ mit $0 \leq r_z < d$ sind. Wir zeigen nun, dass die so entstehenden Reste r_z immer $= 0$ sind.

Da $d \in M$, ist nach Voraussetzung auch $q_z \cdot d \in M$, also auch $r_z = z - q_z \cdot d \in M$. Da aber $0 \leq r_z < d$ und d die kleinste positive Zahl in M ist, muss $r_z = 0$ gelten.

Daher liegt jedes $z \in M$ automatisch auch in $I(d)$. (Denn $z = q_z \cdot d$ mit ganzzahligem q_z, da ja die jeweiligen Reste $r_z = 0$ sind.)

$\underline{I(d) \subseteq M}$:
Umgekehrt liegt natürlich auch jedes $z \in I(d)$, also jedes ganzzahlige Vielfache von d, in der Menge M (nach der zweiten Eigenschaft der Menge M), denn wir haben ja $d \in M$. □

Satz 1.4.17 (Hauptsatz über den größten gemeinsamen Teiler)**.** *Seien $a, b, d \in \mathbb{Z}$. Dann sind die folgenden Aussagen äquivalent:*

1. $d \geq 0$ *und* $I(a, b) = I(d)$
2. $d = \mathrm{ggT}(a, b)$

Beweis. $\underline{1. \Rightarrow 2.}$: Das ist gerade die Aussage aus Lemma 1.4.15.

$\underline{2. \Rightarrow 1.}$: Falls $I(a, b) \neq \{0\}$ ist, gibt es nach Lemma 1.4.16 immer ein $d \in \mathbb{N}$ mit $I(a, b) = I(d)$, denn $I(a, b)$ ist nach Satz 1.4.14 gerade so eine Teilmenge der ganzen Zahlen, die die Bedingungen wie das M in dem Lemma 1.4.16 erfüllt. Nach Lemma 1.4.15 muss dieses d, so es denn überhaupt existiert, automatisch der $\mathrm{ggT}(a, b)$ sein, und wir erhalten, dass $I(a, b) = I(\mathrm{ggT}(a, b))$ ist.
Ist $I(a, b) = \{0\}$, so ist natürlich $I(a, b) = I(0) = \{0\}$; wir können in diesem Fall also $d = 0$ wählen. Auch dieses d ist automatisch der $\mathrm{ggT}(a, b)$, denn die einzige Möglichkeit, bei der $I(a, b) = \{0\}$ auftreten kann, ist, wenn schon $a = b = 0$ ist. Damit ist auch hier $I(a, b) = I(\mathrm{ggT}(a, b))$. □

Beispiel 1.4.18.

- $a = 2$, $b = 3$. *Dann ist nach Satz 1.4.17*

$$I(2, 3) = \{z \in \mathbb{Z} \mid \textit{es gibt } x, y \in \mathbb{Z} \textit{ mit } z = x \cdot 2 + y \cdot 3\} = I(1) = \mathbb{Z},$$

da $\mathrm{ggT}(2, 3) = 1$.

- $a = 4$, $b = 6$. *Dann ist nach Satz 1.4.17*

$$I(4,6) = \{z \in \mathbb{Z} \mid \textit{es gibt } x, y \in \mathbb{Z} \textit{ mit } z = x \cdot 4 + y \cdot 6\}$$
$$= I(2) = \{z \in \mathbb{Z} \mid \textit{es gibt } s \in \mathbb{Z} \textit{ mit } z = s \cdot 2\},$$

also die Menge der geraden Zahlen, da $\mathrm{ggT}(4,6) = 2$.

Beispiel 1.4.19 (Auflösung durch den Euklidischen Algorithmus)**.**

- $a = 3$, $b = 2$. *Dann ist:*

$$3 = 1 \cdot 2 + 1,$$
$$2 = 2 \cdot 1(+0).$$

Also

$$1 = 1 \cdot 3 - 1 \cdot 2.$$

- $a = 6$, $b = 4$. *Dann ist:*

$$6 = 1 \cdot 4 + 2,$$
$$4 = 2 \cdot 2(+0).$$

Also

$$2 = 1 \cdot 6 - 1 \cdot 4.$$

- $a = 48$, $b = 26$. *Dann ist:*

$$48 = 1 \cdot 26 + 22,$$
$$26 = 1 \cdot 22 + 4,$$
$$22 = 5 \cdot 4 + 2,$$
$$4 = 2 \cdot 2(+0)$$

Also

$$\begin{aligned} 2 &= 1 \cdot 22 - 5 \cdot 4 && \textit{(3. Gleichung)} \\ &= 1 \cdot 22 - 5 \cdot (1 \cdot 26 - 1 \cdot 22) && \textit{(2. Gleichung)} \\ &= 1 \cdot (1 \cdot 48 - 1 \cdot 26) - 5 \cdot (1 \cdot 26 - 1 \cdot (1 \cdot 48 - 1 \cdot 26)) && \textit{(1. Gleichung)} \\ &= 6 \cdot 48 - 11 \cdot 26 && \textit{(ausgerechnet)} \end{aligned}$$

- $a = k \cdot b$. *Dann ist:*

$$a = k \cdot a + 0$$

(und wir erhalten hier keine „vorletzte“ Zeile im Euklidischen Algorithmus). Aber

$$\mathrm{ggT}(a,b) = b.$$

Also $b = 0 \cdot a + k \cdot b$.

- *$a = 12$, $b = 6$. Dann ist:*

$$12 = 2 \cdot 6$$

und

$$6 = \mathrm{ggT}(12, 6).$$

Also

$$6 = 0 \cdot 12 + 1 \cdot 6.$$

Bemerkung 1.4.20. *Wir haben gesehen, dass uns der Hauptsatz über den größten gemeinsamen Teiler zweier Zahlen für deren größten gemeinsamen Teiler immer eine Darstellung als ganzzahlige Linearkombination aus den beiden Zahlen liefert. Ganz allgemein können wir den größten gemeinsamen Teiler zweier ganzer Zahlen a und b als ganzzahlige Linearkombination derselben darstellen, indem wir den Euklidischen Algorithmus erweitern.*

Im Fall, dass $b = 0$ ist, ist $\mathrm{ggT}(a, b) = |a|$, also zum Beispiel

$$\mathrm{ggT}(a, b) = \pm 1 \cdot a + 0 \cdot b.$$

Insbesondere haben wir in diesem Fall eine Darstellung von $\mathrm{ggT}(a, b)$ als ganzzahlige Linearkombination von a und b gefunden. (Analog für den Fall $a = 0$.) Wir beschränken uns daher auf den Fall, dass beide *Zahlen $a \neq 0$ und $b \neq 0$ sind. Weiterhin können wir $a, b \in \mathbb{N}$ wählen, denn falls $b < 0$, so ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, -b)$, und haben wir eine Darstellung*

$$\mathrm{ggT}(a, -b) = \tilde{x} \cdot a + \tilde{y} \cdot (-b)$$

mit $\tilde{x}, \tilde{y} \in \mathbb{Z}$ gefunden, so ist natürlich

$$\mathrm{ggT}(a, b) = \tilde{x} \cdot a + (-\tilde{y}) \cdot b$$

eine Darstellung als ganzzahlige Linearkombination von a und b. (Entsprechend für $a < 0$.)

Satz 1.4.21 (Erweiterter Euklidischer Algorithmus/Lemma von Bézout)**.** *Seien $a_0 \in \mathbb{Z}, a_1 \in \mathbb{N}$ mit $a_0 \neq 0$ und $a_1 \leq |a_0|$.*

Mit Hilfe des Euklidischen Algorithmus erhalten wir folgende Gleichungen:

$$\begin{aligned} a_0 &= q_1 \cdot a_1 + a_2, \\ a_1 &= q_2 \cdot a_2 + a_3, \\ &\vdots \\ a_{n-2} &= q_{n-1} \cdot a_{n-1} + a_n, \\ a_{n-1} &= q_n \cdot a_n + a_{n+1}, \end{aligned}$$

wobei $q_1, \ldots, q_n, a_2, \ldots, a_n \in \mathbb{Z}$ sind mit $0 \leq a_{i+1} < a_i$ für alle $i = 1, \ldots, n$ und $a_{n+1} = 0$. Dann lässt sich $a_n = \mathrm{ggT}(a_0, a_1)$ mit Hilfe dieser Gleichungen als ganzzahlige Linearkombination von a_0 und a_1 schreiben.

Beweis. Ist schon $a_1 \mid a_0$, so ist

$$\text{ggT}(a_0, a_1) = a_1 = 0 \cdot a_0 + 1 \cdot a_1.$$

Sonst stellen wir die Gleichungen um und beginnen mit der vorletzten Gleichung:

$$a_n = a_{n-2} - q_{n-1} \cdot a_{n-1},$$

die uns eine ganzzahlige Linearkombination von a_n aus den beiden Zahlen a_{n-2} und a_{n-1} liefert.

Ist nun bereits

$$a_n = \hat{x} \cdot a_{n-k} + \hat{y} \cdot a_{n-k-1}$$

mit $\hat{x}, \hat{y} \in \mathbb{Z}$ – also a_n eine ganzzahlige Linearkombination von a_{n-k} und a_{n-k-1} – und

$$a_{n-k} = a_{n-k-2} - q_{n-k-1} a_{n-k-1},$$

was wir durch Umstellung der Gleichungen aus dem Euklidischen Algorithmus erhalten, so ist natürlich auch

$$\begin{aligned} a_n &= \hat{x} \cdot (a_{n-k-2} - q_{n-k-1} a_{n-k-1}) + \hat{y} \cdot a_{n-k-1} \\ &= \hat{x} \cdot a_{n-k-2} + (\hat{y} - \hat{x} \cdot q_{n-k-1}) \cdot a_{n-k-1}, \end{aligned}$$

also a_n eine ganzzahlige Linearkombination von a_{n-k-2} und a_{n-k-1}.
(Wir haben also mit Hilfe einer (umgestellten) Gleichung aus dem Euklidischen Algorithmus aus der Darstellung von a_n als ganzzahlige Linearkombination von a_{n-k} und a_{n-k-1} eine Darstellung von a_n als ganzzahlige Linearkombination von a_{n-k-1} und a_{n-k-2} hergestellt.)

Für $k = n - 2$ erhalten wir so eine Darstellung von $\text{ggT}(a_0, a_1) = a_n$ als ganzzahlige Linearkombination von a_0 und a_1. □

Satz 1.4.22. *Seien $a, b, c \in \mathbb{Z}$ mit $\text{ggT}(a, b) \neq 0$.*

Ist (x_0, y_0) irgendeine Lösung der linearen Gleichung $ax + by = c$ (in den Variablen x und y), so ist die Lösungsmenge der Gleichung genau die Menge

$$\left\{ \left(x_0 + \frac{kb}{ggT(a,b)}, y_0 - \frac{ka}{ggT(a,b)} \right) \mid k \in \mathbb{Z} \right\}.$$

Beweis. Dass all diese Paare von ganzen Zahlen Lösungen der linearen Gleichung sind, kann man nachrechnen (s. Übungsaufgabe 1, Übungsblatt 7).
Etwas schwieriger ist es zu zeigen, dass alle Lösungen so erhalten werden können. *[Beweisidee folgt...]* □

Bemerkung 1.4.23. *Die lineare Gleichung $ax + by = c$ mit $a, b, c \in \mathbb{Z}$ braucht keine Lösung zu haben. Eine Lösung hat sie (nach Satz 1.4.17) genau dann, wenn* $\mathrm{ggT}(a, b) \mid c$ *ist.*

Hat die Gleichung eine Lösung, so können wir eine Lösung mit Hilfe des erweiterten Euklischen Algorithmus berechnen, und Satz 1.4.22 liefert uns dann alle *Lösungen der Gleichung.*

Beispiel 1.4.24. *Wir suchen alle ganzzahligen Lösungen der Gleichung*

$$30x + 14y = 2.$$

Eine Lösung erhalten wir durch den Euklidischen Algorithmus:

$$30 = 2 \cdot 14 + 2$$

$$14 = 7 \cdot 2 + 0$$

Die vorletzte Zeile ergibt:

$$2 = 30 \cdot 1 + 14 \cdot (-2),$$

also ist $(x_0, y_0) := (1, -2)$ *eine Lösung der Gleichung in den Variablen x und y.*
Weitere Lösungen finden wir, indem wir Satz 1.4.22 anwenden, etwa mit:

$k = 1$*:*
$(1 + 14, -2 - 30) = (15, -32)$*, Einsetzen liefert:* $30 \cdot 15 + 14 \cdot (-32) = 450 - 448 = 2$

$k = 2$*:*
$(1 + 28, -2 - 60) = (29, -62)$*, Einsetzen liefert:* $30 \cdot 29 + 14 \cdot (-62) = 870 - 868 = 2$

$k = -3$*:*
$(1 - 42, -2 + 90) = (-41, 88)$*, Einsetzen liefert:* $30 \cdot (-41) + 14 \cdot 88 = -1230 + 1232 = 2$

1.5 Diophantische Gleichungen

1.5.1 Lineare diophantische Gleichungen

Bemerkung 1.5.1. *Im letzten Abschnitt haben wir gesehen, wir man ganzzahlige Lösungen linearer Gleichungen in zwei Variablen berechnen kann. Entsprechend kann man auch die ganzzahlige Lösungen linearer Gleichungen in mehr als zwei Variablen berechnen, wenn man für n ganze Zahlen $a_1, \ldots, a_n \in \mathbb{Z}$ den* $\mathrm{ggT}(a_1, \ldots, a_n)$ *rekursiv durch*

$$\mathrm{ggT}(a_1, \ldots, a_n) := \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$$

definiert (und sich davon überzeugt, dass das ganze nicht von der Reihenfolge der a_i, $i = 1, \ldots, n$, abhängig ist). Dabei soll dann $\mathrm{ggT}(a_1) = a_1$ *sein, falls $n = 1$ ist, und* $\mathrm{ggT}(a_1, a_2)$ *so definiert sein wie oben.*

Ebenso kann man auch (durch mehrfaches Anwenden des erweiterten Euklidischen Algorithmus) $\mathrm{ggT}(a_1, \ldots, a_n)$ *als ganzzahlige Linearkombination von* $a_1, \ldots, a_n$ *darstellen, also* $x_1, \ldots, x_n \in \mathbb{Z}$ *finden mit*

$$\mathrm{ggT}(a_1, \ldots, a_n) = x_1 a_1 + \ldots + x_n a_n.$$

Eine Übungsaufgabe dazu ist auf dem Übungsblatt 7 (Aufgabe 3) zu finden.

Definition 1.5.2. Wir nennen eine polynomielle Gleichung in den Variablen $x_1, \ldots, x_n$ eine *diophantische Gleichung*, wenn wir nach ganzzahligen Lösungen dieser Gleichung suchen. Eine *polynomielle Gleichung* ist dabei eine Gleichung der Form $p(x_1, \ldots, x_n) = 0$, wobei p ein Polynom in den Variablen $x_1, \ldots, x_n$ ist.

1.5.2 Quadratische diophantische Gleichungen

Der Große Satz von Fermat besagt z. B., dass die diophantische Gleichung $x^n + y^n = z^n$ in den Variablen x, y, z keine *nicht-trivialen* ganzzahligen Lösungen hat, falls $n > 2$ ist. Der Beweis ist jedoch so umfangreich und umfasst mathematische Hilfsmittel, die wir hier nicht bereitstellen können, so dass wir hier darauf verzichten.

Wir befassen uns im Folgenden mit den Lösungen der quadratischen diophantischen Gleichung

$$x^2 + y^2 = z^2$$

in den Variablen x, y, z. (Diese nennt man auch *pythagoräische Tripel*.)

Bemerkung 1.5.3. *Mit jeder Lösung* (x_0, y_0, z_0) *der Gleichung* $x^2 + y^2 = z^2$ *ist natürlich auch jedes* $(k \cdot x_0, k \cdot y_0, k \cdot z_0)$ *(mit* $k \in \mathbb{R}$*) eine (nicht unbedingt ganzzahlige) Lösung der Gleichung.*

Weiterhin erhalten wir aus jeder ganzzahligen Lösung (x_0, y_0, z_0) *insgesamt acht ganzzahlige Lösungen der Gleichung, indem wir die Vorzeichen von* x_0*,* y_0 *und* z_0 *wechseln.*

Man kann zeigen:

Lemma 1.5.4. *Ist* (x_0, y_0, z_0) *eine Lösung der diophantischen Gleichung* $x^2 + y^2 = z^2$*, so gilt* $\mathrm{ggT}(x_0, y_0) \mid z_0$.

Beweis. Übungsaufgabe 1, Übungsblatt 8. □

Bemerkung 1.5.5. *Haben wir eine gannzahlige Lösung* (x_0, y_0, z_0) *der Gleichung* $x^2 + y^2 = z^2$ *gefunden, so ist nach Bemerkung 1.5.3 und Lemma 1.5.4 auch* $\left(\frac{x_0}{\mathrm{ggT}(x_0,y_0)}, \frac{y_0}{\mathrm{ggT}(x_0,y_0)}, \frac{z_0}{\mathrm{ggT}(x_0,y_0)}\right)$ *eine ganzzahlige Lösung der Gleichung.*

Definition 1.5.6. Wir nennen eine Lösung (x_0, y_0, z_0) der diophantischen Gleichung $x^2 + y^2 = z^2$ eine *Fundamentallösung*, wenn $\mathrm{ggT}(x_0, y_0) = 1$ ist.

Lemma 1.5.7. *Ist (x_0, y_0, z_0) eine Fundamentallösung der diophantischen Gleichung $x^2 + y^2 = z^2$, so ist genau eine der Zahlen x_0 und y_0 gerade.*

Beweis (durch Kontraposition). Falls x_0 und y_0 *beide* gerade sind, so ist $\mathrm{ggT}(x_0, y_0) \geq 2 \neq 1$, da ja 2 ein gemeinsamer Teiler von x_0 und y_0 ist (und $\mathrm{ggT}(x_0, y_0)$ der zahlenmäßig größte unter allen gemeinsamen Teilern). Damit ist (x_0, y_0, z_0) (nach Definition) keine Fundamentallösung.

Falls x_0 und y_0 *beide* ungerade sind, so gibt es $m, n \in \mathbb{Z}$, so dass $x_0 = 2m+1$ und $y_0 = 2n+1$ gilt. Wäre nun (x_0, y_0, z_0) eine Fundamentallösung (und damit eine ganzzahlige Lösung) von $x^2 + y^2 = z^2$, so wäre $z_0^2 = x_0^2 + y_0^2 = (2m+1)^2 + (2n+1)^2 = 4 \cdot (m^2 + m + n^2 + n) + 2$.

Wir zeigen nun: „Eine Quadratzahl hat beim Teilen durch 4 niemals Rest 2."

Fall 1: z_0 ist ungerade. Dann gibt es ein $a \in \mathbb{Z}$ mit $z_0 = 2a + 1 \Rightarrow z_0^2 = (2a + 1)^2 = 4 \cdot (a^2 + a) + 1$, also Rest 1 (beim Teilen durch 4)

Fall 2: z_0 ist gerade. Dann gibt es ein $a \in \mathbb{Z}$ mit $z_0 = 2a \Rightarrow z_0^2 = (2a)^2 = 4 \cdot a^2$, also Rest 0 (beim Teilen durch 4)

Also kann (x_0, y_0, z_0) keine ganzzahlige Lösung der Gleichung $x^2 + y^2 = z^2$ sein, also auch keine Fundamentallösung. □

Man kann die Fundamentallösungen (bis auf die Vorzeichen und Vertauschung der Rollen von x und y) nun wie folgt charakterisieren:

Satz 1.5.8. *Sei (x_0, y_0, z_0) eine Lösung der diophantischen Gleichung $x^2 + y^2 = z^2$, so dass $x_0, y_0, z_0 \in \mathbb{N}_0$ sind und x_0 gerade ist. Dann sind die folgenden Aussagen äquivalent:*

- *(x_0, y_0, z_0) ist eine Fundamentallösung.*
- *Es gibt $m, n \in \mathbb{N}_0$ mit $\mathrm{ggT}(m, n) = 1$, wobei genau eines von m und n gerade ist, so dass*
$$x_0 = 2mn, \quad y_0 = m^2 - n^2 \quad \text{und} \quad z_0 = m^2 + n^2$$
gilt.

Der Beweis ist genauso wie der von Satz 1.4.22 etwas länger.

2 Zahlentheorie in allgemeineren Ringen

2.1 Ringe

Nachdem wir nun einige Kapitel zur Zahlentheorie in den ganzen Zahlen gesehen haben, wird es im Folgenden darum gehen, sich davon zu überzeugen, dass viele Dinge auch auf allgemeinere Ringe übertragbar sind, und zu sehen, dass gewisse andere Dinge nicht funktionieren.

Definition 2.1.1. Eine Menge R mit zwei Verknüpfungen $+ : R \times R \to R$ (Addition) und $\cdot : R \times R \to R$ (Multiplikation) heißt *Ring*, falls die Verknüpfungen folgende Bedingungen erfüllen:

- $r_1 + r_2 = r_2 + r_1$ (Kommutativgesetz der Addition)
- $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$ für alle $r_1, r_2, r_3 \in R$ (Assoziativgesetz der Addition)
- es gibt ein Element $n \in R$ mit $r + n = n + r = r$ für alle $r \in R$ (neutrales Element bzgl. der Addition)
- zu jedem $r \in R$ gibt es ein $r' \in R$ mit $r + r' = r' + r = 0$ (inverse Elemente bzgl. der Addition)
- $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$ für alle $r_1, r_2, r_3 \in R$ (Assoziativgesetz der Multiplikation)
- es gibt ein Element $e \in R$ mit $r \cdot e = e \cdot r = r$ für alle $r \in R$ (neutrales Element bzgl. der Multiplikation)
- $(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$ und $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$ für alle $r_1, r_2, r_3 \in R$ (Distributivgesetze)

Gilt zusätzlich $r_1 \cdot r_2 = r_2 \cdot r_1$, so nennen wir den Ring R *kommutativ*.
Folgt aus $r_1 \cdot r_2 = n$ mit $r_1, r_2 \in R$ stets $r_1 = n$ oder $r_2 = n$, so nennen wir den Ring *nullteilerfrei*.

Lemma 2.1.2. *Sei $(R, +, \cdot)$ ein Ring. Dann gilt:*

- *n und e sind eindeutig bestimmt.*
- *Zu jedem $r \in R$ ist auch r' eindeutig bestimmt.*
- *Ist der Ring nullteilerfrei, so folgt aus $r_1 \cdot r_2 = r_1 \cdot r_3$ und $r_1 \neq 0$ stets $r_2 = r_3$. (Kürzungsregel)*

Beweis. Übungsaufgabe 2, Übungsblatt 8. □

Beispiel 2.1.3.

- *Die ganzen Zahlen bilden bzgl. ihrer Addition und Multiplikation einen (nullteilerfreien) kommutativen Ring.*
- *Die rationalen Zahlen bilden bzgl. ihrer Addition und Multiplikation einen (nullteilerfreien) kommutativen Ring.*
- *Die reellen Zahlen bilden bzgl. ihrer Addition und Multiplikation einen (nullteilerfreien) kommutativen Ring.*
- *Die natürlichen Zahlen bilden bzgl. ihrer Addition und Multiplikation* keinen *Ring. (Es gibt keine additiv inversen Elemente.)*
- *Die Paare von ganzen Zahlen bilden mit komponentenweiser Addition und Multiplikation einen kommutativen Ring, der nicht nullteilerfrei ist. (Hier gilt z. B.:* $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$*.)*

2.1.1 Polynomringe

Falls nichts anderes gesagt wird, bezeichnen wir in dem Rest dieses Kapitels mit n das additiv neutrale Element eines Rings R.

Definition 2.1.4. Ein *Polynom* in der Variablen X über einem Ring R ist ein Ausdruck der Form

$$r_0 + r_1X + r_2X^2 + r_3X^3 + \ldots + r_mX^m,$$

wobei $r_0, \ldots, r_m \in R$ und $m \in \mathbb{N}_0$ ist.

Zwei Polynome $f := r_0 + r_1X + r_2X^2 + r_3X^3 + \ldots + r_mX^m$ und $g := s_0 + s_1X + s_2X^2 + s_3X^3 + \ldots + s_\ell X^\ell$ in der Variablen X über dem Ring R sind genau dann *gleich*, wenn $m = \ell$ und $r_i = s_i$ für alle $i = 0, \ldots, m$ gilt.

Die Menge alle Polynome in X über R bezeichnen wir mit $R[X]$.

Wir definieren eine *Addition* auf $R[X]$ durch

$$f + g := (r_0 + s_0) + (r_1 + s_1)X + \ldots + (r_{\max(m,\ell)} + s_{\max(m,\ell)})X^{\max(m,\ell)},$$

wobei wir $r_i := n$ und $s_j := n$ setzen für $i > m$ und $j > \ell$.

Wir definieren außerdem eine *Multiplikation* auf $R[X]$ durch

$$f \cdot g := r_0 \cdot s_0 + (r_1s_0 + r_0s_1)X + (r_2s_0 + r_1s_1 + r_0s_2)X^2 + (r_3s_0 + r_2s_1 + r_1s_2 + r_0s_3)X^3$$
$$+ \ldots + (r_{m+\ell}s_0 + r_{m+\ell-1}s_1 + \ldots + r_1s_{m+\ell-1} + r_0s_{m+\ell})X^{m+\ell},$$

wobei wir $r_i := n$ und $s_j := n$ setzen für $i > m$ und $j > \ell$.

Lemma 2.1.5. *Mit der oben angegebenen Addition und Multiplikation ist $R[X]$ ein Ring.*

Beweis. Übungsaufgabe 3, Übungsblatt 8. (Insbesondere ist es wichtig, sich zu überlegen, wie die neutralen Elemente sowie zu jedem Element das additiv inverse Element aussehen.) □

Beispiel 2.1.6. *Sei $R := \mathbb{Z}$ und $f := 1 + X$, $g := 2 - 5X + 4X^2$. (Dann sind $f, g \in R[X]$.)*

- $f + g = (1 + X) + (2 - 5X + 4X^2) = (1 + 2) + (1 - 5)X + 4X^2 = 3 - 4X + 4X^2$
- $f \cdot g = (1 + X) \cdot (2 - 5X + 4X^2)$

$$= (1 \cdot 2) + (1 \cdot 2 + 1 \cdot (-5))X + (0 \cdot 2 + 1 \cdot (-5) + 1 \cdot 4)X^2$$
$$+(0 \cdot 2 + 0 \cdot (-5) + 1 \cdot 4 - 1 \cdot 0)X^3$$
$$= 2 + (-3)X + (-1)X^2 + 4X^3$$

Definition 2.1.7. Ist R ein Ring und $f := r_0 + r_1X + r_2X^2 + r_3X^3 + \ldots + r_mX^m \in R[X]$ ein Polynom mit $r_m \neq n$, so nennen wir m den *Grad von f*.

Lemma 2.1.8 (Gradsatz)**.** *Sei R ein Ring.*

- *Sind $f, g \in R[X]$ mit $f, g, f+g \neq n$, so ist* $\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$.
- *Sind $f, g \in R[X]$ mit $f, g, f \cdot g \neq n$, so ist* $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$. *Ist R zusätzlich nullteilerfrei, so gilt sogar:* $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$.

Beweis. Die beiden Polynome $f, g \in R[X]$ lassen sich schreiben als

$$f = r_0 + r_1 X + r_2 X^2 + r_3 X^3 + \ldots + r_m X^m$$

und

$$g = s_0 + s_1 X + s_2 X^2 + s_3 X^3 + \ldots + s_\ell X^\ell$$

mit $r_m \neq n$ und $s_\ell \neq n$.

Damit ist $\operatorname{grad} f = m$ und $\operatorname{grad} g = \ell$.

Nach Definition ist dann:

$$f + g = (r_0 + s_0) + (r_1 + s_1)X + \ldots + (r_{\max(m,\ell)} + s_{\max(m,\ell)})X^{\max(n,m)},$$

wobei wir $r_i := n$ und $s_j := n$ setzen für $i > m$ und $j > \ell$.

Damit muss aber $\operatorname{grad}(f+g) \leq \max(m, \ell) = \max(\operatorname{grad} f, \operatorname{grad} g)$ sein. (Es tauchen ja gar keine X mit „höheren Exponenten“ auf.)

Nach Definition ist:

$$f \cdot g = r_0 \cdot s_0 + (r_1 s_0 + r_0 s_1)X + (r_2 s_0 + r_1 s_1 + r_0 s_2)X^2 + (r_3 s_0 + r_2 s_1 + r_1 s_2 + r_0 s_3)X^3$$
$$+ \ldots + (r_{m+\ell} s_0 + r_{m+\ell-1} s_1 + \ldots + r_m s_\ell + \ldots + r_1 s_{m+\ell-1} + r_0 s_{m+\ell})X^{m+\ell},$$

wobei wir $r_i := n$ und $s_j := n$ setzen für $i > m$ und $j > \ell$.

Damit muss aber $\operatorname{grad}(f \cdot g) \leq m + \ell = \operatorname{grad} f + \operatorname{grad} g$ sein. (Es tauchen ja gar keine X mit „höheren Exponenten“ auf.)

Nun schauen wir uns, um Gleichheit beim Produkt im nullteilerfreien Fall zu zeigen, noch einmal genau den Vorfaktor von dem $X^{m+\ell}$ an:

$$\underbrace{\underbrace{r_{m+\ell}}_{=n}\, s_0}_{=n} + \underbrace{\underbrace{r_{m+\ell-1}}_{=n}\, s_1}_{=n} + \ldots + \underbrace{\underbrace{r_{m+1}}_{=n}\, s_{\ell-1}}_{=n} + r_m s_\ell + \underbrace{r_{m-1}\, \underbrace{s_{\ell+1}}_{=n}}_{=n} + \ldots + \underbrace{r_1\, \underbrace{s_{m+\ell-1}}_{=n}}_{=n} + \underbrace{r_0\, \underbrace{s_{m+\ell}}_{=n}}_{=n} = r_m s_\ell$$

(In jedem einzelnen der Produkte taucht mindestens ein n (das additiv neutrale Element von R) auf, so dass sich alles weghebt bis auf ggf. den Ausdruck $r_m s_\ell$.[3])

[3] Das sieht man so: $n \cdot q = (n+n) \cdot q = n \cdot q + n \cdot q$, also $n = n \cdot q + (-n \cdot q) = n \cdot q + n \cdot q + (-n \cdot q) = n \cdot q$, also ist immer $n \cdot q = n$ für alle $q \in R$ und (analog zeigt man) $q \cdot n = n$ für alle $q \in R$. Da n additiv neutral ist, bleibt also wirklich höchstens $r_m s_\ell$ übrig.

Da aber $r_m \neq n$ und $s_\ell \neq n$ und der Ring nullteilerfrei ist, ist auch $r_m s_\ell \neq n$. (Der Vorfaktor zu $X^{m+\ell}$ ist also $\neq n$.)

Damit gilt für den nullteilerfreien Fall: $\operatorname{grad}(f \cdot g) = m + \ell = \operatorname{grad} f + \operatorname{grad} g$ □

Bemerkung 2.1.9. *Im ersten Fall kann echte Ungleichheit auftreten:*
$\operatorname{grad}(f+g) < \max(\operatorname{grad} f, \operatorname{grad} g)$.
Beispiel:

$$(1 + 3X + 4X^2) + (7 + (-4)X^2) = 8 + 3X,$$

wobei $1+3X+4X^2$ *und* $7+(-4)X^2$ *beide von Grad* 2 *sind, aber* $8+3X$ *nur vom Grad* 1.

Dass bei Ringen, die nicht nullteilerfrei sind, im letzten Fall auch echte Ungleichheit, also $\operatorname{grad}(f \cdot g) < \operatorname{grad} f + \operatorname{grad} g$*, gelten kann, sieht man u. a. an folgendem Beispiel:*
Wir nehmen uns als Ring R *die Menge* $\mathbb{Z}^2$ *mit komponentenweiser Addition und Multiplikation. Dann gilt:*

$$((1,0)X) \cdot ((0,1)X + (7,0)) = (1 \cdot 0, 0 \cdot 1)X^2 + (1 \cdot 7, 0 \cdot 0)X = (0,0)X^2 + (7,0)X = (7,0)X,$$

wobei $(1,0)X$, $(0,1)X + (7,0)$ *und* $(7,0)X$ *alle vom Grad* 1 *sind.*

2.1.2 Quadratische Zahlbereiche

Definition 2.1.10. Sei $m \in \mathbb{Z}$ fest vorgegeben. Wir betrachten die Paare $(r,s) \in \mathbb{Z}^2$ und definieren eine Addition und eine Multiplikation auf der Menge dieser Paare durch

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_1)$$

sowie

$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2 + s_1 s_2 m, r_1 s_2 + r_2 s_1)$$

für $(r_1, s_1), (r_2, s_2) \in \mathbb{Z}^2$. Dabei sind zwei Paare (r_1, s_1) und (r_2, s_2) genau dann *gleich*, wenn $r_1 = r_2$ und $s_1 = s_2$ gilt.

Lemma 2.1.11. *Bezüglich der oben angegebenen Addition und Multiplikation bilden die Elemente in* $\mathbb{Z}^2$ *einen kommutativen Ring.*

Beweis. Übungsaufgabe 3, Übungsblatt 8. □

Definition 2.1.12. Die oben angegebene Multiplikation hängt von dem gewählten $m \in \mathbb{Z}$ ab. Wir bezeichnen den so entstandenen Ring mit $\mathbb{Z}[\sqrt{m}]$.

Man sieht sofort Folgendes:

Lemma 2.1.13. *Ist die Zahl* m *oben eine Quadratzahl, so ist der dadurch definierte Ring* $\mathbb{Z}[\sqrt{m}]$ *nicht nullteilerfrei.*

Beweis. Da m eine Quadratzahl ist, gibt es ein $r \in \mathbb{Z}$ mit $m = r^2$. Dann gilt: $(r,1) \cdot (r,-1) = (r \cdot r + 1 \cdot (-1) \cdot m, r \cdot (-1) + 1 \cdot r) = (r^2 - m, -r + r) = (0,0)$. □

Bemerkung 2.1.14. *Man kann sogar zeigen: $\mathbb{Z}[\sqrt{m}]$ ist genau dann nullteilerfrei, wenn m* keine *Quadratzahl ist.*

Bemerkung 2.1.15. *Die Bezeichnung $\mathbb{Z}[\sqrt{m}]$ kommt daher, dass man statt $(r, s) \in \mathbb{Z}$ auch formal $r+s\sqrt{m}$ schreiben könnte und wie in den reellen Zahlen „rechnen“ könnte, wobei die Multiplikation oben gerade so gemacht ist, dass $\sqrt{m}\cdot\sqrt{m} = m$ gilt: Seien $(r, s), (r', s') \in \mathbb{Z}^2$. Dann gilt in $\mathbb{Z}[\sqrt{m}]$ folgende Gleichheit: $(r, s) \cdot (r', s') = (rr' + ss'm, rs' + r's)$, und würde man wie in $\mathbb{R}$ rechnen, so wäre $(r + s\sqrt{m}) \cdot (r' + s'\sqrt{m}) = rr' + ss'm + (rs' + r's)\sqrt{m}$.*

2.2 Teilbarkeit

Wir können die Definition der Teilbarkeit in den ganzen Zahlen auch auf allgemeine kommutative Ringe übertragen:

Definition 2.2.1. Sei R ein kommutativer Ring. Eine Zahl $d \in R$ heißt *Teiler von $a \in R$*, wenn es eine Zahl $c \in R$ gibt mit $a = d \cdot c$. Wir sagen auch „*d teilt a*“ oder „*a ist Vielfaches von d*“ und schreiben verkürzt:

$$d \mid a.$$

Ist d *kein* Teiler von a, so schreiben wir auch: $d \nmid a$.

Wie in den ganzen Zahlen kann man Folgendes beweisen:

Lemma 2.2.2 (Rechenregeln für Teilbarkeit)**.** *Sei R ein kommutativer Ring, und seien $a, b, c, d \in R$.*

1. *Es gilt immer: $a \mid a$.*
2. *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
3. *Gilt $a \mid b$ und $c \mid d$, so gilt auch $a \cdot c \mid b \cdot d$.*
4. *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid (x \cdot b + y \cdot c)$ für alle $x, y \in R$.*

Beweis. Der Beweis geht ganz genauso wie der entsprechende in den ganzen Zahlen. (Überall, wo am Anfang der Vorlesung bei dem Beweis $\mathbb{Z}$ stand, schreiben wir nun einfach R.) □

Definition 2.2.3. Sei R ein kommutativer Ring mit multiplikativ neutralem Element e. Wir nennen ein Element $f \in R$ eine *Einheit*, falls $f \mid e$.

Beispiel 2.2.4.

- *In den ganzen Zahlen sind die einzigen Einheiten 1 und -1, da das die einzigen Teiler von 1 sind.*
- *Sei R ein nullteilerfreier kommutativer Ring mit additiv neutralem Element n und multiplikativ neutralem Element e. Ist $f \in R[X]$ ein Polynom vom Grad ≥ 1, so kann f* keine *Einheit sein. (Das folgt aus dem Gradsatz: Gäbe es ein Polynom $g \in R[X]$ mit $f \cdot g = e \in R[X]$, so wäre auf jeden Fall $g \neq n$, da sonst $e = f \cdot g = f \cdot n = n \neq e$ wäre. Dann ist aber $0 = \text{grad } e = \text{grad } (f \cdot g) = \text{grad } f + \text{grad } g \geq 1 + 0 = 1$. Widerspruch!)*

Bemerkung 2.2.5.
- *In jedem kommutatitiven Ring R mit multiplikativ neutralem Element e sind e und $-e$ Einheiten, denn: $e = e \cdot e$ und $e = -e \cdot (-e)$ in jedem Ring.*
- *Sind f_1 und f_2 Einheiten in einem Ring R, so ist auch $f_1 \cdot f_2$ eine Einheit in R, denn: $f_1 \mid e$ und $f_2 \mid e$, also (nach Lemma 2.2.2) auch $f_1 \cdot f_2 \mid e \cdot e = e$.*
- *Ist f eine Einheit in einem Ring R, so ist $f \mid r$ für jedes $r \in R$, denn: $f \mid e$, wobei e das multiplikativ neutrale Element in R bezeichne, und $e \mid r$ für jedes $r \in R$, also (nach Lemma 2.2.2) auch $f = f \cdot e \mid e \cdot r = r$ für alle $r \in R$.*
- *In $\mathbb{Z}[\sqrt{0}]$ sind beispielsweise $(1,1)$ und $(1,-1)$ Einheiten, denn: $(1,0) = (1,1) \cdot (1,-1) = (1,-1) \cdot (1,1)$.*

In den ganzen Zahlen hatten wir gesehen, dass für zwei Zahlen $a, b > 0$ aus den beiden Beziehungen $a \mid b$ und $b \mid a$ schon immer $a = b$ folgt.

Sind $a, b \in \mathbb{Z}$ mit $a \mid b$ und $b \mid a$, so folgt im Allgemeinen nur $a = b$ oder $a = -b$.

Definition 2.2.6. Sei R ein kommutativer Ring. Wir nennen $a, b \in R$ *assoziiert*, wenn $a \mid b$ und $b \mid a$ gilt (und schreiben dann: $a \sim b$).

Man kann leicht einsehen, dass für a, b, c in jedem kommutativen Ring R Folgendes gilt:

Lemma 2.2.7.
- $a \sim a$
- *Gilt $a \sim b$, so auch $b \sim a$.*
- *Gilt $a \sim b$ und $b \sim c$, so auch $a \sim c$.*
- *Sei $a \sim b$. Dann ist $a \mid c$ genau dann, wenn $b \mid c$.*
- *$a \sim b$ genau dann, wenn es eine Einheit $f \in R$ gibt mit $b = af$.*

Beweis. Übungsaufgabe 1, Übungsblatt 9. □

Beispiel 2.2.8. *In den ganzen Zahlen gilt z.B. $3 \not\sim 4$, denn sowohl $3 \nmid 4$ als auch $4 \nmid 3$. Auch ist $2 \not\sim 4$, denn es ist zwar $2 \mid 4$, aber $4 \nmid 2$. Allerdings ist $2 \mid -2$, denn $2 \mid -2$ und $-2 \mid 2$.*
Im Ring $\mathbb{Z}[\sqrt{0}]$ gilt: $(1,1) \mid (1,-1)$, denn $(1,1) \mid (1,1) \cdot (1,-1) \cdot (1,-1) = (1,0) \cdot (1,-1) = (1,-1)$ und $(1,-1) = (1,-1) \cdot (1,1) \cdot (1,1) = (1,0) \cdot (1,1) = (1,1)$.

Definition 2.2.9. Ist R ein kommutativer Ring, so nennen wir einen Teiler b von $a \in R$ einen *echten Teiler von a*, wenn b keine Einheit ist und nicht $a \sim b$ gilt.

Weiterhin kann man mit Hilfe der Charakterisierung der Assoziiertheit aus dem vorangegangenen Lemma zeigen:

Lemma 2.2.10. *Sei R einkommutativer Ring mit additiv neutralem Element n, und seien $a, b, c \in R$, $a \neq n$ und $a = bc$. Dann ist b ein echter Teiler von a genau dann, wenn c ein echter Teiler von a ist.*

2.3 Unzerlegbarkeit und Primelemente

In den ganzen Zahlen hatten wir gesehen, wie man Primzahlen charakterisieren kann. In dem ganzen Kapitel bezeichne R einen fest vorgegebenen kommutativen Ring und n das additiv neutrale Element des Rings.

Definition 2.3.1. Wir nennen $u \in R$ *unzerlegbar*, wenn $u \neq n$ ist, u keine Einheit in R ist und u keine echten Teiler in R hat.

Davon zu unterscheiden ist in allgemeinen kommutativen Ringen folgende Eigenschaft:

Definition 2.3.2. Wir nennen ein Element $p \in R$ *Primelement*, wenn $p \neq n$ ist, p keine Einheit in R ist und aus $p \mid a \cdot b$ immer $p \mid a$ oder $p \mid b$ folgt.

Wir hatten gesehen, dass die beiden Definitionen in den (positiven) ganzen Zahlen äquivalent sind (Lemma 1.2.8). In allgemeinen kommutativen Ringen ist das jedoch *nicht* der Fall.
Es gilt jedoch:

Lemma 2.3.3. *Ist $p \in R$ ein Primelement, so ist p unzerlegbar.*

Beweis. Wir müssen nur zeigen, dass für jedes Primelement $p \in R$ auch die letzte Bedingung bei der Unzerlegbarkeit gilt, dass p also keine echten Teiler hat:

Sei $a \in R$ ein Teiler von p und p ein Primelement. Dann gibt es ein $b \in R$ mit $p = a \cdot b$. Da p ein Primelement ist, gilt $p \mid a$ oder $p \mid b$. Gleichzeitig gilt aber: $a \mid p$ und $b \mid p$. Falls $p \mid a$, so ist $p \sim a$, also a kein echter Teiler von p. Falls $p \mid b$, so ist $p \sim b$, also b kein echter Teiler von p. Dann ist aber a nach Lemma 2.2.10 ebenfalls kein echter Teiler von p. □

Um zu sehen, dass die Begriffe „unzerlegbares Element“ und „Primelement“ nicht übereinstimmen, kann man entweder ein Beispiel angeben, zu dem man ganz viel durchrechnen muss, oder aber mit etwas mehr Theorie leicht einsehen, dass sie in dem Fall nicht übereinstimmen. Dazu stellen wir in den folgenden Abschnitten eine Verbindung zwischen der Teilbarkeit in einem allgemeinen Ring R und der Teilbarkeit in den ganzen (bzw. den natürlichen) Zahlen mit Hilfe so genannter Normfunktionen her.

2.4 Normfunktionen

Auch in diesem Abschnitt sei R immer ein fest vorgegebener kommutativer Ring mit additiv neutralem Element n und multiplikativ neutralem Element e.

Wir versuchen nun, die Teilbarkeitsrelation in den ganzen Zahlen zu verallgemeinern. Dazu betrachten wir eine so genannte Normfunktion.

Definition 2.4.1. Sei $N : R \to \mathbb{N}_0$ eine Funktion mit folgenden Eigenschaften:

- $N(a) = 0$ genau dann, wenn $a = n$, und

- $N(ab) = N(a) \cdot N(b)$ für alle $a, b \in R$.

Dann nennen wir N eine *Normfunktion* auf R.

Zunächst einige Beispiele von Normfunktionen:

Beispiel 2.4.2.

- $\mathbb{Z}$ *mit* $N(z) := |z|$ *für alle* $z \in \mathbb{Z}$ *(Betragsfunktion), denn:*
  - $z = 0$ *ist die einzige ganze Zahl mit* $N(z) = |z| = 0$.
  - *Sind* $z_1, z_2 \in \mathbb{Z}$, *so ist* $N(z_1 \cdot z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2| = N(z_1) \cdot N(z_2)$.
- $R[X]$, *wobei* R *nullteilerfrei ist, zusammen mit* $N(f) := \begin{cases} 0, & \text{falls } f = n \\ 2^{\text{grad } f}, & \text{falls } f \neq n \end{cases}$, *denn:*
  - *Nach Definition von* N *ist* $f = n$ *gerade das einzige Polynom in* $R[X]$ *mit* $N(f) = 0$.
  - *Sind* $f, g \in R[X]$ *und* beide $\neq n$, *so ist* $N(f \cdot g) = 2^{\text{grad } (f \cdot g)} = 2^{\text{grad } f + \text{grad } g} = 2^{\text{grad } f} \cdot 2^{\text{grad } g} = N(f) \cdot N(g)$ *(nach dem Gradsatz).*

    Ist nun $f = n$ *oder* $g = n$, *so ist aber auch* $f \cdot g = n$, *und es gilt:*

    $$N(f \cdot g) = N(n) = 0.$$

    Andererseits ist $N(f) = 0$, *falls* $f = n$, *und* $N(g) = 0$, *falls* $g = n$, *also ist in beiden Fällen auch* $N(f) \cdot N(g) = 0$.
- $m \in \mathbb{Z}$ *kein Quadrat,* $\mathbb{Z}[\sqrt{m}]$ *mit der Funktion* $N((r, s)) := |r^2 - s^2 m|$, *denn:*
  - *Zunächst einmal gilt* $N((0, 0)) = |0^2 - 0^2 \cdot m| = 0$.

    Wir müssen aber noch zeigen, dass $(r, s) = (0, 0)$ *das* einzige *Element in* $\mathbb{Z}[\sqrt{m}]$ *ist, für das* $N((r, s)) = 0$ *gilt.*

    Sei also $(r, s) \in \mathbb{Z}[\sqrt{m}]$ *mit* $N((r, s)) = 0$. *Dann gilt:* $|r^2 - s^2 m| = 0$. *Also folgt:* $r^2 - s^2 m = 0$, *(da* 0 *die einzige ganze Zahl* z *ist mit* $|z| = 0$*). Dann ist aber* $r^2 = s^2 m$, *was aber nur der Fall sein kann, wenn* $r^2 = 0$ *und* $s^2 m = 0$ *ist, da* m *ja keine Quadratzahl ist. Dann ist aber auch* $r = 0$ *und* $s^2 = 0$, *also* $s = 0$, *denn* m *ist keine Quadratzahl, also insbesondere* $m \neq 0$.

– *Sind* $(r,s),(r',s') \in \mathbb{Z}[\sqrt{m}]$*, so ist*

$$\begin{aligned} N((r,s)\cdot(r',s')) &= N((rr'+ss'm, rs'+r's)) \\ &= |(rr'+ss'm)^2-(rs'+r's)^2m| \\ &= |r^2(r')^2+2rr'ss'm+s^2(s')^2m^2 \\ &\quad -(r^2(s')^2-2rr'ss'+(r')^2s^2)\cdot m| \\ &= |r^2(r')^2+s^2(s')^2m^2-r^2(s')^2m-(r')^2s^2m| \\ &= |(r^2-s^2m)\cdot((r')^2-(s')^2m)| \\ &= |r^2-s^2m|\cdot|(r')^2-(s')^2m| \\ &= N((r,s))\cdot N((r',s')) \end{aligned}$$

Man kann zeigen, dass Folgendes gilt:

Lemma 2.4.3. *Ist R ein nullteilerfreier kommutativer Ring mit Normfunktion N, und seien $a,b \in R$. Dann gilt:*

- *Ist $b \neq n$ und $a \mid b$, so ist auch $N(a) \mid N(b)$ und $1 \leq N(a) \leq N(b)$.*
- *Sind a und b assoziiert, so ist $N(a) = N(b)$.*
- *Ist $f \in R$ eine Einheit, so ist $N(f) = 1$.*

Beweis. Übungsaufgabe 2, Übungsblatt 9. □

Definition 2.4.4. Wir nennen eine Normfunktion N auf einem Ring R *monoton*, falls für jeden echten Teiler b von $a \in R$ auch $N(b) < N(a)$ gilt.

In nullteilerfreien kommutativen Ringen mit monotoner Normfunktion lassen sich die Einheiten als genau die Elemente charakterisieren, deren Normfunktion gerade den Wert 1 annimmt:

Lemma 2.4.5. *Ist R ein nullteilerfreier kommutativer Ring mit monotoner Normfunktion N, so ist $f \in R$ genau dann eine Einheit, wenn $N(f) = 1$ ist.*

Beweis. Übungsaufgabe 2, Übungsblatt 9. □

2.5 Unzerlegbarkeit und Primelemente II

Mit Hilfe dieser Charakterisierung der Einheiten (aus dem letzten Abschnitt) kann man zeigen:

Satz 2.5.1. *Sei R ein nullteilerfreier kommutativer Ring mit monotoner Normfunktion. Dann ist jede Nichteinheit $r \in R$ mit $r \neq n$ ein Produkt von endlich vielen unzerlegbaren Elementen.*

Die Frage, die sich nun stellt, ist, ob so eine Zerlegung, wie wir es von den ganzen Zahlen her kennen, immer eindeutig ist. Das ist im Allgemeinen *nicht* der Fall. Als Beispiel betrachten wir den quadratischen Zahlbereich $\mathbb{Z}[\sqrt{-5}]$. (Man kann zeigen, dass die oben angegebene Normfunktion (für $m = -5$) monoton ist.)

Beispiel 2.5.2. *Sei* $R := \mathbb{Z}[\sqrt{-5}]$. *Dann ist* $(6,0) = (2,0) \cdot (3,0) = (1,1) \cdot (1,-1)$.

Alle Elemente $(2,0)$, $(3,0)$, $(1,1)$ *und* $(1,-1)$ *sind unzerlegbar in* $\mathbb{Z}[\sqrt{-5}]$.

$(2,0) \nmid (1,1)$, $(2,0) \nmid (1,-1)$, *also ist auch* $(2,0)$ *zu keinem der beiden Elemente assoziiert.*

Insbesondere ist $(2,0)$ *kein Primelement.*

Beweis der Behauptungen im Beispiel.
Rechnung, dass sich $(6,0)$ als beide Produkte schreiben lässt:

$$(2,0) \cdot (3,0) = (2 \cdot 3 - (-5) \cdot 0 \cdot 0, 2 \cdot 0 + 0 \cdot 3) = (6,0)$$

und

$$(1,1) \cdot (1,-1) = (1 \cdot 1 - (-5) \cdot 1 \cdot (-1), 1 \cdot (-1) + 1 \cdot 1) = (6,0)$$

Zur Unzerlegbarkeit der vier Elemente:

Wir benutzen die Normabbildung, um zu zeigen, dass es für die vier Elemente keine echten Teiler geben kann:
Für die Norm N eines Elementes $(r,s) \in \mathbb{Z}[\sqrt{-5}]$ gilt (nach Definition):

$$N((r,s)) = |r^2 + 5s^2| = r^2 + 5s^2,$$

also $N((2,0)) = |2^2 + 5 \cdot 0^2| = 4$, $N((3,0)) = |3^2 + 5 \cdot 0^2| = 9$, $N((1,1)) = |1^2 + 5 \cdot 1^2| = 6$ und $N((1,-1)) = |1^2 + 5 \cdot (-1)^2| = 6$.

Hätte nun eines der vier Elemente einen *echten* Teiler, so wäre dessen Norm 2 oder 3. (Das liegt daran, dass die auf $\mathbb{Z}[\sqrt{-5}]$ angegebene Normfunktion N monoton ist. Also stimmen für jeden *echten* Teiler b einer Zahl $a \in \mathbb{Z}[\sqrt{-5}]$ die Normfunktionen $N(b)$ und $N(a)$ *niemals* überein. Andererseits sind alle Elemente $b \in \mathbb{Z}[\sqrt{-5}]$ mit $N(b) = 1$ schon Einheiten, also *auch* keine echten Teiler (s. Lemma 2.4.5).)
Wir müssten also ganzzahlige Lösungen (r,s) der Gleichungen $N((r,s)) = r^2 + 5s^2 = 2$ oder $N((r,s)) = r^2 + 5s^2 = 3$ suchen.
Nun haben die Gleichungen $r^2 + 5s^2 = 2$ sowie $r^2 + 5s^2 = 3$ aber keine ganzzahligen Lösungen in r, s, denn:
Gilt $r^2 + 5s^2 = 2$ bzw. $r^2 + 5s^2 = 3$, so muss $s = 0$ sein, da sonst $r^2 + 5s^2 \geq 5$ wäre. Dann muss aber $r = \pm\sqrt{2}$ bzw. $r = \pm\sqrt{3}$ sein, aber $\pm\sqrt{2} \notin \mathbb{Z}$ und $\pm\sqrt{3} \notin \mathbb{Z}$.

Da $N((2,0)) = 4 \neq 1$, $N((3,0)) = 9 \neq 1$ und $N((1,1)) = N((1,-1)) = 6 \neq 1$, können die vier Ringelemente $(2,0)$, $(3,0)$, $(1,1)$ und $(1,-1)$ keine Einheiten sein.
Weiterhin sind alle Elemente $(2,0)$, $(3,0)$, $(1,1)$ und $(1,-1)$ verschieden von $(0,0)$, dem additiv neutralen Element in $\mathbb{Z}[\sqrt{-5}]$.

Zur Nichtteilbarkeit von $(1,1)$ und $(1,-1)$ durch $(2,0)$:

Wäre $(2,0) \mid (1,1)$ oder $(2,0) \mid (1,-1)$, so wäre nach Lemma 2.4.3 aber auch $N((2,0)) \mid N((1,1))$ oder $N((2,0)) \mid N((1,-1))$ in den ganzen Zahlen, also $4 \mid 6$ in $\mathbb{Z}$. Widerspruch! Damit ist $(2,0)$ insbesondere auch weder zu $(1,1)$ noch zu $(1,-1)$ assoziiert.

$(2,0)$ kann auch kein Primelement sein, denn es ist zwar Teiler des Produktes $(1,1) \cdot (1,-1) = (6,0)$, teilt aber keinen der beiden Faktoren. □

2.6 Faktorielle Ringe, Hauptidealringe

Wie wir im vorangegangenen Abschnitt gesehen haben, ist eine Produktzerlegung von Elementen eines kommutativen Ringes in unzerlegbare Elemente, sofern sie überhaupt existiert, nicht immer eindeutig, sogar noch nicht einmal bis auf die Reihenfolge und Assoziiertheit der Elemente.

Definition 2.6.1. Sei R ein kommutativer Ring mit additiv neutralem Element n. Wir nennen R *faktoriell*, falls Folgendes gilt:

- Jedes Element $r \in R$ mit $r \neq n$, das keine Einheit ist, lässt sich als Produkt von endlich vielen unzerlegbaren Elementen schreiben.
- Ist $r \in R$ mit $r \neq n$ und r keine Einheit und $r = u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$ mit unzerlegbaren Elementen $u_1, \ldots, u_k, v_1, \ldots, v_m \in R$, so ist $k = m$ und es gibt eine Umordnung (Permutation) $f : \{1, \ldots, k\} \to \{1, \ldots, k\}$, so dass $u_i \sim v_{f(i)}$ für alle $i = 1, \ldots, k$ ist.

Beispiel 2.6.2.
- *Der Ring der ganzen Zahlen ist ein faktorieller Ring (s. Satz 1.2.11 (Hauptsatz der EZT)).*
- *Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, s. Beispiel 2.5.2 – die Zerlegung von $(6,0)$ in unzerlegbare Elemente ist hier nicht eindeutig, auch nicht bis auf Reihenfolge und Assoziiertheit.*

Faktorielle Ringe können wie folgt charakterisiert werden:

Satz 2.6.3. *Sei R ein nullteilerfreier kommutativer Ring mit additiv neutralem Element n. Dann sind die folgenden Bedingungen äquivalent:*

- *R ist faktoriell.*
- *Jedes $r \in R$ mit $r \neq n$, das keine Einheit ist, ist ein Produkt aus endlich vielen unzerlegbaren Elementen aus R, und jedes unzerlegbare Element $u \in R$ ist auch Primelement in R.*
- *Jedes $r \in R$ mit $r \neq n$, das keine Einheit ist, ist ein Produkt aus endlich vielen Primelementen aus R.*

Die Frage, die sich nun stellt, ist: Gibt es eine Klasse von kommutativen Ringen, die auf jeden Fall faktoriell sind?

Wir haben bei dem Beweis des Hauptsatzes über den größten gemeinsamen Teiler in $\mathbb{Z}$ Teilmengen I von $\mathbb{Z}$ betrachtet, die die Eigenschaften hatten, dass mit je zwei Elementen $z, z' \in I$ auch deren Differenz $z - z'$ in der Menge I lag und mit jedem $z \in I$ auch jedes ganzzahlige Vielfache $x \cdot z$, $x \in \mathbb{Z}$, in der Menge I lag.

Definition 2.6.4. Sei R ein kommutativer Ring. Wir nennen eine Teilmenge $I \subseteq R$ ein *Ideal*, falls gilt:

- Sind $r, r' \in I$, so ist auch $r - r' \in I$.
- Ist $r \in I$ und $x \in R$, so ist auch $x \cdot r \in I$.

Genau wie für die ganzen Zahlen können wir auch ganz allgemein nachrechnen:

Satz 2.6.5. *Sei $n \in \mathbb{N}$ und seien $r_1, \ldots, r_n \in R$. Wir betrachten die Menge $I(r_1, \ldots, r_n)$ $:= \{r \in R \mid$ es gibt $x_1, \ldots, x_n \in R$ mit $r = x_1 r_1 + \ldots x_n r_n\}$. Dann ist $I(r_1, \ldots, r_n)$ ein Ideal.*

Beweis. Beim Beweis des entsprechenden Satzes für $\mathbb{Z}$ schreiben wir jeweils R statt $\mathbb{Z}$. □

Definition 2.6.6. Wir nennen ein Ideal I eines kommutativen Ringes R ein *Hauptideal*, wenn es ein $r \in R$ gibt mit $I = I(r)$. (Alle Elemente des Ideals sind also bei einem Hauptideal R-Vielfache eines einzigen Elements r.)
Wir nennen einen kommutativen Ring R einen *Hauptidealring*, falls jedes Ideal in R ein Hauptideal ist.

Bemerkung 2.6.7. *Im Abschnitt über den Hauptsatz des größten gemeinsamen Teilers in den ganzen Zahlen, haben wir gesehen, dass $\mathbb{Z}$ ein Hauptidealring ist. Das ist gerade die Aussage von Lemma 1.4.16.*

Die Teilbarkeit in einem Ring lässt sich nun durch Inklusionen von Idealen darstellen:

Lemma 2.6.8. *Sei R ein kommutativer Ring, und seien $r, s \in R$. Dann gilt:*

- *$r \mid s$ genau dann, wenn $I(s) \subseteq I(r)$.*
- *$r \sim s$ genau dann, wenn $I(r) = I(s)$.*
- *$r \in R$ ist eine Einheit genau dann, wenn $I(r) = R$ ist.*
- *$r \in R$ echter Teiler von $s \in R$ genau dann, wenn $I(s) \subsetneq I(r) \neq R$.*

Beweis.
- $r \mid s \Leftrightarrow$ es gibt ein $t \in R$ mit $s = t \cdot r \Leftrightarrow s \in I(r) \Leftrightarrow q \cdot s \in I(r)$ für alle $q \in R \Leftrightarrow I(s) \subseteq I(r)$
- $r \sim s \Leftrightarrow r \mid s$ und $s \mid r \Leftrightarrow I(s) \subseteq I(r)$ und $I(r) \subseteq I(s) \Leftrightarrow I(r) = I(s)$

- $r \in R$ Einheit $\Leftrightarrow r \mid e$, wobei e das multiplikativ neutrale Element in R bezeichnet $\Leftrightarrow r \sim e \Leftrightarrow I(r) = I(e) = R$
- r echter Teiler von $s \Leftrightarrow r \mid s$, r nicht assoziiert zu s und r keine Einheit $\Leftrightarrow I(s) \subseteq I(r)$ und $I(s) \neq I(r)$, also $I(s) \subsetneqq I(r)$, und $I(r) \neq R$

□

Hiermit können wir nun eine ganze Klasse von Ringen angeben, die faktoriell sind:

Satz 2.6.9. *Sei R ein nullteilerfreier kommutativer Hauptidealring. Dann ist jedes unzerlegbare Element in R auch ein Primelement.*

Beweis. Wir bezeichnen mit n das additiv neutrale Element in R, mit e das multiplikativ neutrale Element in R.

Seien $a, b \in R$ und sei u ein unzerlegbares Element mit $u \mid a \cdot b$. Wir müssen nun zeigen, dass dann $u \mid a$ oder $u \mid b$ gilt.

Ist $u \mid a$, so sind wir fertig. Sei also nun $u \nmid a$. (Wir müssen dann zeigen, dass $u \mid b$ gilt.)
Dann ist $a \notin I(u)$ (nach dem vorangegangenen Lemma). Insbesondere ist dann auch $I(u, a) \neq I(u)$, da ja $a = n \cdot u + e \cdot a \in I(u, a)$.
Da R ein Hauptidealring ist, gibt es ein $c \in R$ mit $I(u, a) = I(c)$. Da $u = e \cdot u + n \cdot a \in I(u, a) = I(c)$, also $I(u) \subseteq I(u, a) = I(c)$ ist, ist also nach dem vorangegangenen Lemma $c \mid u$.
Da u unzerlegbar ist, ist nun entweder $c \sim u$ oder c eine Einheit. Wäre nun $c \sim u$, so wäre (abermals nach dem vorangegangenen Lemma) $I(u) = I(c)$, was aber nicht der Fall war. Also ist c eine Einheit.
Nach dem vorangegangenen Lemma ist nun $I(u, a) = I(c) = R$, so dass es Elemente $x, y \in R$ gibt mit $e = xu + ya$, denn $e \in R = I(c)$. Dann ist aber $b = b \cdot e = b \cdot (xu + ya) = (bx)u + y(ab)$.
Nun ist aber $u \mid (bx)u$ und $u \mid ab$. Wegen der Rechenregeln für Teilbarkeit ist nun $u \mid b$. (Denn u ist dann auch Teiler jeder R-Linearkombination von $(bx)u$ und ab, und b ist gerade eine solche.) □

Folgerung 2.6.10. *Jeder nullteilerfreie kommutative Hauptidealring mit monotoner Normfunktion ist faktoriell.*

Beweis. Die Existenz der monotonen Normfunktion impliziert die Existenz der Produktzerlegung von Nicht-Einheiten $\neq n$ in unzerlegbare Elemente, und der vorangegangene Satz besagt, dass unzerlegbare Elemente und Primelemente übereinstimmen. Nach der Charakterisierung der faktoriellen Ringe (Satz 2.6.3) erhalten wir hiermit, dass jeder nullteilerfreie kommutative Hauptidealring mit monotoner Normfunktion faktoriell ist. □