Dem Andenken an meinen Kollegen und Freund

**Professor Dr. Hartmut Lindel**

gewidmet.

# Vorwort

Die Mathematik ist in meinen Augen eine der anmutigsten Unterhaltungen des menschlichen Geistes mit sich selber. Ich hoffe, mit vorliegendem Buch den einen oder anderen Leser für diese Ansicht zu gewinnen. Er braucht nur geringe Vorkenntnisse und wird für das Studium einfacher, aber interessanter Beweise mit Sätzen belohnt, deren Sinn unmittelbar einleuchtet. Sollte mein Buch einige Leser dazu verführen, tiefer in die Zahlentheorie einzudringen, dorthin wo die Beweise komplizierter werden und mehr Hilfsmittel benötigen, wo die Ergebnisse schwieriger zu interpretieren sind, so würde mich das besonders freuen.

Auch wenn das Buch – mit kleinen Ausnahmen – nur Vorkenntnisse voraussetzt, die man bis zum Abitur erwirbt, sollte der Leser bereits ein wenig Übung im Verstehen mathematischer Beweise haben. Es ist für Mathematikstudenten vom zweiten oder dritten Semester an gedacht.

Das Buch hat einen algebraischen Anstrich. Die meistverwendete Methode ist die Benutzung einfacher Aussagen über abelsche Gruppen. Auch werden zwei algebraische Zahlenringe ($\mathbb{Z}[i], \mathbb{Z}\left[\frac{1}{2}(-1+\sqrt{-3})\right]$) und der nichtkommutative Ring der ganzen Quaternionen in die Betrachtung einbezogen.

Der Leser ist aufgefordert, seinen eigenen Weg durch das Buch zu finden. Langweilen ihn die anfänglichen Betrachtungen des §0, so beginne er mit Satz 0.18. (Dies ist übrigens der erste Satz in Gauß' berühmten "Disquisitiones Arithmeticae", wie ich nachträglich festgestellt habe.) Der dritte Paragraf wird, bis auf Satz 3.1, später nicht mehr benötigt. Lesen

Sie ihn, wenn Sie Lust danach verspüren. Das können Sie auch mit §14 so machen, da dieser allenfalls die Paragrafen 1 und 2 voraussetzt. Der vielleicht etwas schwierige §9 wird später nur noch in 10.24 gebraucht. Wenn Sie auf seine Lektüre (zunächst) verzichten wollen, brauchen Sie auch Satz 7.14 nicht zu erarbeiten. Wer sich für die Grundlagen der Mathematik interessiert, mag §16 lesen. Er kann auch mit diesem Paragrafen beginnen.

Viele der Aufgaben gehören in die Kategorie der Mathematischen Puzzles. Sie sollen dem Vergnügen des Lesens dienen und ihm eine lebendige und anschauliche Beziehung zu den Zahlen vermitteln. Dafür sind auch die Abbildungen gedacht. (Der eine oder andere Leser wird mit Überraschung registrieren, daß in diesem Buch neben der Möbiusfunktion auch das Möbiusband eine Rolle spielt.)

Einige der Aufgaben mögen wirklich neu sein. Viele sind Standardaufgaben.

Wie gesagt, hoffe ich, dieses Buch möge für den Leser nur der Beginn seiner Beschäftigung mit der Zahlentheorie sein. Er kann in verschiedenen Richtungen fortfahren:

Anwendungen der Zahlentheorie: [*Forster*], [*Koblitz*].
Analytische Zahlentheorie und Primzahltheorie: [*Chandrasekharan*], [*Davenport*], [*Prachar*], [*Trost*].
Algebraische Zahlentheorie:[*Samuel*], [*Neukirch*], [*Marcus*],

Die Algebraische Zahlentheorie studiert eine Klasse von Ringen, für die hier in den Paragrafen 12 und 15 zwei spezielle Beispiele gegeben werden.

Meine Liebe und Empfehlung gilt vor allem zwei Büchern, deren Lektüre mir besonders motivierend erscheint und deshalb als “Brücke” zu einem systematischen Studium einer zahlentheoretischen Disziplin dienen kann:

Einige sehr interessante Themen werden in [*Serre*] behandelt.

Eine geglückte Synthese der Zahlentheorie mit ihrer Geschichte findet sich in [*Scharlau, Opolka*].

Ich habe vielen Leuten zu danken: Herr G. Bergmann (Münster) half mir bei den Bemerkungen zur Fermat-Vermutung. Einem Gespräch mit Herrn F. Lorenz (Münster) entsprangen zwei Aufgaben. Herr J. Diller (Münster) gab mir zwei wichtige Hinweise zu §16. Herr H. Engesser, der Leiter des B. I.–Wissenschaftsverlages, hat diesen Paragrafen 16 vorab auf Unklarheiten durchgesehen. (Meinen Dank an ihn und den Verlag ist auch irgendwo in den Aufgaben versteckt.) Frau B. Randerath hat meine Vorlage in die LaTex–Sprache übersetzt. Herr M. Krieg und Frau E. Ernsting haben die Korrekturen gemacht. Herr F. Budde hat den Computer zur Anfertigung der Illustrationen veranlaßt. Nicht einmal Abbildung 14 durfte ich selber zeichnen. Die Einbandillustration ist vom Verlag hergestellt worden. Sie ist eine Anspielung auf einen Ergänzungssatz zum quadratischen Reziprozitätsgesetz.

Münster, 19.9.91

(Die Zahl $p = 19991$ ist ein Primzahldrilling, da $p, p+2$ und $p+6$ Primzahlen sind. Der Leser möge überlegen, warum natürliche Zahlen $n, n+2, n+4$ außer im Falle $n = 3$ nie gleichzeitig Primzahlen sein können.)

# Inhaltsverzeichnis

# § 0

# Der Ring $\mathbb{Z}$ der ganzen Zahlen

Wir stellen uns die ganzen Zahlen wie Perlen auf einer (unendlich langen) Schnur vor:

Abb. 1

Ihre Gesamtheit (Menge) wird mit $\mathbb{Z}$ bezeichnet. $\mathbb{Z}$, zusammen mit der Addition und der Multiplikation ist ein kommutativer Ring. Was heißt das?

**Definition: 0.1** *Ein kommutativer Ring ist eine Menge $A$ zusammen mit zwei Verknüpfungen (Rechenarten) „+“ und „·“, so dass folgendes gilt:*

*(i)* $a + (b + c) = (a + b) + c$
*(i')* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(Assoziativität)*

*(ii)* $a + b = b + a$
*(ii')* $a \cdot b = b \cdot a$ *(Kommutativität)*

*(iii) Es gibt ein Element $0 \in A$ mit $a + 0 = a$;*
*(iii') Es gibt ein Element $1 \in A$ mit $a \cdot 1 = a$* *(Existenz neutraler Elemente)*

*(iv) Für ein bezüglich „+“ neutrales Element 0 gibt es zu jedem $a$ ein Element $-a \in A$ mit $a + (-a) = 0$.*
*(Existenz eines Inversen bezüglich der Addition)*

*(v)* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *(Distributivität)*

*In diesem Buch werden wir – mit Ausnahme des Paragrafen 13 – unter einem Ring stets einen kommutativen Ring, in dem (ii') gilt, verstehen.*
(Der in 13.5 eingeführte Ring der ganzen Quaternionen erfüllt (ii') nicht.)

**Bemerkung: 0.2** a) Es gibt bzgl. „+“ und „·“ je nur ein neutrales Element. Denn seien etwa $0, 0'$ neutral bzgl. $+$.
Dann ist $0 \overset{\text{(iii)}}{=} 0 + 0' \overset{\text{(ii)}}{=} 0' + 0 \overset{\text{(iii)}}{=} 0'$.

b) Zu jedem $a \in A$ gibt es nur ein Inverses bzgl. $+$.
Denn gelte $a + (-a) = 0 = a + (\neg\, a)$.
So ist $-a \overset{\text{(iii)}}{=} (-a) + 0 \overset{\text{(iv)}}{=} (-a) + (a + (\neg\, a)) \overset{\text{(i)}}{=} ((-a) + a) + (\neg\, a) \overset{\text{(ii)}}{=} (a + (-a)) + (\neg\, a) \overset{\text{(iv)}}{=} 0 + (\neg\, a) \overset{\text{(ii)}}{=} (\neg\, a) + 0 \overset{\text{(iii)}}{=} \neg\, a$.

c) Assoziativität und Kommutativität bedeuten, dass es in Ausdrükken, in denen nur „+“ (bzw. nur „·“) als Verknüpfung vorkommt, auf Klammerung und die Reihenfolge der „Summanden“ (bzw. „Faktoren“) nicht ankommt. Wir lassen Klammern, soweit möglich, weg.

**Konventionen: 0.3** a) Wir schreiben wie üblich:
$ab$ statt $a \cdot b$ (wenn's geht),
$ab + ac$ statt $(ab) + (ac)$,
$a - b + c - d$ statt $a + (-b) + c + (-d)$ usw.

b) Die Ausdrücke Addition, Multiplikation, Summe, Produkt, Summand, Faktor werden wie üblich benutzt.

**0.4** Aus den Axiomen (i) – (v) für Ringe lassen sich sofort die folgenden Regeln ableiten:

a) $\quad -(-a) = a$.
Denn $(-a) + a = 0$ und $(-a) + -(-a) = 0$; aber das Inverse von $-a$ ist eindeutig bestimmt (0.2b)).

b) $\quad a \cdot 0 = 0$.
Denn $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Also
$0 \overset{\text{(iv)}}{=} a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) \overset{\text{(iv)}}{=} a \cdot 0$.

c) $\quad a \cdot (-b) = -(ab)$.
Denn $ab + a \cdot (-b) = a(b + (-b)) = a \cdot 0 = 0$, und das additiv Inverse von $ab$ ist eindeutig bestimmt.

d) $\quad$ Wegen der Kommutativität der Multiplikation gilt auch
$(-a) \cdot b = -(ab)$. Wir schreiben $-ab$ statt $-(ab)$.

e) $\quad (-a) \cdot (-b) \overset{\text{d)}}{=} -(a(-b)) \overset{\text{c)}}{=} -(-ab) \overset{\text{a)}}{=} ab$.

**Definition: 0.5** *Ein Ring ist ein Körper, wenn in ihm $1 \neq 0$ gilt und zu jedem $a \neq 0$ ein („multiplikativ Inverses“) $a^{-1}$ existiert mit $aa^{-1} = 1$.*

**Bemerkung: 0.6** Man zeigt wie oben die Eindeutigkeit des multiplikativ Inversen und $(a^{-1})^{-1} = a$.

**Beispiele: 0.7** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Ringe. $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind sogar Körper, aber $\mathbb{Z}$ nicht. ($\mathbb{Q} = \{$rationale Zahlen$\}$, $\mathbb{R} = \{$reelle Zahlen$\}$,
$\mathbb{C} = \{$komplexe Zahlen$\}$.)
Ein weiterer Ring, der kein Körper ist, ist $\mathbb{G} := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, der Gaußsche Zahlenring.
Wir werden im Laufe dieses Buches (unendlich viele) weitere Ringe kennenlernen.

**0.8** $\quad \mathbb{Z}$ ist nicht nur ein Ring, sondern besitzt mit der Relation „$\leq$“ (kleiner oder gleich) eine sogenannte Anordnung.

In Abb. 1 hat „$\leq$“ die Bedeutung „links von oder gleich“.

Die Relation „$\leq$“ in $\mathbb{Z}$ genügt folgenden „Axiomen“ einer totalen (d.h. linearen oder vollständigen) Anordnung: Für alle $a, b, c, \in \mathbb{Z}$ gilt:

(i) $a \leq a$ (Reflexivität);

(ii) $a \leq b, b \leq c \implies a \leq c$ (Transitivität);

(iii) $a \leq b, b \leq a \implies a = b$ (Antisymmetrie);

(iv) $a \leq b$ oder $b \leq a$ (Totalität, Linearität oder Vollständigkeit).

**0.9 Definition:**
$a < b :\iff a \leq b$ *und* $a \neq b$ *;*
$a \geq b :\iff b \leq a;$
$a > b :\iff b < a.$

**0.10** Für alle $a, b, c \in \mathbb{Z}$ gilt:

(i) $b < c \Rightarrow a + b < a + c;$

(ii) $0 < a, \quad b < c \Rightarrow ab < ac$

(Monotonie der Addition bzw. Multiplikation).

Ein Ring mit einer Anordnungsrelation, die die Gesetze (i) bis (iv) in 0.8 und (i), (ii) in 0.10 erfüllt, heißt ein angeordneter Ring. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ sind in diesem Sinne angeordnete Ringe. (Sie sind „angeordnete Körper".)

**0.11** Der angeordnete Ring $\mathbb{Z}$ besitzt folgende Eigenschaft:

(M) *Jede nach unten beschränkte nichtleere Teilmenge $M$ von $\mathbb{Z}$ besitzt ein kleinstes Element.*

($M$ heißt nach unten beschränkt, wenn es ein $s \in \mathbb{Z}$ gibt mit $s \leq x$ für alle $x \in M$. Ferner heißt $y$ ein kleinstes Element von $M$, wenn $y \in M$ und $y \leq x$ für alle $x \in M$ gilt.)

**Bemerkung: 0.12** Im Rahmen der klassischen Mengenlehre lässt sich zeigen, dass zwei angeordnete Ringe, welche der Bedingung (M) genügen, zueinander als angeordnete Ringe „isomorf" sind. D.h. es gibt eine bijektive Abbildung des einen auf den anderen, welche mit den Verknüpfungs- und Anordnungsstrukturen verträglich ist. Man hätte also eine axiomatische Beschreibung von $\mathbb{Z}$.
Ich habe allerdings nicht vor, die Zahlentheorie aus einer solchen Axiomatik zu entwickeln. Stattdessen wird im Anhang ein konstruktiver Aufbau des Ringes der ganzen Zahlen beschrieben. Abgesehen von diesem Anhang sollen die Begriffe „ganze", „rationale", „reelle" und „komplexe" Zahl als bekannt vorausgesetzt werden.

Zur Menge $\mathbb{N}$ der natürlichen Zahlen rechne ich die 0 hinzu, also
$\mathbb{N} := \{x \in \mathbb{Z} | x \geq 0\}$. Dann hat jede endliche Menge – auch die leere – eine natürliche Zahl als Kardinalzahl (= Anzahl ihrer Elemente). Die Kardinalzahl einer endlichen Menge $M$ wird mit $\#M$ bezeichnet. Für eine unendliche Menge $M$ schreiben wir in der Regel $\#M = \infty$.
Wir werden die folgenden Tatsachen verwenden:

*Die Kardinalzahl einer Vereinigung zweier disjunkter endlicher Mengen ist die Summe und die Kardinalzahl ihres cartesischen Produktes das Produkt ihrer Kardinalzahlen.*

Ferner benutzen wir das sogenannte Dirichletsche Schubfachprinzip:

*Seien $M, N$ zwei endliche Mengen mit $\#M > \#N$, so gibt es keine injektive Abbildung $M \to N$ und keine surjektive Abbildung $N \to M$.*

**Definition: 0.13** *Für $k \in \mathbb{N}$ sei*

$$\mathbb{N}_k := \{x \in \mathbb{N} | x \geq k\}.$$

*Insbesondere ist dann $\mathbb{N}_1 = \{1, 2, 3, \cdots\}$.*

**0.14** Für $\mathbb{N}$ gilt das bekannte Induktionsprinzip (oder –axiom):

(I) *Sei $\mathcal{A}(x)$ eine Aussage über natürliche Zahlen $x$ mit folgenden beiden Eigenschaften:*

*(i) $\mathcal{A}(0)$ ist richtig,*

*(ii) für alle $n \in \mathbb{N}$ folgt $\mathcal{A}(n+1)$ aus $\mathcal{A}(n)$.*

*Dann gilt $\mathcal{A}(n)$ für alle $n \in \mathbb{N}$.*

Dieses Prinzip ist für angeordnete Ringe äquivalent zu (M).

Wenn man mit diesem Prinzip eine Aussage $\mathcal{A}(x)$ nur für alle $x \in \mathbb{N}_k$ beweisen will (etwa weil $\mathcal{A}(n)$ für $n < k$ keinen Sinn hat), so kann man (I) auf die Aussage $\mathcal{B}(x) := \mathcal{A}(x + k)$ anwenden.

In vielen Induktionsbeweisen schließt man auf die Richtigkeit von $\mathcal{A}(n+1)$ aus der von allen Aussagen $\mathcal{A}(k)$ mit $k \leq n$. Auch dies kann man auf (I) formal zurückführen, indem man

$\mathcal{B}(x)$ als die Aussage

"$\mathcal{A}(y)$ gilt für alle natürlichen Zahlen $y \leq x$ „

definiert.

Im Beweis von 3.11 werden wir (I) auf die Aussage $\mathcal{A}(x)$ anwenden, wobei

$\mathcal{A}(x)$ bedeuten soll:

$\pi(n) < \frac{8}{5}\frac{n}{\log n}$ gilt für alle $n \in \mathbb{N}_2$ mit $n \leq 2^{16} + x$.

**0.15** Weitere Eigenschaften von $\mathbb{Z}$:

a) Die Abbildung $\mathbb{Z} \to \mathbb{Z}, a \longmapsto -a$ ist zu sich selbst invers, also bijektiv. (Dies gilt wegen 0.4 a) in jedem Ring.) Sie kehrt die Anordnung um, d.h. $a \leq b \Rightarrow -a \geq -b$. (Anschaulich gesehen, ist sie die Spiegelung am Nullpunkt in Abb. 1.)
Wegen (M) gilt also auch
(M') *Jede nichtleere nach oben beschränkte Teilmenge von $\mathbb{Z}$ besitzt ein größtes Element.*

b) Wenn $a, b, c \in \mathbb{Z}, a \neq 0$ und $ab = ac$ gilt, ist auch $b = c$. Insbesondere ist $ab \neq 0$, wenn $a, b \neq 0$ sind.
Dies gilt keinesfalls in jedem Ring! (Vgl. §4)

c) Das kleinste Element von $\{x \in \mathbb{Z} | x > 0\}$ ist 1.

**0.16** Folgende Teilmengen von $\mathbb{Z}$ werden noch eine große Rolle spielen:

**Definition:** *Seien $a, m \in \mathbb{Z}$.*

$$m\mathbb{Z} := \{mx \,|\, x \in \mathbb{Z}\}$$

$$a + m\mathbb{Z} := \{a + mx \,|\, x \in \mathbb{Z}\}.$$

**Bemerkungen: 0.17** a) $m\mathbb{Z} = (-m)\mathbb{Z}$ und $a + m\mathbb{Z} = a + (-m)\mathbb{Z}$. Es ist also keine Einschränkung, nur $a + m\mathbb{Z}$ mit $m \geq 0$ zu betrachten.

b) Es gilt $0 \in m\mathbb{Z}$. Mit $a, b$ liegen auch $a + b$ und $a - b$ in $m\mathbb{Z}$.

c) Wenn $m \neq 0$ ist, ist $m\mathbb{Z}$ weder nach oben noch nach unten beschränkt. Denn sei (wegen a)) o.E. $m > 0, s > 0$. Dann ist $m(s + 1) \geq 1 \cdot (s + 1) > s$

und $m(-s-1) < -s$.

d) Wenn $m \neq 0$ ist, ist $a+m\mathbb{Z}$ weder nach oben noch nach unten beschränkt. Wäre nämlich $s$ eine obere (untere) Schranke für $a+m\mathbb{Z}$, so wäre $s-a$ eine solche für $m\mathbb{Z}$.

**0.18** Man erhält alle Elemente von $a+m\mathbb{Z}$, wenn man mit $a$ beginnend beim Durchlaufen der Zahlenreihe nach links und rechts jede $|m|$–te Zahl auswählt. Deshalb ist folgendes anschaulich klar:

**Satz:** *Sei $m \in \mathbb{Z} - \{0\}, a, b \in \mathbb{Z}$. Dann fällt genau 1 Element von $a+m\mathbb{Z}$ in das Intervall $[b, b+|m|[$ (in welchem $|m|$ aufeinanderfolgende ganze Zahlen liegen).*

**Beweis:** Wir dürfen $m > 0$ annehmen. Da $a+m\mathbb{Z}$ nicht nach oben beschränkt ist, ist

$$M := \{x \in a+m\mathbb{Z} \mid x \geq b\} \neq \emptyset.$$

Sei $y = a+mx$ minimal in dieser Menge. Wäre $y \geq b+m$, so wäre auch $y-m = a+m(x-1) \in M$. Dies stünde im Widerspruch zur Minimalität von $y$. Also ist $y$ das gesuchte Element. Wenn ferner $y' = a+mx' \in [b, b+m[$ gilt, so ist $m > y'-y = m(x'-x) \geq 0$, also $m > m|x'-x| \geq 0$, mithin $1 > |x'-x| \geq 0$, d.h. $x' = x$ wegen 0.15 c). Es folgt $y' = y$. □

**Korollar: 0.19** *(Division mit Rest)*
*Seien $a, m \in \mathbb{Z}, m \neq 0$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit*

*1) $a = qm + r$ und*

*2) $0 \leq r < |m|$.*

**Beweis:** Nach Satz 0.18 gibt es genau ein $r \in a+m\mathbb{Z}$ mit $0 \leq r < |m|$. Man kann also ein $q \in \mathbb{Z}$ so wählen, dass $r = a + m \cdot (-q)$, d.h. $a = qm + r$ ist. Falls auch $a = q'm + r$ gilt, folgt $qm = q'm$ und somit $q = q'$, da $m \neq 0$ ist. □

**Korollar: 0.20** *0.19 bleibt gültig, wenn man 2) durch*

*2')* $-\frac{|m|}{2} < r \leq \frac{|m|}{2}$.

*ersetzt.*

**0.21** Häufig braucht man nur folgende schwache Form von 0.19:

**Korollar:** *Zu* $a, m \in \mathbb{Z}, m \neq 0$*, gibt es* $q, r \in \mathbb{Z}$ mit:

1) $a = qm + r$,

2) $|r| < |m|$.

(Hier sind $q, r$ in der Regel nicht eindeutig bestimmt.)

## AUFGABEN UND HINWEISE

**1)** Es ist für den Leser durchaus nicht schwierig, die in diesem Paragrafen nicht bewiesenen Behauptungen, nämlich die Äquivalenz von (I) und (M), die „eindeutige“ Definiertheit von $\mathbb{Z}$ und die Behauptungen in 0.15 durch die angegebenen Axiome selber zu beweisen.

**2)** Eine hübsche Anwendung des Induktionsprinzips ist der Beweis, dass man in dem – im folgenden beschriebenen – Spiel (Puzzle) der „Türme von Hanoi“ (*Lucas*) immer zum Ziele kommen kann.

Das Spiel besteht aus einem Stapel von $n$ kreisrunden Scheiben, die (gleich dick sind, aber) paarweise verschiedene Durchmesser haben. Sie liegen der

Größe nach aufeinander, die größte Scheibe unten, auf einem von 3 Spielfeldern.

Abb. 2

Die Aufgabe ist nun, diesen Stapel in mehreren Schritten auf ein anderes der drei Spielfelder auf folgende Weise zu bringen: Bei jedem Schritt ist eine Scheibe auf ein anderes Spielfeld bzw. auf einen dort bereits befindlichen Stapel zu legen, ohne dass jemals eine größere Scheibe auf einer kleineren zu liegen kommt. (In den praktischen Ausführungen dieses Spiels haben in der Regel die Scheiben in der Mitte ein Loch und werden durch drei senkrecht stehende Stäbe fixiert.)
Beim Beweis verwende man Induktion nach $n$. Oder man schließe mit Induktion nach $k$, wobei die Aussage $\mathcal{A}(k)$ bedeuten soll: Man kann die $k$ obersten Scheiben des Ausgangsstapels auf eines der beiden anderen Spielfelder den Spielregeln gemäß stapeln.

**3)** Jeder kennt die Darstellung natürlicher Zahlen im Dezimalsystem. Mathematisch gesprochen, besitzt jede natürliche Zahl $n$ eine Darstellung der Form

$$n = \sum_{i=0}^{m} a_i \cdot 10^i$$

mit $a_i \in \{0, 1, \ldots, 9\}$. Diese Darstellung ist (für $n > 0$) eindeutig, wenn man $a_m \neq 0$ verlangt. Der Leser möge dies – etwa durch Division mit Rest und vollständige Induktion – wirklich beweisen. Dabei sollte er 10 durch eine beliebige Zahl $d \in \mathbb{N}_2$ ersetzen.
Im Falle $d = 2$ schreibt sich jede natürliche Zahl mit den Ziffern 0 und 1. Man spricht von Binärschreibweise. Für allgemeine $d$ spricht man leider manchmal von $d$–adischer Schreibweise. Man sollte von $d$–alschreibweise oder $d$–alsystem reden.

**4)** Welche Zahlen lassen sich eigentlich in der Form $\sum_{i=0}^{m} a_i 3^i$ mit $a_i \in \{-1, 0, 1\}$ ausdrücken?

**5)** Gesucht ist ein möglichst kleiner Satz von Gewichten, so dass man mit einer Balkenwaage jedes volle Grammgewicht bis einschließlich $2000g$ abwiegen kann. Man unterscheide, ob man die Gewichte nur in eine Waagschale legen darf oder in beide. (Beachten Sie A3 und A4.)

**6)** Zeigen Sie: $\sum_{k=0}^{n} k \cdot k! = (n+1)! - 1$. (Dies geschieht mit vollständiger Induktion ohne Mühe. Wie man allerdings auf diese Identität gekommen ist, ist dem Beweis nicht anzusehen.)

**7)** Zeigen Sie: Für jedes $n \in \mathbb{N}$ ist $2 \cdot 5^{3n+1} + 4^n$ durch 11 teilbar, d.h. es gibt zu jedem $n$ ein (von $n$ abhängiges) $k \in \mathbb{N}$ mit $11 \cdot k = 2 \cdot 5^{3n+1} + 4^n$. (Auch hier führt ein Induktionsbeweis zum Ziele, ohne dass Sie leicht erkennen können, wie ich auf solch eine Behauptung überhaupt gekommen bin. Mit der Kenntnis des Paragrafen 4 sollte Ihnen das schon leichter fallen.)

# § 1

# Untergruppen von $\mathbb{Z}$, größter gemeinsamer Teiler

Lieber Leser, ich wette, dass die Jahreszahl Ihres Geburtsdatums die Summe eines Vielfachen von 30 und eines solchen von 49 ist.
Nach dem Lesen der folgenden Ausführungen werden Sie nicht dagegen halten.

**Definition: 1.1** *Eine abelsche Gruppe ist eine Menge $G$ zusammen mit einer Verknüpfung „+", welche die Axiome der Addition für Ringe* (0.1, (i)-(iv)) *erfüllt.*

Mit dem Wort „abelsch" ist „kommutativ" gemeint. D.h. in einer abelschen Gruppe gilt insbesondere $a + b = b + a$. Wenn man auf dieses Gesetz verzichtet, spricht man von „Gruppe" schlechthin. In diesem Buch haben wir es fast nur mit abelschen Gruppen zu tun.

Häufig benutzt man auch die sogenannte multiplikative Schreibweise. D.h. für die Verknüpfung wird $a \cdot b$ oder $ab$ geschrieben. In diesem Falle wird das neutrale Element mit 1 und das Inverse von $a$ mit $a^{-1}$ bezeichnet.
Wir stellen die Axiome für eine abelsche Gruppe noch einmal in multiplikativer Schreibweise zusammen:

(i) $a(bc) = (ab)c$;

(ii) $ab = ba$;

(iii) es gibt ein Element 1 mit $a \cdot 1 = a$;

(iv) für eine solche 1 gilt: Zu jedem $a$ existiert ein $a^{-1}$ mit $aa^{-1} = 1$.

**Beispiele: 1.2** a) Wenn man in einem Ring $A$ die Multiplikation unbeachtet lässt („vergisst"), so ist $A$ eine abelsche Gruppe, die sogenannte (unterliegende) additive Gruppe von $A$.
b) Die Elemente $\neq 0$ eines Körpes $K$ bilden bezüglich der Multiplikation eine abelsche Gruppe. Diese wird mit $K^*$ bezeichnet und heißt multiplikative Gruppe von $K$.

**Definition: 1.3** *Eine Untergruppe einer abelschen Gruppe $G$ ist eine Teilmenge $H$ von $G$, für die gilt:*

*(i)* $0 \in H$;

*(ii)* $a, b \in H \;\Rightarrow\; a + b \in H$;

*(iii)* $a \in H \;\Rightarrow\; -a \in H$.

Eine Untergruppe einer abelschen Gruppe ist wieder eine abelsche Gruppe.

**Bemerkung: 1.4** Eine Teilmenge $H$ einer abelschen Gruppe $G$ ist schon dann eine Untergruppe, wenn folgendes gilt:

1) $H \neq \emptyset$ (etwa $0 \in H$),

2) $a, b \in H \;\Rightarrow\; a - b \in H$.

Denn wenn $a \in H$, folgt mit 2), dass auch $0 = a - a \in H$, somit ferner $-a = 0 - a \in H$ ist. Wenn nun $a, b \in H$, ist auch $-b \in H$, also mit 2) auch $a + b = a - (-b) \in H$.

**Beispiele: 1.5** a) Die multiplikative Gruppe $\mathbb{C}^*$ der komplexen Zahlen hat u.a. folgende Untergruppen: $\{1\}, \{1, -1\}, \mathbb{Q}^*, \mathbb{R}^*$,
$\{x \in \mathbb{R} | x > 0\}, \{z \in \mathbb{C} |\ |z| = 1\}, \left\{ e^{r \cdot 2\pi i/m} \middle| \, r = 0, 1, \ldots, m-1 \right\}$.
b) Für $m \in \mathbb{Z}$ ist die Menge $m\mathbb{Z}$ eine Untergruppe (der additiven Gruppe) von $\mathbb{Z}$; siehe 0.17 b).

**Satz: 1.6** *Wenn $H$ eine Untergruppe von $\mathbb{Z}$ ist, so gibt es ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $H = m\mathbb{Z}$.*

**Beweis:** Wenn $H = \{0\}$ ist, ist $H = 0 \cdot \mathbb{Z}$ und $H \neq m\mathbb{Z}$ für jedes $m \neq 0$.
Sei $H \neq \{0\}$, dann besitzt $H$ Elemente $a > 0$. Sei nämlich $b \in H - \{0\}$.
Wenn $b > 0$ ist, setze $a = b$. Wenn $b < 0$ ist, setze $a = -b \in H$.
Sei jetzt $m$ das kleinste (strikt) positive Element aus $H$.
Dann ist $m\mathbb{Z} \subset H$. Denn für $c \in \mathbb{Z}$ gilt $mc = \pm \underbrace{(m + \ldots + m)}_{|c|-\text{mal}} \in H$.

*Behauptung:* $m\mathbb{Z} = H$.

Sei nämlich $a \in H$ beliebig. Dividiere $a$ gemäß 0.19 durch $m$ mit Rest: $a = mq + r$ mit $0 \leq r < m$.

Da $a$ und $m$, also auch $mq$ zu $H$ gehören, gilt $r = a - mq \in H$.

Wäre nun $r \neq 0$, so wäre $r$ ein kleineres positives Element aus $H$ als $m$. Widerspruch!
Aus $r = 0$ folgt nun $a = mq \in m\mathbb{Z}$.

Zur Eindeutigkeit von $m (\in \mathbb{N})$ bemerke man, dass $m$ das kleinste positive Element von $m\mathbb{Z}$ ist, also $m\mathbb{Z} = m'\mathbb{Z}$ zusammen mit $m, m' \in \mathbb{N}$ die Gleichheit $m = m'$ ergibt. $\square$

**Definition: 1.7** *Seien $H_1, H_2$ Untergruppen einer additiv geschriebenen abelschen Gruppe $G$.*
*Schreibe $H_1 + H_2 := \{h_1 + h_2 \,|\, h_1 \in H_1, h_2 \in H_2\}$.*
*(Bei multiplikativer Schreibweise schreibt man $H_1 H_2$ für die so gebildete Teilmenge von $G$.)*

**Satz: 1.8** *Seien $H_1$ und $H_2$ Untergruppen einer (additiv geschriebenen) abelschen Gruppe $G$. Dann sind auch*

$$H_1 \cap H_2 \text{ und } H_1 + H_2$$

*solche.*

**Beweis:** **a)** Zu $H_1 \cap H_2$:
$0 \in H_1, 0 \in H_2 \Longrightarrow 0 \in H_1 \cap H_2$.
$a, b \in H_1 \cap H_2 \Longrightarrow a, b \in H_1,\ a, b \in H_2 \Longrightarrow a - b \in H_1,\ a - b \in H_2 \Longrightarrow a - b \in H_1 \cap H_2$.

**b)** Zu $H_1 + H_2$:
$0 = 0 + 0 \in H_1 + H_2$.
Seien $a = a_1 + a_2 \in H_1 + H_2$, $b = b_1 + b_2 \in H_1 + H_2$ mit $a_i,\ b_i \in H_i$. Dann ist $a - b = (a_1 - b_1) + (a_2 - b_2) \in H_1 + H_2$. □

**Bemerkungen: 1.9** a) Eine entsprechende Aussage gilt nicht für die Vereinigung zweier Untergruppen. Z.B. gilt $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, aber $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.
b) Zum Beweis, dass $H_1 + H_2$ eine Untergruppe ist, wurde die Kommutativität gebraucht. Für nichtabelsche Gruppen gilt diese Aussage i.a. nicht.
c) Der Satz gilt auch für unendliche Durchschnitte und Summen. (Wie würden Sie solche definieren?)
d) Seien $H, H_1, H_2$ Untergruppen einer abelschen Gruppe, so gilt

$$H \supset H_1, H_2 \iff H \supset H_1 + H_2.$$

**Korollar: 1.10** *(Folgerung aus 1.6 und 1.8)*
*Zu $a, b \in \mathbb{Z}$ gibt es genau ein $d \in \mathbb{N}$ mit $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

**Beweis:** Da $a\mathbb{Z}$ und $b\mathbb{Z}$ Untergruppen von $\mathbb{Z}$ sind, ist nach 1.8 auch $a\mathbb{Z} + b\mathbb{Z}$ eine solche, also von der Form $d\mathbb{Z}$ mit eindeutig bestimmten $d \in \mathbb{N}$ nach 1.6. □

**Definition: 1.11** *Seien $a, b \in \mathbb{Z}$. Man sagt, $a$ ist ein Teiler von $b$ oder $a$ teilt $b$, und schreibt $a|b$, wenn es ein $c \in \mathbb{Z}$ mit $a \cdot c = b$ gibt.*

**1.12 Grundlegende Feststellung:** $a|b \iff a\mathbb{Z} \supset b\mathbb{Z}$.

**Beweis:** „$\Rightarrow$“: Sei $bx \in b\mathbb{Z}$ mit $x \in \mathbb{Z}$ beliebig. Aus $ac = b$ folgt $bx = acx \in a\mathbb{Z}$.
„$\Leftarrow$“: $a\mathbb{Z} \supset b\mathbb{Z} \Rightarrow b \in a\mathbb{Z} \Rightarrow \exists c \in \mathbb{Z}$ mit $b = ac$. $\square$

**1.13** Grundlegende Eigenschaften von „$|$“:

a) $\pm 1|a$, $a|0$.
b) $a|b \iff |a|\,\Big|\,|b|$.
c) $a|b$, $b|c \Rightarrow a|c$.
d) $a|b$, $a|c \Rightarrow a|bb' + cc'$.
(Dies kann man direkt zeigen, aber auch mit 1.9 d) und 1.12:
$a\mathbb{Z} \supset b\mathbb{Z},\ a\mathbb{Z} \supset c\mathbb{Z} \Longrightarrow a\mathbb{Z} \supset b\mathbb{Z} + c\mathbb{Z}$.)
e) $a|b$, $a\not|\,c \Rightarrow a\not|\,bb' + c$.
Sonst wäre $a|bb' + c - bb' = c$.

**1.14** Seien $a, b \in \mathbb{Z}$. Nach 1.10 gibt es genau ein $d \in \mathbb{N}$ mit
$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
Für dieses $d$ gilt folgende

**Feststellung:** 1) $d|a$, $d|b$;
2) $c|a$, $c|b \Longrightarrow c|d$;
3) *es gibt* $a', b' \in \mathbb{Z}$ *mit* $d = aa' + bb'$.

**Beweis:** 1) $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \overset{1.9d)}{\Longrightarrow} d\mathbb{Z} \supset a\mathbb{Z},\ d\mathbb{Z} \supset b\mathbb{Z}$.
2) $c\mathbb{Z} \supset a\mathbb{Z},\ b\mathbb{Z} \overset{1.9d)}{\Rightarrow} c\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
3) $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. $\square$

**Definition: 1.15** *Wenn $d \in \mathbb{N}$ zu $a, b$ wie oben bestimmt ist, heißt $d$ der größte gemeinsame Teiler von $a$ und $b$. Man schreibt $d = ggT(a, b)$.*

**Satz: 1.16** *Seien* $a, b \in \mathbb{Z}$, $d \in \mathbb{N}$.
*a) Wenn* $d$ *die Eigenschaften 1) und 2) aus 1.14 hat, ist* $d = ggT(a, b)$.
*b) Wenn* $d$ *die Eigenschaften 1) und 3) aus 1.14 hat, ist ebenfalls* $d = ggT(a, b)$.

**Beweis: a)** Wegen 1) gilt $d\mathbb{Z} \supset a\mathbb{Z}, b\mathbb{Z}$, also $d\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z}$.
Wenn $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ ist, so gilt $c\mathbb{Z} \supset d\mathbb{Z}$ wegen 2).
Also ist $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z} \supset d\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z}$, mithin $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
**b)** Wegen 1) gilt wie oben $d\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z}$. Wegen 3) hat man $d \in a\mathbb{Z} + b\mathbb{Z}$, also $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. Insgesamt ist $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. □

### 1.17 Der Euklidische Algorithmus

Ein schnelles Verfahren zur Berechnung des größten gemeinsamen Teilers.

**Hilfsbemerkung:** *In* $\mathbb{Z}$ *gelte* $a = bc + d$. *Dann ist jeder gemeinsame Teiler von* $a$ *und* $b$ *auch ein solcher von* $b$ *und* $d$ *und umgekehrt. D.h. für* $t \in \mathbb{Z}$ *hat man:*

$$t|a,\ t|b \iff t|b,\ t|d.$$

Der Algorithmus läuft wie folgt: Seien $a, b \in \mathbb{Z} - \{0\}$. (ggT$(a, 0) = |a|$.) Setze $r_0 := a,\ r_1 = b$. Dividiere mit Rest nach und nach:

$$\begin{array}{lll} r_0 = r_1 q_1 + r_2 & \text{mit} & |r_2| < |r_1| \\ r_1 = r_2 q_2 + r_3 & \text{mit} & |r_3| < |r_2| \\ r_2 = r_3 q_3 + r_4 & \text{mit} & |r_4| < |r_3| \quad \textit{usw.} \end{array}$$

Solange $r_i \neq 0$ ist, kann man $q_i, r_{i+1}$ finden mit

$$r_{i-1} = r_i q_i + r_{i+1} \qquad \text{und} \qquad |r_{i+1}| < |r_i|.$$

Da aber $|r_1| > |r_2| > \ldots > |r_i| > |r_{i+1}|$ gilt, muss zweifellos für ein $n$ der Rest $r_{n+1}$ verschwinden. Das Verfahren bricht also ab:

$$\begin{array}{rcl} r_{n-2} & = & r_{n-1} q_{n-1} + r_n \qquad \text{mit} \qquad 0 < |r_n| < |r_{n-1}| \\ r_{n-1} & = & r_n q_n + 0. \end{array}$$

**Behauptung:** $|r_n| = \text{ggT}(a, b)$.

Denn da $a = r_0,\ b = r_1$, gilt $t|a,b \iff t|r_0,r_1$.
Wegen obiger Hilfsbemerkung hat man die Äquivalenzen

$$t|r_0,r_1 \iff t|r_1,r_2 \iff t|r_2,r_3 \iff \dots t|r_{n-1},r_n \iff t|r_n,0.$$

Es folgt $\mathrm{ggT}(a,b) = \mathrm{ggT}(r_n,0) = |r_n|$ mit 1.14, 1.16. □

**1.18** Man bekommt mit obigem Algorithmus auch eine Darstellung von $r_n$ in der Form $aa' + bb'$, d.h. als sogenannte Linearkombination von $a$ und $b$.

**Hilfsbemerkung:** *Seien $c = aa_1 + bb_1$ und $d = aa_2 + bb_2$ als Linearkombinationen von $a$ und $b$ gegeben. Dann erhält man jede Linearkombination $cc' + dd'$ von $c$ und $d$ explizit als Linearkombination von $a$ und $b$; es ist nämlich $cc' + dd' = (aa_1 + bb_1)c' + (aa_2 + bb_2)d' = a(a_1c' + a_2d') + b(b_1c' + b_2d')$.*

Wir betrachten wieder die Gleichungsfolge aus 1.17. Zunächst sind $r_1 = b$ nach $r_2 = a - bq_1$ als Linearkombinationen von $a$ und $b$ gegeben. Falls man schon induktiv $r_{i-1}$ und $r_i$ als Linearkombinationen von $a$ und $b$ gewonnen hat, gewinnt man auch $r_{i+1}$ als eine solche, da $r_{i+1} = r_{i-1} - r_iq_i$ gilt.

**1.19** Wenn man beim euklidischen Algorithmus mit möglichst wenigen Schritten auskommen will, muss man negative Reste zulassen, um $|r_{i+1}| \le |r_i|/2$ gemäß 0.20 zu erreichen.

**Definition: 1.20** *$a, b \in \mathbb{Z}$ heißen (zueinander) teilerfremd, wenn* $\mathrm{ggT}(a,b) = 1$ *ist.*

**Bemerkungen: 1.21** a) $a, b$ sind teilerfremd genau dann, wenn es $a'$ und $b' \in \mathbb{Z}$ mit $aa' + bb' = 1$ gibt. Dies folgt wegen $1|a,b$ aus 1.16 b).
b) Wenn $a, b$ teilerfremd sind, gibt es für alle $c \in \mathbb{Z}$ Zahlen $\overline{a}, \overline{b} \in \mathbb{Z}$ mit $a\overline{a} + b\overline{b} = c$. ($c = 1 \cdot c = aa'c + bb'c$.)

## AUFGABEN UND HINWEISE

**1)** Welche Massen können Sie mit einer Balkenwaage wiegen, wenn Sie beliebig viele Gewichte von 70g und von 125g zur Verfügung haben und in beide Waagschalen Gewichte legen dürfen?

**2)** Zwei große, etwa halbvolle Badewannen stehen nebeneinander. Können Sie mit einem 7- und einem 19-Litermaß durch Hin- und Hergießen erreichen, dass schließlich das Wasser der einen Badewanne um einen Liter vermehrt, das der anderen um einen Liter vermindert ist?

**3)** Seien $a$ und $b$ teilerfremde ganze Zahlen. Dann gibt es ja $a', b' \in \mathbb{Z}$ mit $aa' + bb' = 1$.

Überlegen Sie, auf welche (einfache) Weise man $a'$ und $b'$ verändern kann, ohne dass obige Gleichung an Gültigkeit verliert.
Kann man zum Beispiel $a' \geq 0$ erreichen? (Dies geht, wenn $b \neq 0$ ist.) Mit den Mitteln des §2 kann man sämtliche $a', b'$ mit $aa' + bb' = 1$ bestimmen. Vgl. 2.A5

**4)** Seien $m, n \in \mathbb{N}_1$ zueinander teilerfremd. Zeigen Sie:
a) Es gibt ein $k \in \mathbb{N}$ mit $m|k$ und $n|k+1$. (Man benutze A3.)
b) Die Gleichung $x^m + y^m = z^n$ hat eine Lösung in $\mathbb{N}_1^3$.
(Lösen Sie zunächst $x^k + y^k = z^{k+1}$.)

**5)** Seien $a, b, c \in \mathbb{N}_1$, $\mathrm{ggT}(a, b) = 1$ und $c \geq (a-1)(b-1)$.
Zeigen Sie: Es gibt $a', b' \in \mathbb{N}$(!) mit $c = aa' + bb'$.
(Hinweis: Sei $a' \in \mathbb{N}$ minimal gewählt, so dass $c = aa' + bb'$ mit einem $b' \in \mathbb{Z}$ ist. Dann gilt $a' \leq b-1$. Aus $b' < 0$ würde $aa' + bb' < (a-1)(b-1)$.) folgen.)
Vgl. 2.A7.

**6)** Schreiben Sie die Jahreszahl Ihres Geburtsdatums in der Form $n \cdot 30 + m \cdot 49$ mit $n, m \in \mathbb{N}$.

**7)** a) Seien $a, b \in \mathbb{Z}$. Zeigen Sie: Das lineare Gleichungssystem

$$\begin{aligned} x + y &= a \\ x - y &= b \end{aligned}$$

hat genau dann eine Lösung in $\mathbb{Z}^2$, wenn entweder $a$ und $b$ beide gerade oder $a$ und $b$ beide ungerade sind.

b) Ein quadratischer Platz sei mit $n$ quadratischen Steinplatten gleicher Größe so ausgelegt, dass ein quadratisches Beet ausgespart bleibt. Zeigen Sie: $n \notin 2 + 4\mathbb{Z}$. Die Umkehrung gilt auch, wenn das Beet die Größe 0 haben darf.

c) Welche ganzen Zahlen sind Summen aufeinanderfolgender ungerader Zahlen, d.h. von der Form

$$\sum_{k=m}^{n} (2k+1) \quad ?$$

d) Welche ganzen Zahlen sind von der Form

$$x^2 + y^2 - z^2 \quad ?$$

e) (Am 6. Dezember zu lösen.) Frau Nicole Niklas wurde von ihrem Sohn Kolja gefragt, wie alt sie sei. Aus verständlichen Gründen gab sie nur eine verschlüsselte Antwort: Wenn Du die vierte Potenz meines Alters von der vierten Potenz des Alters Deines Vaters Klaus abziehst, erhältst Du die Zahl 1606160. (Mit dem Alter ist jeweils eine ganze Anzahl von Jahren gemeint.)

**8)** a) Bestimmen Sie $\mathrm{ggT}(11\,111\,111,\ 111\,111\,111\,111\,111)$.
b) Allgemeiner: Bestimmen Sie

$$\mathrm{ggT}(1.....1,\ 1.....1)\ ,$$

wenn die erste Zahl $m$, die zweite $n$ Stellen hat.

c) Noch allgemeiner: Bestimmen Sie

$$\mathrm{ggT}\ \left(\sum_{i=0}^{n-1} d^i,\ \sum_{i=0}^{m-1} d^i\right) \quad \text{für} \ \ n, m, d \in \mathbb{N}_1 .$$

**9)** Sei $m \in \mathbb{N}_2$ und $M$ die Menge aller positiven Teiler von $m$ (einschließlich 1 und $m$). Auf der Menge $M$ kann man folgendes Spiel für 2 Spieler spielen: Abwechselnd belegen die Spieler je eine der Zahlen aus $M$ mit einem Spielstein unter Beachtung folgender Regel: Ist bereits $d \in M$ belegt und gilt $d'|d$, so darf $d'$ nicht mehr belegt werden.

Wer $m$ belegt, hat verloren.
Zeigen Sie: Es gibt eine Gewinnstrategie für den beginnenden Spieler.
(Hinweis: Eine besondere Rolle spielt die Zahl 1. Allgemeiner als angegeben, darf $M$ eine beliebige endliche teilweise – d.h. nicht notwendig total – geordnete Menge mit einem kleinsten und einem davon verschiedenen größten Element sein. Ich kenne übrigens keinen Beweis obiger Behauptung, der eine Gewinnstrategie konkret angibt.)

**10)** Betrachten Sie $\mathbb{Z}^2$ als Punktmenge der Ebene $\mathbb{R}^2$ (wie $\mathbb{G}$ in $\mathbb{C}$ in §12 Abbildung 12). Für welche Punkte aus $\mathbb{Z}^2$ liegt auf ihrer Verbindungsstrecke mit dem Ursprung $(0,0)$ kein weiterer Punkt aus $\mathbb{Z}^2$?

# § 2

# Eindeutige Primfaktorzerlegung

In der Schule hat man gelernt, natürliche Zahlen ($\neq 0$) in Primfaktoren zu zerlegen, z.B. $12 = 2 \cdot 2 \cdot 3$. Und man hat sich daran gewöhnt, dass dies – bis auf die Reihenfolge der Faktoren – nur auf eine Weise möglich ist.
Trotzdem, bevor man seine Hand dafür ins Feuer legt, dass es wirklich keine sehr großen natürlichen Zahlen $n, m (\neq 0)$ gibt, für die $17^n = 19^m$ wäre, möchte man vielleicht doch einen Beweis für die Eindeutigkeit der Primfaktorzerlegung einer Zahl sehen.

**Bemerkung: 2.1** Seien $a, b \in \mathbb{N}_1$. Wenn $a|b$ gilt, ist $a \leq b$ – aber natürlich nicht umgekehrt.
Denn $a|b$ bedeutet $b = ac$ für ein $c$, welches offenbar in $\mathbb{N}_1$ liegt. Also ist $b = a \cdot c \geq a \cdot 1 = a$.
Insbesondere folgt für $a, b \in \mathbb{N}_1$ aus $a|b$ und $b|a$, dass $a = b$ ist.

Diese Tatsache ist auf $\mathbb{N}_1$ beschränkt: $1001|0$ und $3| - 6$.

**Definition: 2.2** *a) Eine Zahl $a \in \mathbb{N}_1$ heißt irreduzibel, wenn*

*1) $a \neq 1$ ist und*

*2) aus $a = bc$ mit $b, c \in \mathbb{N}_1$ folgt, dass $b = 1$ oder $c = 1$ ist.*

*(Äquivalent zu 2) ist jede der beiden folgenden Aussagen:*

*2') Aus $a = bc$ mit $b, c \in \mathbb{N}_1$ folgt, dass $c = a$ oder $b = a$ ist;*

*2") aus $b|a$ und $b \in \mathbb{N}_1$ folgt, dass $b = 1$ oder $b = a$ ist.)*

*b) Ein Element $a \in \mathbb{N}_1$ heißt prim, wenn*

*1) $a \neq 1$ ist und*

*2) aus $a|bc$ mit $b, c \in \mathbb{N}$ folgt, dass $a|b$ oder $a|c$ gilt.*

**Bemerkungen: 2.3** a) Man beachte, dass wir die irreduziblen Zahlen vorläufig nicht als Primzahlen bezeichnen. Wir werden allerdings sofort zeigen, dass in $\mathbb{N}_1$ die Begriffe „irreduzibel" und „prim" äquivalent sind.

b) Wenn $a$ prim ist und $a|b_1 \cdot \ldots \cdot b_n$ gilt, ist $a|b_i$ für (mindestens) ein $i \in \{1, \ldots, n\}$. (Induktion nach $n$.)

c) Sei $a \in \mathbb{N}_1$. Dann gilt die Äquivalenz:

$a$ ist irreduzibel $\iff$

$a\mathbb{Z}$ ist eine maximale Untergruppe von $\mathbb{Z}$, d.h.

1) $a\mathbb{Z} \neq \mathbb{Z}$ und
2) wenn $H$ eine Untergruppe von $\mathbb{Z}$ mit $a\mathbb{Z} \subset H \subset \mathbb{Z}$ ist, gilt $H = a\mathbb{Z}$ oder $H = \mathbb{Z}$.

Dies folgt aus den Tatsachen, dass $H$ von der Form $b\mathbb{Z}$ und $b\mathbb{Z} \supset a\mathbb{Z}$ zu $b|a$ äquivalent ist.

**2.4 Lemma** *(Euklid): Ein Element $a \in \mathbb{N}_1$ ist genau dann irreduzibel, wenn es prim ist.*

**Beweis:** Sei $a$ prim und $a = bc$. Dann gilt $a|bc$, also nach Voraussetzung $a|b$ oder $a|c$; etwa $a|b$. Da auch $b|a$ ist, erhalten wir $b = a$.
Die eigentliche Aussage ist die Umkehrung: Sei also $a$ irreduzibel mit $a|bc$. Zu zeigen ist dann $a|b$ oder $a|c$.

Erster Beweis hierfür (GAUSS):
Die Menge $H := \{x \in \mathbb{Z} \mid a|bx\}$ ist – wie man leicht sieht – eine Untergruppe von $\mathbb{Z}$. ($a|b\cdot 0$; wenn $a|bx, by$, dann $a|bx - by = b(x-y)$.) Ferner sind $a, c \in H$. Ist nun $H = m\mathbb{Z}$ mit $m \in \mathbb{N}$, so gilt mithin $m|a, m|c$. Da $a$ irreduzibel ist, ist $m = 1$ oder $m = a$. Im ersten Fall gilt $a|b \cdot 1 = b$, im zweiten $a = m|c$.

Zweiter Beweis: Die irreduzible Zahl $a$ teile $bc$, aber nicht $b$. Dann sind $b$, $a$ teilerfremd und es gibt deshalb $b'$, $a' \in \mathbb{Z}$ mit $bb' + aa' = 1$. Es folgt $a \mid cbb' + caa' = c$. $\square$ Im zweiten Beweis wird 1.16 gebraucht, während der Gaußsche Beweis mit 1.6 auskommt.

**Definition: 2.5** *Eine Primzahl ist ein primes Element aus* $\mathbb{N}_1$. *Die Menge aller Primzahlen wird mit* $\mathbb{P}$ *bezeichnet.*
*Also* $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$.

**Satz: 2.6** *a) Jedes* $a \in \mathbb{N}_1$ *lässt sich als Produkt von Primzahlen schreiben. (1 ist das „leere“ Produkt – ein Produkt ohne Faktoren –, eine Primzahl ein Produkt mit nur einem Faktor.)*
*b) Eine solche Darstellung ist bis auf die Reihenfolge eindeutig, d.h. wenn*

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

*mit Primzahlen* $p_i, q_j$ *ist, so gilt*

1) $r = s$ *und*

2) *es gibt eine Permutation* $\sigma$ *der Menge* $\{1, \ldots, r\}$ *mit* $p_i = q_{\sigma(i)}$ *für alle* $i$.

*(Dass* $\sigma$ *eine Permutation ist, heißt* $\sigma : \{1, \ldots, r\} \longrightarrow \{1, \ldots, r\}$ *ist eine bijektive Abbildung.)*

**Beweis:** a) Wir nehmen an, die Behauptung sei falsch und $a$ die kleinste Zahl aus $\mathbb{N}_1$, die nicht Produkt von Primzahlen ist. Dann ist $a$ weder gleich 1 noch eine Primzahl, also auf nicht triviale Weise ein Produkt $a = bc$. Es folgt $b < a$ und $c < a$, da $b \neq a \neq c$. Da sich $b$ und $c$ wegen der Minimalitätsannahme über $a$ als Produkt von Primzahlen schreiben lassen, gilt dies aber auch für $a$. Widerspruch!

b) Wir nehmen wieder das Gegenteil der Behauptung an. Sei $n \in \mathbb{N}_1$ die kleinste Zahl, die zwei verschiedene Primfaktorzerlegungen besitzt, etwa die folgenden:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

Dann ist $n > 1$, also $r, s > 0$, und es gilt $p_i \neq q_j$ für alle $i$ und $j$. Wäre nämlich $p_i = q_j$, so hätte die kleinere Zahl $n/p_i (= n/q_j)$ offenbar ebenfalls zwei verschiedene Primfaktorzerlegungen. Da $p_1|n$ und $p_1$ eine Primzahl ist, gilt $p_1|q_k$ für ein $k$. Hieraus folgt $p_1 = q_k$, da $q_k$ irreduzibel und $p_1 \neq 1$ ist. Widerspruch! □

**Bemerkungen: 2.7** a) Ohne Euklids Lemma 2.4 würde obiger Beweis nur folgendes zeigen:

1) Jedes $a \in \mathbb{N}_1$ ist Produkt irreduzibler Zahlen.

2) Wenn $a$ ein Produkt von primen Zahlen ist, so sind diese bis auf die Reihenfolge eindeutig bestimmt.

b) Dass die Eindeutigkeit der Zerlegung in irreduzible Faktoren nicht selbstverständlich ist, kann man an folgendem Beispiel erkennen.
Sei $H := \mathbb{N}_1 - \{2\} = \{1, 3, 4, 5, \ldots\}$. Für $a, b \in H$ gilt $ab \in H$. In $H$ sind z.B. die folgenden Elemente irreduzibel: 3, 4, 6, 8. Und es gilt $3 \cdot 8 = 4 \cdot 6$.

**Korollar: 2.8** *Sei $a \in \mathbb{Z} - \{0\}$. Dann ist $a = \pm p_1 \cdot \ldots \cdot p_r$ mit Primzahlen $p_i$, die im wesentlichen eindeutig bestimmt sind, d.h. für jede Primzahl $p$ ist eindeutig bestimmt, wie oft sie in dem Produkt $p_1 \cdot \ldots \cdot p_r$ auftritt. (Natürlich treten nur endlich viele Primzahlen mehr als 0-mal auf.)*

**Definition: 2.9** *Man nennt die Darstellung $a = \pm p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von $a$ und die auftretenden $p_i$ die Primfaktoren von $a$.
Ein Primfaktor von $a$ ist also eine Primzahl $p$ mit $p|a$.*

**2.10** Man kann die eindeutige Darstellbarkeit ganzer Zahlen als Produkt von Primzahlen auch anders formulieren:

Dazu bezeichnen wir die Primzahlen der Größe nach mit $p_1, p_2, p_3, \ldots$, also $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$.

Für $a \in \mathbb{Z} - \{0\}$ gilt dann $a = \pm \prod\limits_{i=1}^{\infty} p_i^{\alpha_i}$ mit geeigneten $\alpha_i \in \mathbb{N}$, wobei $\alpha_i = 0$ für fast alle $i$ ist. In dieser Darstellung sind die $\alpha_i$ durch $a$ eindeutig bestimmt.

**Definition: 2.11** *Für $p \in \mathbb{P}$, $a \in \mathbb{Z} - \{0\}$ definieren wir $v_p(a) := \alpha_i$, wenn $p = p_i$ – gemäß den Bezeichnungen von 2.10 ist.*

Es gilt also $v_p(a) = n$, wenn $p^n | a$ und $p^{n+1} \nmid a$. Insbesondere ist genau dann $v_p(a) = 0$, wenn $p$ kein Primfaktor von $a$ ist.

Man kann noch $v_p(0) := \infty$ definieren. (Dabei ist $\infty$ nichts Geheimnisvolles, sondern lediglich ein Symbol, welches hier gewählt wurde, weil $p^n | 0$ für alle $n \in \mathbb{N}$ gilt.)

Für jedes $p \in \mathbb{P}$ erhält man also eine Abbildung $v_p : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{\infty\}$.
Es gilt: $a = \pm \prod\limits_{p \in \mathbb{P}} p^{v_p(a)}$ für $a \neq 0$.

**Feststellungen: 2.12** *Seien $a, b \in \mathbb{Z}$.*
*a)* $v_p(ab) = v_p(a) + v_p(b)$.
Denn Primfaktorzerlegungen von $a$ und $b$ ergeben eine solche von $ab$. Und es gibt im wesentlichen nur eine Primfaktorzerlegung von $ab$.
*b)* $a | b \iff v_p(a) \leq v_p(b)$ *für alle* $p \in \mathbb{P}$.
*c)* $v_p(\mathrm{ggT}(a, b)) = \mathrm{Min}\,\{v_p(a), v_p(b)\}$. *Mit anderen Worten:*
$\mathrm{ggT}\left(\pm \prod\limits_{i=1}^{\infty} p_i^{\alpha_i}, \pm \prod\limits_{i=1}^{\infty} p_i^{\beta_i}\right) = \prod\limits_{i=1}^{\infty} p_i^{\mathrm{Min}\{\alpha_i, \beta_i\}}$ . *(* $\mathrm{Min}\{\alpha_i, \beta_i\}$ *ist die kleinere der beiden Zahlen $\alpha_i, \beta_i$ und nicht etwa als Minimum aller $\alpha_i, \beta_i$, $i \in \mathbb{N}_1$ misszuverstehen.)*

Der Satz von der eindeutigen Primfaktorzerlegung hat Konsequenzen auch außerhalb des Bereiches der ganzen Zahlen:

**Satz: 2.13** *Sei $\rho \in \mathbb{Q} - \mathbb{Z}$. Dann ist $\rho^r \notin \mathbb{Z}$ für alle $r \in \mathbb{N}_1$.*

**Beweis:** Sei $\rho = a/b$ mit $a, b \in \mathbb{Z}$ und $\mathrm{ggT}(a, b) = 1$ – d.h. der Bruch $a/b$ sei gekürzt. Es gelte etwa $a = \pm p_1 \cdot \ldots \cdot p_s$, $b = q_1 \cdot \ldots \cdot q_t$ mit $p_i$, $q_j \in \mathbb{P}$. Da $a, b$ teilerfremd sind, ist $p_i \neq q_j$ für alle $i$ und $j$. Aus $\rho \notin \mathbb{Z}$ folgt $t > 0$. Dann ist $\rho^r = \dfrac{a^r}{b^r} = \pm \dfrac{p_1^r \cdot \ldots \cdot p_s^r}{q_1^r \cdot \ldots \cdot q_t^r}$. Wegen der Eindeutigkeit der Primfaktorzerlegung ist letzter Bruch ebenfalls gekürzt mit einem von $\pm 1$ verschiedenen Nenner. Mithin ist $\rho^r \notin \mathbb{Z}$. □

**Korollar: 2.14** *Sei $a \in \mathbb{N}_1$ keine $r$–te Potenz einer ganzen Zahl. Dann ist $\sqrt[r]{a}$ irrational (d.h. $\notin \mathbb{Q}$).*

**Beweis:** Angenommen, $\rho = \sqrt[r]{a}$ wäre rational (d.h. $\in \mathbb{Q}$). Da $\rho$ nach Voraussetzung nicht ganz ist, würde mit 2.13 folgen $a = \rho^r \notin \mathbb{Z}$. Widerspruch. □

**Satz: 2.15** *(Verallgemeinerung von 2.14)*
*Jede (komplexe) Nullstelle eines Polynoms $\sum\limits_{i=0}^{n} a_i X^i$ mit $a_n = 1$ und $a_i \in \mathbb{Z}$ ist ganz (d.h. $\in \mathbb{Z}$) oder irrational (d.h. $\notin \mathbb{Q}$).*

**Beweis:** Sei $\rho = \dfrac{b}{c} \in \mathbb{Q}$ eine Nullstelle, $b, c \in \mathbb{Z}$, $\mathrm{ggT}(b, c) = 1$. Es gilt $\sum\limits_{i=0}^{n} a_i \rho^i = 0$, d.h. $\sum\limits_{i=0}^{n-1} a_i \dfrac{b^i}{c^i} + \dfrac{b^n}{c^n} = 0$, da $a_n = 1$ ist. Durch Multiplikation mit $c^n$ erhält man die Gleichung

$$b^n = -\sum_{i=0}^{n-1} a_i b^i c^{n-i}.$$

Für $i \leq n - 1$ ist $n - i > 0$.

Wäre nun $c \neq \pm 1$, so hätte $c$ einen Primfaktor $p$. Da offenbar $p$ die rechte Seite teilt, erhielte man $p | b^n$. Wegen der Eindeutigkeit der Primfaktorzerlegung (oder 2.3 b)) folgte $p | b$. Deshalb hätten $b$ und $c$ den gemeinsamen Teiler $p$ im Widerspruch zu ihrer Teilerfremdheit. □

## AUFGABEN UND HINWEISE

**1)** Ohne Benutzung des euklidischen Lemmas kann man nach Zermelo zeigen:
*Jede natürliche Zahl* $> 0$ *lässt sich (bis auf die Reihenfolge) auf nur eine Weise als Produkt irreduzibler Faktoren darstellen.*
Beweisskizze: Sei $a \in \mathbb{N}_1$ minimal mit zwei verschiedenen Zerlegungen in irreduzible Faktoren:

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s.$$

Dann sind $r, s > 0$, und man kann $p_i \neq q_j$ für alle $i, j$ zeigen. Man kann also ohne Beschränkung der Allgemeinheit annehmen, dass $q_1 < p_1$ ist. Damit besitzt

$$b := (p_1 - q_1)p_2 \cdot \ldots \cdot p_r = a - q_1 p_2 \cdot \ldots \cdot p_r = q_1(q_2 \cdot \ldots \cdot q_s - p_2 \cdot \ldots \cdot p_r)$$

zwei verschiedene Zerlegungen in irreduzible Faktoren, ist aber kleiner als $a$ (und größer als 0).
Aus *Zermelos* Satz folgt das euklidische Lemma.

**2)** Theoretisch kann man die Primfaktorzerlegung einer natürlichen Zahl $n$ durch systematisches Probieren finden: $p_1$ sei der kleinste Teiler $> 1$ von $n$, $p_2$ derjenige von $n/p_1$ usw.
Der Leser mag Überschlagsrechnungen darüber anstellen, wie lange ein guter Computer für dieses Verfahren bei einer 100–stelligen Zahl bräuchte. (Ein Jahr hat knapp 32 Mio. Sekunden.) Für schnellere Verfahren, siehe [*Riesel*].
Den ggT bestimmt man (zumindest für größere Zahlen) mit dem euklidischen Algorithmus (oder Verfeinerungen desselben) und nicht etwa mit 2.12 c)!

**3)** Ein Zahlenrätsel:

$$\begin{aligned} EULER &= SB \cdot RL^E \\ GAUSS &= L \cdot A \cdot LUL \cdot E^E \\ ABEL &= A \cdot RR \cdot RL \cdot L \end{aligned}$$

Wenn man jeden Buchstaben durch eine Ziffer des Dezimalsystems ersetzt, steht in jeder Gleichung rechts die Primfaktorzerlegung der linken Seite. (Natürlich sind gleiche Buchstaben durch gleiche Ziffern zu ersetzen, aber nicht notwendig verschiedene Buchstaben durch verschiedene Ziffern. Die Zahlen dürfen mit der Ziffer 0 beginnen.)
Bestimmen Sie sämtliche Lösungen. (Durch geschicktes Vorgehen kann man erreichen, dass man nur einmal mehrere Möglichkeiten durchprobieren muss.)

**4)** Bestimmen Sie die ganzzahligen Lösungen einer Gleichung folgender Gestalt:

$$ax = by, \ a, b \in \mathbb{Z}.$$

(Man kann auf den Fall $\mathrm{ggT}(a, b) = 1$ reduzieren.)

**5)** Betrachten Sie eine Gleichung der Form

$$ax + by = c \text{ mit } a, b, c \in \mathbb{Z}.$$

a) Unter welcher Bedingung existieren ganzzahlige Lösungen?
b) Wie kann man – im Falle der Lösbarkeit – eine Lösung bestimmen?
c) Wie kann man alle Lösungen bestimmen, wenn man eine bereits kennt? (A4)
d) Vergleichen Sie Ihre Ergebnisse mit denen zu 1.A3.

**6)** Die AAA (Amelsbürener Arithmetische Association) kauft für ihr Weihnachtsfest 123 Stück Geflügel (Hähnchen, Wachteln, Gänse) für 456 Gulden. Ein Hähnchen kostet $1\frac{2}{3}$, eine Wachtel $4\frac{5}{6}$, eine Gans $7\frac{8}{9}$ Gulden. Wieviel Stück kauft die AAA von jeder Sorte?
*(Paul Chybiorz 1874)*

**7)** Seien $a, b \in \mathbb{N}$, $\mathrm{ggT}(a, b) = 1$. Gibt es $x, y \in \mathbb{N}$ mit

$$ax + by = (a - 1)(b - 1) - 1?$$

(Mit A5, vgl. 1.A5.)
In [*Scheid*] VII.9 wird das in 1.A5 und hier betrachtete Problem für mehr als nur zwei Zahlen $a, b$ behandelt.

**8)** Bei einer Uhr seien der Stunden-, der Minuten- und der Sekundenzeiger kontinuierlich laufend, zentral angebracht und genau koordiniert, so dass um Punkt 12 Uhr alle 3 Zeiger genau übereinanderstehen. Zu welchen anderen Zeiten stehen alle 3 Zeiger genau übereinander?
(Vgl. A4)

**9)** Seien $p_1, \ldots, p_n$ untereinander verschiedene Primzahlen.
Zeigen Sie:
$\sum\limits_{i=1}^{n} \dfrac{1}{p_i} \notin \mathbb{Z}$. (Man kann durch Multiplikation mit einer Zahl alle Summanden bis auf einen ganz machen.)

**10)** Ähnlich, aber nicht völlig analog beweist man folgende Aussagen:

$$\sum_{k=1}^{n} \frac{1}{k} \notin \mathbb{Z} \quad , \quad \sum_{k=1}^{n} \frac{1}{2k-1} \notin \mathbb{Z}$$

für $n \geq 2$.

**11)** Sei $p$ eine (fest gewählte) Primzahl. Zeigen Sie:
a) Jede von 0 verschiedene rationale Zahl $\alpha$ lässt sich in der Form $\alpha = p^n \cdot \frac{a}{b}$ mit $a, b, n \in \mathbb{Z},\ p \nmid ab$ schreiben. Dabei ist $n$ durch $\alpha$ eindeutig bestimmt. Definiere $v_p(\alpha) = n$, wenn $\alpha$ obige Darstellung hat, ferner $v_p(0) = \infty$.

b) Diese Abbildung setzt die in 2.11 definierte Abbildung

$$v_p : \mathbb{Z} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

zu einer Abbildung

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

fort.

c) $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ hat folgende Eigenschaften:

1) $v_p(x) = \infty \iff x = 0$;

2) $v_p(xy) = v_p(x) + v_p(y)$;

3) $v_p(x + y) \geq \text{Min}\,\{v_p(x), v_p(y)\}$.

**12)** a) Sei $S \subset \mathbb{Z} - \{0\}$ eine multiplikative Teilmenge, d.h. $1 \in S$, und mit $s, t \in S$ ist auch $st \in S$. Zeigen Sie:
Die Menge $S^{-1}\mathbb{Z} := \left\{\frac{a}{s} | a \in \mathbb{Z},\ s \in S\right\}$ ist ein Unterring von $\mathbb{Q}$.
b) Sei $A$ ein Unterring von $\mathbb{Q}$ und $a/s \in A$ mit $a, s \in \mathbb{Z}$, $\mathrm{ggT}(a, s) = 1$. Zeigen Sie: $1/s \in A$.
c) Zeigen Sie: Jeder Unterring von $\mathbb{Q}$ ist von der Form $S^{-1}\mathbb{Z}$ mit einer multiplikativen Menge $S \subset \mathbb{Z} - \{0\}$.

d) Zeigen Sie: Die abbrechenden Dezimalbrüche bilden einen Unterring von $\mathbb{Q}$ **13)** Sei $p$ eine Primzahl und $v_p$ wie in A11 definiert. Zeigen Sie:
a) $\{x \in \mathbb{Q} | v_p(x) \geq 0\}$ ist ein Unterring $\mathbb{Z}_{(p)}$ von $\mathbb{Q}$.
b) $\mathbb{Z}_{(p)} := S^{-1}\mathbb{Z}$, wobei $S = \left\{ n \in \mathbb{N}_1 \;\middle|\; p \nmid n \right\}$.

**14)** Mit den in A11 definierten Abbildungen $v_p$ kann man 2.13 und 2.15 noch etwas eleganter beweisen. Wie?

**15)** a) Seien $p_1, \ldots, p_n$ verschiedene Primzahlen. Zeigen Sie:
$\log p_1, \ldots, \log p_n$ sind linear unabhängig in dem $\mathbb{Q}$–Vektorraum $\mathbb{R}$.
b) Folgern Sie: Es gibt höchstens eine Primzahl $p$ mit $\log p \in \mathbb{Q}$. (In Wahrheit gibt es gar keine solche, da $e$ transzendent ist. Mit log wird hier der natürliche Logarithmus bezeichnet.)

**16)** Für $a, b \in \mathbb{Z}$, $b \neq 0$, definiere $\mathrm{kgV}(a, b) := \dfrac{|ab|}{\mathrm{ggT}(a, b)}$. Zeigen Sie:
a) $\mathrm{kgV}(a, b) \in \mathbb{N}$ und $a, b |\ \mathrm{kgV}(a, b)$.
b) $a, b | c \Longrightarrow \mathrm{kgV}(a, b) | c$.
c) $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{kgV}(a, b)\mathbb{Z}$.

**17)** Bestimmen Sie $\mathrm{ggT}(n! + 1, (n + 1)! + 1)$.

**18)** a) Gibt es eine quadratische Tischplatte, die man mit Postkarten lückenlos und ohne Überlappungen bedecken kann? Die Länge einer Postkarte verhält sich zur Breite wie $\sqrt{2} : 1$.
(Nehmen Sie an, die Tischplatte sei $n$ Kartenbreiten plus $m$ Kartenlängen breit. Wie viele Karten brauchen Sie, um eine Fläche entsprechenden

Ausmaßes zu bedecken?)

b) Etwas geometrischer als für a) muss man vielleicht argumentieren, wenn man die allgemeinere Frage beantworten will, ob man ein Quadrat mit zueinander kongruenten Rechtecken ohne Überlappung bedecken kann, deren Länge und Breite zueinander inkommensurabel sind (d.h. in einem irrationalen Verhältnis zueinander stehen).

**19)** In der Musik werden zwei Tonintervalle als „gleichgroß“ bezeichnet – und auch als gleichgroß empfunden, wenn die beiden Tonfrequenzverhältnisse des jeweils höheren Tones zum jeweils tieferen Ton eines Intervalles gleich sind.
a) Die Frequenzverhältnisse sind bei einer (reinen) Oktave 2, bei einer reinen Quint $\frac{3}{2}$, bei einer reinen großen Terz $\frac{5}{4}$.
Wenn man von einem Grundton aus 4 reine Quinten auf- und anschließend 2 Oktaven absteigt, ist man dann eine reine große Terz oberhalb des Grundtones gelandet? („Syntonisches“ oder „didymisches Komma“)
Könnte man dieses eventuell erreichen, indem man andere Anzahlen von Quinten und Oktaven auf- und absteigt?
b) Die Oktave sei in $n$ ($\in \mathbb{N}_1$) gleichgroße Tonschritte (Intervalle) geteilt. Was ist das Frequenzverhältnis der beiden Töne eines solchen Tonschrittes? (Für $n = 12$ erhält man die 12 Halbtonschritte der temperierten Stimmung.)
c) Gesucht ist ein $n \in \mathbb{N}_1$, so dass für die Unterteilung der Oktave in $n$ gleichgroße Tonschritte folgendes gilt:
Wenn man vom Grundton der Oktave geeignet viele solche Tonschritte aufsteigt, landet man eine reine Quinte oberhalb des Grundtones.
Frage: Gibt es ein solches $n$ ?
d) Wenn man von einem Grundton aus einerseits 6 reine Quinten auf- und anschließend 3 Oktaven absteigt, andererseits 6 reine Quinten ab- und anschließend 4 Oktaven aufsteigt, trifft man dann auf exakt denselben Ton? („Pythagoreisches Komma“)

**20)** Ein weiterer Beweis des euklidischen Lemmas:
Sei $p \in \mathbb{N}$ irreduzibel. Sei $a \in \mathbb{N}_1$ minimal, derart, dass es ein $b \in \mathbb{N}_1$ gibt, so dass zwar $p|ab$, aber $p \nmid a$, $p \nmid b$ gilt. Insbesondere ist $a \neq p$. Betrachten Sie zwei Fälle:
1. Fall: $a > p$. Dann gilt $p|(a-p) \cdot b$, aber $p \nmid a - p$ und $p \nmid b$.

2. Fall: $a < p$. Es gibt $q, r \in \mathbb{N}$ mit $p = aq + r$, $r < a$. Die Möglichkeit $r = 0$ kann ausgeschlossen werden. Somit folgt $p \nmid aq$. Wieder gilt: $p|(p - aq)b = rb$, aber $p \nmid r$, $p \nmid b$, $r < a$.

**21)** Zeigen Sie: $e := \sum_{\nu=0}^{\infty} 1/\nu!$ ist irrational. (Hinweis: Für jedes $n \in \mathbb{N}_1$ ist $n! \cdot e \notin \mathbb{N}$. Man kann nämlich $n! \cdot e$ als Summe zweier Summanden schreiben, deren erster offensichtlich ganz ist und deren zweiter echt zwischen 0 und 1 liegt. Diese Abschätzung ist leichter, wenn man $e^{-1} = \sum_{\nu=0}^{\infty} (-1)^\nu/\nu!$ behandelt.) Interessanter und schwieriger zu zeigen ist, dass $e$ sogar transzendent ist, d.h. keiner (nichttrivialen) algebraischen Gleichung mit rationalen Koeffizienten genügt. Siehe z.B.[*Lorenz*] §17.

**22)** Wer etwas über Determinanten und ihren Nutzen weiß, mag versuchen, folgendes zu zeigen: Für alle $a, b, c, d \in \mathbb{Q}$ besitzt das lineare Gleichungssystem

$$\begin{array}{rrrcl} x & +5y & +az & = & b \\ (a-1)x & -4y & & = & c \\ & (a+7)y & +z & = & d \end{array}$$

genau eine Lösung in $\mathbb{Q}^3$.

# § 3

# Primzahlen

Wenn man eine Primzahltafel studiert, sieht man, dass die Primzahlen anscheinend recht willkürlich unter den natürlichen Zahlen verteilt sind. Mal gibt es große Lücken zwischen ihnen, mal kleine. Und das, obwohl die Definition einer Primzahl (etwa als irreduzible natürliche Zahl) sehr einfach ist. Um so bemerkenswerter erscheint mir, dass es gelungen ist, interessante Gesetzmäßigkeiten für Primzahlen zu entdecken, von denen wir hier nur einen schwachen Abglanz geben können.
Der Inhalt dieses Paragrafen wird im übrigen Buch nicht gebraucht werden. Den folgenden Satz (3.1) sollte allerdings jeder gebildete Erwachsene kennen.

**3.1 Satz** (Euklid): *Es gibt unendlich viele Primzahlen.*

**Beweis:** Zu jeder endlichen Menge $\{p_1, \ldots, p_n\}$ von Primzahlen konstruieren wir eine weitere Primzahl. Sei nämlich $N := p_1 \cdot \ldots \cdot p_n$. Wenn $n = 0$ ist, ist $N = 1$. Da $N + 1 > 1$ ist, besitzt $N + 1$ wenigstens einen Primfaktor $p$. Ein solcher ist verschieden von allen $p_i$, da letztere $N$, aber nicht 1, also $N + 1$ nicht teilen. □

**Bemerkungen: 3.2** a) Der Beweis zeigt folgendes: Wenn $p_1, \ldots, p_n$ die ersten $n$ Primzahlen sind, so gilt für die $(n + 1)$–te Primzahl

$$p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1.$$

Wir werden im folgenden wesentlich mehr zeigen, z.B. die – immer noch schwache – Aussage

$$p_{n+1} \leq \frac{5}{2} p_n.$$

b) Es ist keineswegs so, dass $p_1 \cdot \ldots \cdot p_n + 1$ wieder eine Primzahl sein muss, wenn $p_1, \ldots, p_n$ die ersten $n$ Primzahlen sind. Z.B. ist

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

**Satz: 3.3** *Es gibt beliebig große Lücken zwischen aufeinanderfolgenden Primzahlen.*

**Beweis:** Für $n \geq 2$ sind alle natürlichen Zahlen $x$ mit $n! + 2 \leq x \leq n! + n$ durch eine der Zahlen $2, 3, 4, \ldots, n$ teilbar und größer als $n$, also keine Primzahlen. □

**Bemerkungen: 3.4** a) Seien $p_1, \ldots, p_n, p_{n+1}$ die ersten $n + 1$ Primzahlen und $N = p_1 \cdot \ldots \cdot p_n$. Dann liegt im Intervall $[N + 2,\, N + p_{n+1} - 1]$ keine Primzahl. Für $n \geq 3$ (d.h. $p_n \geq 5$) gilt das gleiche schon für das Intervall $[N - p_{n+1} + 1, N - 2]$. Diese Primzahllücken liegen in der Zahlenreihe deutlich weiter „links“ als die im Beweis des Satzes angegebenen. In Wirklichkeit liegen „große“ Lücken zwischen Primzahlen in der Regel noch „weiter links“.

b) Man könnte 3.1 auch „analog“ zu 3.3 beweisen: Jeder Primfaktor von $n! + 1$ ist größer als $n$.
Der zuerst gegebene Beweis hat allerdings den Vorteil, dass er sich unmittelbar auf Polynomringe in einer Unbestimmten über (insbesondere endlichen) Körpern übertragen lässt.

Wir wollen uns mit diesen etwas dürftigen Sätzen nicht zufriedengeben. Unendliche Teilmengen von $\mathbb{N}$ können sehr „dünn“ sein, wie zum Beispiel $\{10^n | n \in \mathbb{N}\}$, oder dichter, wie $\{n^2 | n \in \mathbb{N}\}$ oder noch dichter.

**Definition: 3.5** *Für $x \in \mathbb{R}$ wird mit $[x]$ die größte ganze Zahl $\leq x$ bezeichnet. (Gaußklammer)*

Es ist also $[x] \in \mathbb{Z}$ und $x = [x] + \rho$ mit $0 \leq \rho < 1$.
Z.B. $[\sqrt{2}] = 1$, $[-\sqrt{2}] = -2$.

Der folgende Satz könnte – in abgeschwächter Form – aus einem späteren Ergebnis abgeleitet werden. Wir wollen jedoch seinen schönen direkten Beweis bringen.

**3.6 Satz** *(Euler):* $\displaystyle\sum_{p \in \mathbb{P}} \frac{1}{p}$ *divergiert. Genauer gilt*

$\displaystyle\sum_{p \leq x} \frac{1}{p} > \log\log x - \frac{1}{2}$ *für reelle* $x \geq 2$.

(Mit log wird, wie in der Zahlentheorie üblich, der natürliche Logarithmus bezeichnet. Und $p$ ist eine Variable für Primzahlen.)

**Beweis:** Definiere

$$P(x) := \prod_{p \leq x} \frac{1}{1 - p^{-1}} = \prod_{p \leq x} (1 + p^{-1} + p^{-2} + \ldots) = \sum_{\substack{n \in \mathbb{N}_1, \\ \text{deren Primfaktoren } \leq x \text{ sind}}} \frac{1}{n}.$$

Die erste Gleichung entsteht dadurch, dass die Faktoren $1/(1 - p^{-1})$ in geometrische Reihen entwickelt werden. Da diese Reihen absolut konvergieren, erhält man gemäß [*Knopp*] Satz 91 (§17) ihr Produkt, indem man sie entsprechend dem Distributivitätsgesetz ausmultipliziert und die entstehenden Produkte in *beliebiger* Reihenfolge addiert. Jedes Produkt von Gliedern der geometrischen Reihen ist von der Form $p_1^{-\alpha_1} \cdot \ldots \cdot p_r^{-\alpha_r}$, wo $p_1, \ldots, p_r$ die Primzahlen $\leq x$ und die $\alpha_i \in \mathbb{N}$ sind. Für jedes $n \in \mathbb{N}_1$, dessen sämtliche Primfaktoren $\leq x$ sind, erhält man also genau einmal einen Summanden $\frac{1}{n}$. (Eindeutige Primfaktorzerlegung!) Da insbesondere alle $n \leq x$ nur Primfaktoren $p \leq x$ haben und alle Summanden der letzten Reihe positiv sind, erhalten wir die Ungleichung

$$P(x) > \sum_{n=1}^{[x]} \frac{1}{n} = \int_1^{[x]+1} \frac{1}{[t]}\, dt.$$

Die letzte Gleichung gilt, weil die Funktion $\frac{1}{[t]}$ eine Treppenfunktion ist, die auf jedem Intervall $[n, n+1[$ mit $n \in \mathbb{N}_1$ den konstanten Wert $1/n$ annimmt. Da aber $1/[t] \geq 1/t$ für reelle $t \geq 1$ gilt und außerdem $[x]+1 > x$ ist, erhalten wir

$$\int_1^{[x]+1} \frac{1}{[t]}\, dt \geq \int_1^x \frac{1}{t}\, dt = \log x.$$

Abb. 3

Insgesamt gilt $\prod_{p \leq x} \frac{1}{1-p^{-1}} > \log x > 0$ und folglich

$-\sum_{p \leq x} \log(1-p^{-1}) > \log \log x \quad$ für $x > 1$.

Die Taylorreihe des Logarithmus ergibt:

$$-\log\left(1 - \frac{1}{p}\right) = \frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \ldots < \frac{1}{p} + \frac{1}{2p^2}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right)$$

$$= \frac{1}{p} + \frac{1}{2p^2}\left(1 - \frac{1}{p}\right)^{-1} = \frac{1}{p} + \frac{1}{2p(p-1)},$$

wobei wieder die Formel für die geometrische Reihe verwendet wurde. So haben wir schließlich

$$\log \log x < \sum_{p \leq x} \frac{1}{p} + \sum_{p \leq x} \frac{1}{2p(p-1)} < \sum_{p \leq x} \frac{1}{p} + \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \sum_{p \leq x} \frac{1}{p} + \frac{1}{2}.$$

($\sum_{n=2}^{\infty} 1/n(n-1) = 1$ zu zeigen, ist eine beliebte Übungsaufgabe.) □

**3.7** Wenn man dieses Ergebnis mit der Tatsache vergleicht, dass $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2}$ konvergiert, so sieht man, dass man mit einigem Recht sagen kann, die Primzahlen seien häufiger als die Quadratzahlen. Dennoch ist es eine offene und anscheinend sehr schwierige Frage, ob zwischen je zwei aufeinanderfolgenden Quadratzahlen immer eine Primzahl liegt.

**Definition: 3.8** *Für $x \in \mathbb{R}$ sei*

$$\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}.$$

Jede Aussage über das Wachstum dieser Funktion bedeutet eine Aussage über die „Häufigkeit“ der Primzahlen.

**3.9** Im folgenden spielen die Binomialkoeffizienten $\binom{n}{k}$ eine große Rolle. Das liegt daran, dass man einerseits sie selbst, andererseits $v_p\left(\binom{n}{k}\right)$ für Primzahlen $p$ gut abschätzen kann.

Wir erinnern an die triviale Bemerkung $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$. Hieraus folgt sofort $\binom{2n}{n} < 2^{2n} = 4^n$.

**Satz: 3.10** *Für $\pi(2n) - \pi(n)$ (d.h. die Anzahl der Primzahlen zwischen $n$ und $2n$) gilt:*

$$\pi(2n) - \pi(n) < \log 4 \cdot \frac{n}{\log n}, \text{ wenn } n \in \mathbb{N}_2 \text{ ist.}$$

*(Beachte:* $\log 4 = 2\log 2 < \frac{7}{5}$.*)*

**Beweis:** Für Primzahlen $p$ mit $n < p \leq 2n$ gilt $v_p\binom{2n}{n} = 1$. Denn es ist $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, und die genannten Primzahlen tauchen im Zähler $(2n)!$ genau einmal und im Nenner $(n!)^2$ nicht auf:

$v_p\left((2n)!\right) = 1$, $v_p\left((n!)^2\right) = 0$ für die obengenannten $p$.
Also ist $\prod\limits_{n<p\le 2n} p \le \binom{2n}{n} < 4^n$. Andererseits ist $n^{\pi(2n)-\pi(n)} < \prod\limits_{n<p\le 2n} p$.
Aus $n^{\pi(2n)-\pi(n)} < 4^n$ erhält man durch Logarithmieren

$$(\pi(2n) - \pi(n)) \cdot \log n < n \cdot \log 4$$

und daraus den Satz. □

**3.11 Korollar** *(Čebyšev):* $\pi(n) < \frac{8}{5} \cdot \frac{n}{\log n}$ *für* $n > 1$.

**Beweis:** Wir verwenden Induktion nach $n$ und nehmen den Satz für $n \le 2^{16} = 65536$ als nachgeprüft an – etwa durch Nachzählen in Primzahltabellen. (Wer mit dem Faktor 2 anstelle von $\frac{8}{5}$ zufrieden ist, braucht diese Nachprüfung nur für $n \le 2^7 = 128$ vorzunehmen.)
Zum Induktionsschritt: Sei zunächst $n = 2m$ gerade und $> 2^{16}$. Dann ist

$$\pi(n) = \pi(m) + (\pi(2m) - \pi(m)) \tag{1}$$

und

$$\pi(m) < \tfrac{8}{5} \cdot \tfrac{m}{\log m} \tag{2}$$

nach Induktionsvoraussetzung. Ferner ergibt Satz 3.10:

$$\pi(2m) - \pi(m) < \tfrac{m}{\log m} \cdot \log 4 = \tfrac{2m}{\log m} \cdot \log 2. \tag{3}$$

Einer Logarithmentafel oder dem Taschenrechner entnehmen wir:

$$\log 2 \approx 0,6931, \quad \text{also} \quad 0,693 < \log 2 < 0,694,$$

$$\text{und deshalb} \quad 0,8 + \log 2 < 1,494.$$

Hiermit und aus (1) – (3) erhalten wir

$$\pi(n) = \pi(2m) < \left(\frac{8}{5} + \log 4\right) \frac{m}{\log m}$$

$$= \left(\frac{8}{10}+\log 2\right)\frac{2m}{\log(2m)-\log 2} \overset{(4)}{<} 1,494\cdot\frac{16}{15}\left(\frac{2m}{\log(2m)}\right)$$
$$< \frac{15}{10}\cdot\frac{16}{15}\cdot\frac{2m}{\log(2m)} = \frac{8}{5}\frac{n}{\log n},$$

wobei wir (4) wie folgt begründen:

$$\begin{aligned} &\frac{2m}{\log(2m)-\log 2} < \frac{16}{15}\cdot\frac{2m}{\log(2m)} \\ &\iff 15\log(2m) < 16\log(2m) - 16\log 2 \\ &\iff 16\log 2 < \log(2m) \iff 2^{16} < 2m. \end{aligned}$$

Letztere Ungleichung war vorausgesetzt.
Sei jetzt $n = 2m+1$ ungerade.
Es gilt $\pi(n) = \pi(2m+1) \leq \pi(2m)+1 \overset{(5)}{<} 1,494\cdot\frac{16}{15}\frac{2m}{\log(2m)}+1$, wobei wir (5) im ersten Fall bis zur Ungleichung (4) gezeigt haben.
Wir setzen jetzt $a := 1,494\cdot\frac{16}{15}$ und benutzen, dass $\frac{x}{\log x}$ für $x > e$ streng monoton wachsend ist (Ableitung!). Also:

$$\pi(2m+1) \leq a\cdot\frac{2m}{\log(2m)}+1 < a\cdot\frac{2m+1}{\log(2m+1)}+1$$
$$= a\cdot\frac{n}{\log n}+1 = \left(a+\frac{\log n}{n}\right)\cdot\frac{n}{\log n}.$$

Für $n > 2^{16}$ gilt:

$$\frac{\log n}{n} < \frac{\log 2^{16}}{2^{16}} = \frac{16\log 2}{2^{16}} < \frac{16}{60000} < 0,001 < 0,001\cdot\frac{16}{15},$$

und damit

$$a+\frac{\log n}{n} < 1,494\cdot\frac{16}{15}+0,001\frac{16}{15} < 1,5\cdot\frac{16}{15} = \frac{8}{5}.$$

Deshalb gilt auch für ungerade $n$:

$$\pi(n) < \frac{8}{5}\frac{n}{\log n}. \qquad \square$$

Für eine Abschätzung von $\pi(x)$ nach unten brauchen wir einige Vorbereitungen:

**3.12 Lemma** *(Gauß): Für $p \in \mathbb{P}$ und $n \in \mathbb{N}_1$ gilt:*

$$v_p(n!) = \sum_{\nu=1}^{\infty} \left[\frac{n}{p^\nu}\right] = \sum_{\nu=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^\nu}\right].$$

**Beweis:** Die 2. Gleichung gilt wegen folgender Äquivalenzen:

$$\nu > \frac{\log n}{\log p} \iff p^\nu > n \iff \frac{n}{p^\nu} < 1 \iff \left[\frac{n}{p^\nu}\right] = 0.$$

Nun zur 1. Gleichung:
Es ist $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, also $v_p(n!) = \sum\limits_{k=1}^{n} v_p(k)$.
Wir machen folgende anschauliche Betrachtung:
In $n$ Schubladen mögen Kugeln liegen, und zwar $m_k$ Kugeln in der $k$–ten Schublade. Die Gesamtzahl der Kugeln $\sum\limits_{k=1}^{n} m_k$ kann man auch folgendermaßen bestimmen: Sei $a_\nu$ die Anzahl der Schubladen mit mindestens $\nu$ Kugeln. Dann ist

$$(1) \qquad \sum_{k=1}^{n} m_k = \sum_{\nu=1}^{\infty} a_\nu.$$

Denn für jedes $k$ liefert die $k$–te Schublade einen Beitrag von 1 zu jeder der $m_k$ Zahlen $a_1, a_2, \dots, a_{m_k}$. Z.B. betrachte man folgendes Bild mit 4 Schubladen:

Abb. 4

Die $m_k$ sind die Anzahlen der Kugeln in den Spalten, die $a_\nu$ die Anzahlen in den Zeilen des Schemas.

Man kann die Aussage (1) auch leicht mit Induktion nach $n$ beweisen:

Für $n = 1$ ist $a_\nu = \begin{cases} 1 & \text{für} \quad 1 \le \nu \le m_1 \\ 0 & \text{für} \quad \nu > m_1 \end{cases}$ .

Wenn man zu $n$ Schubladen, für die (1) schon gezeigt ist, eine $(n+1)$–te hinzufügt, kommt links der Summand $m_{n+1}$ hinzu, während rechts die Summanden $a_1, \dots, a_{m_{n+1}}$ um 1 größer werden.

Was bedeutet dies für unser Lemma? Wir legen für $k = 1, \dots, n$ in die $k$–te Schublade $v_p(k)$ Kugeln. Dann ist $a_\nu$ die Anzahl der $k \in \{1, \dots, n\}$ mit $\nu \le v_p(k)$, d.h. $p^\nu | k$. Von diesen $k$ gibt es $\left[\frac{n}{p^\nu}\right]$ Stück, nämlich $1 \cdot p^\nu, 2 \cdot p^\nu, \dots, r \cdot p^\nu$, wobei $r$ die größte natürliche Zahl mit $r \cdot p^\nu \le n$ ist, also $r = \left[\frac{n}{p^\nu}\right]$ gilt. Aus

(1) erhält man somit

$$\sum_{k=1}^{n} v_p(k) = \sum_{\nu=1}^{\infty} \left[\frac{n}{p^\nu}\right]. \qquad \square$$

**Korollar: 3.13** *Für $k, n \in \mathbb{N}, 0 \leq k \leq n$ gilt:*

$$v_p \begin{pmatrix} n \\ k \end{pmatrix} = \sum_{\nu=1}^{\left[\frac{\log n}{\log p}\right]} \left( \left[\frac{n}{p^\nu}\right] - \left[\frac{k}{p^\nu}\right] - \left[\frac{n-k}{p^\nu}\right] \right).$$

**Beweis:** Es ist $\begin{pmatrix} n \\ k \end{pmatrix} = \dfrac{n!}{k!(n-k)!}$, also

$$v_p \left( \begin{pmatrix} n \\ k \end{pmatrix} \right) = v_p(n!) - v_p(k!) - v_p\left((n-k)!\right),$$

ferner

$$\left[\frac{n}{p^\nu}\right] = 0 \text{ für } p^\nu > n, \text{ d.h. } \nu > \frac{\log n}{\log p}. \qquad \square$$

**3.14 Hilfsbemerkung:** *Seien $a, b \in \mathbb{R}$. Dann ist $[a+b] - [a] - [b] \in \{0, 1\}$. Insbesondere ist jeder Summand auf der rechten Seite von 3.13 entweder $0$ oder $1$; folglich gilt*

$$v_p \begin{pmatrix} n \\ k \end{pmatrix} \leq \left[\frac{\log n}{\log p}\right] \leq \frac{\log n}{\log p}.$$

**Beweis:** Seien $a = m + \sigma$, $b = n + \rho$ mit $m, n \in \mathbb{Z}$, $\sigma, \rho \in [0, 1[$. Dann ist $[a] = m, [b] = n$ und

$$[a+b] = \begin{cases} m+n+1 & \text{falls } \sigma + \rho \geq 1 \\ m+n & \text{falls } \sigma + \rho < 1. \end{cases} \qquad \square$$

**Korollar: 3.15** *Für $0 \leq k \leq n$ gilt*

*a)* $v_p \left( \begin{pmatrix} n \\ k \end{pmatrix} \right) \leq \dfrac{\log n}{\log p}$, *somit* *b)* $p^{v_p(\binom{n}{k})} \leq n$ *und deshalb*

*c)* $\displaystyle \binom{n}{k} = \prod_{p \leq n} p^{v_p(\binom{n}{k})} \leq n^{\pi(n)}.$

**Beweis:** a) folgt sofort aus 3.13, 3.14.
b) folgt aus a).
c) folgt aus b), wenn man bedenkt, dass kein Primfaktor von $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ größer als $n$ sein kann. □

**3.16 Satz** *(Čebyšev): Für* $n \in \mathbb{N}_3$ *ist*

$$\pi(n) > \frac{2}{3} \frac{n}{\log n}.$$

**Beweis:** Aus der in 3.15 gezeigten Abschätzung

$$\binom{n}{k} \leq n^{\pi(n)}$$

und $\binom{n}{0} = \binom{n}{n} = 1$ erhalten wir

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n-1) \cdot n^{\pi(n)} + 2 < n \cdot n^{\pi(n)}.$$

Also $2^n < n^{\pi(n)+1}$.
Durch Logarithmieren folgt:

$$n \log 2 \leq (\pi(n) + 1) \log n, \text{ somit}$$

$$\pi(n) \geq \log 2 \frac{n}{\log n} - 1.$$

Da $\log 2 \geq 0,693 > \frac{2}{3}$ und $\lim\limits_{n \to \infty} \frac{n}{\log n} = \infty$ ist, folgt $\pi(n) \geq \frac{2}{3} \frac{n}{\log n}$ für große $n$. Man rechnet nach, dass dies für $n > 250$ gilt. Für $n \leq 250$ kann man den Satz anhand von Primzahltabellen nachprüfen. □

**3.17** Ohne Beweis zitieren wir den sogenannten

$$\text{Primzahlsatz:} \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

(Zum Beweis siehe [*Korevaar*].)
Auch dieser Primzahlsatz ist keineswegs das beste, was man über das Wachstum der Funktion $\pi$ weiß. Siehe [*Prachar*]. Die Einleitung dieses Buches enthält einen lesenswerten Abriss der Geschichte der Primzahltheorie. Vgl. auch [*Ischebeck*].

Der Primzahlsatz besagt:
Zu jedem $\varepsilon > 0$ gibt es eine Schranke $s$, so dass
$(1-\varepsilon)\dfrac{n}{\log n} < \pi(n) < (1+\varepsilon)\dfrac{n}{\log n}$ für $n \geq s$ gilt.

**3.18** Wir wollen vergleichen, was man aus unseren Sätzen 3.11 und 3.16 folgern kann, mit dem, was aus dem Primzahlsatz folgen würde. Deshalb betrachten wir folgende Hypothese:

$H(c_1, c_2, s)$: Es gilt

$$c_1 \cdot \frac{x}{\log x} < \pi(x) < c_2 \cdot \frac{x}{\log x} \quad \text{für alle } x \geq s.$$

(Dabei sind $c_1, c_2, s \in \mathbb{R}$ vorgegeben mit $0 < c_1 \leq 1 < c_2 \leq \frac{8}{5}$.)
Man beachte dabei folgendes:
Wegen $\pi(x) = \pi([x])$ und $\dfrac{[x]}{\log[x]} < \dfrac{x}{\log x}$ für $x \geq 3$ folgt aus 3.11 sofort die Ungleichung

$$\pi(x) < \frac{8}{5}\frac{x}{\log x} \quad \text{für } \textit{reelle } x \geq 3.$$

Da andererseits die Differenz $\dfrac{x}{\log x} - \dfrac{[x]}{\log[x]} < \dfrac{1}{\log[x]}$, also für große $x$ ziemlich klein wird, ist es möglich, die Ungleichung

$$\pi(x) > \frac{2}{3}\frac{x}{\log x}$$

für alle *reellen* $x \geq 3$ zu zeigen. Wir wollen dies hier nicht ausführen.

**Satz: 3.19** *Sei mit $p_n$ die $n$–te Primzahl bezeichnet. Unter Voraussetzung der Hypothese $H(c_1, c_2, s)$ gilt:*

*a) Es ist $p_n > \frac{1}{c_2} n \cdot \log n$ für $p_n \geq s$.*

*b) Zu jedem $\varepsilon$ mit $0 < \varepsilon < 1$ gibt es ein $s_1 \in \mathbb{N}$ mit $p_n < \frac{1}{(1-\varepsilon)c_1} n \log n$ für $n > s_1$.*

**Beweis:** a) Es ist

$$\pi(x) < c_2 \frac{x}{\log x} \tag{1}$$

für $x > s$.
Aus $\pi(x) < x$ folgt

$$\log \pi(x) < \log x \tag{2}$$

Durch Multiplikation der beiden Ungleichungen erhält man

$$\pi(x) \log \pi(x) < c_2 x.$$

Setze nun $x = p_n$; dann folgt die Behauptung, da $\pi(p_n) = n$ gilt.

b) Analog zu a) erhält man aus

$$\pi(x) > c_1 \frac{x}{\log x} \tag{3}$$

$$\begin{aligned} \log \pi(x) &> \log x + (\log c_1 - \log \log x) \\ &= \log x \left(1 - \frac{\log c_1^{-1} + \log \log x}{\log x}\right). \end{aligned}$$

Es ist $\log c_1^{-1} \geq 0$, da $c_1 \leq 1$ und $\log\log x \geq 0$ für $x \geq e$, ferner sind $\dfrac{\log c_1^{-1}}{\log x}$ und $\dfrac{\log\log x}{\log x}$ für $x > 1$ bzw. $x \geq e$ monoton fallend mit dem Limes 0 für $x \longrightarrow \infty$. Also gibt es ein $s'$ mit

$$\log \pi(x) > (1-\varepsilon) \cdot \log x \ \text{ für } \ x \geq s'. \tag{4}$$

Wie oben erhält man durch Multiplikation der Ungleichungen (3), (4)

$$\pi(x) \log \pi(x) > c_1(1-\varepsilon)x$$

für $x \geq \operatorname{Max}\{s, s'\}$.
Es folgt durch Einsetzen $x = p_n$:

$$p_n < \frac{1}{c_1(1-\varepsilon)} \cdot n \log n. \qquad \square$$

**Korollar: 3.20** *Aus dem Primzahlsatz folgt* $\lim\limits_{n\to\infty} \dfrac{p_n}{n \cdot \log n} = 1.$

**Satz: 3.21** *Unter der Voraussetzung der Hypothese $H(c_1, c_2, s)$ gilt:*
*Für jedes $a > \dfrac{c_2}{c_1}$ ist*

$$\lim_{x\to\infty} \#(\mathbb{P} \cap \,]x, ax]) = \infty.$$

*Insbesondere gibt es eine Schranke $s_1 \in \mathbb{R}$, so dass für jedes $x \geq s_1$ in dem Intervall $]x, ax]$ mindestens eine Primzahl liegt.*

**Beweis:** Für $x \geq s$ haben wir

$$\#(\mathbb{P} \cap \,]x, ax]) = \pi(ax) - \pi(x) > c_1 \cdot \frac{ax}{\log(ax)} - c_2 \frac{x}{\log x}$$

$$= c_1 \frac{ax}{\log x + \log a} - c_2 \frac{x}{\log x} = \frac{x}{\log x} \left( \frac{c_1 a}{1 + \log(a)/\log(x)} - c_2 \right).$$

Für die Faktoren des letzten Ausdrucks gilt:

$$\lim_{x\to\infty} \frac{x}{\log x} = \infty$$

und

$$\lim_{x\to\infty} \left( \frac{c_1 a}{1 - \log(a)/\log(x)} - c_2 \right) = c_1 a - c_2 > 0,$$

da $a > c_2/c_1$ ist. Daraus ergibt sich die Behauptung. $\square$

**Korollar: 3.22** *Unter Voraussetzung des Primzahlsatzes gilt: Für jedes* $\varepsilon > 0$ *ist* $\lim\limits_{x\to\infty} \#(\mathbb{P}\cap\,]x,(1+\varepsilon)x]) = \infty$. *Insbesondere liegt für genügend große* $x$ *im Intervall* $]x,(1+\varepsilon)x]$ *mindestens eine Primzahl.*

**Beweis:** Der Primzahlsatz besagt, dass die Hypothese $H(c_1, c_2, s)$ für $c_1, c_2$ gilt, die – auf Kosten der Schranke $s$ – beliebig nahe bei 1 liegen, so dass also $\dfrac{c_2}{c_1} < 1 + \varepsilon$ angenommen werden kann. Die Behauptung folgt nun aus 3.21 mit $a = 1 + \varepsilon$. $\square$

**Korollar: 3.23** *Ohne die Voraussetzung hier nicht bewiesener Sätze gilt:*

$$\lim_{n\to\infty} \#(\mathbb{P}\cap\,]n, \frac{5}{2}n]) = \infty.$$

**Beweis:** Wir haben die Hypothese $H(c_1, c_2, s)$ mit $c_1 = \frac{2}{3}, c_2 = \frac{8}{5}$ bewiesen. Wende 3.21 mit $a = \dfrac{5}{2} > \dfrac{24}{10} = \dfrac{c_2}{c_1}$ an. $\square$

**Bemerkung: 3.24** Die Schranke $s_1$ aus Satz 3.21 ergibt sich hier als $e^{24} \approx 2,65 \cdot 10^{10}$. D.h. wir haben hier nur für $x > e^{24}$ gezeigt, dass im Intervall $]x, \frac{5}{2}x]$ mindestens eine Primzahl liegt. In Wahrheit gilt dies jedoch für alle $x \in \mathbb{N}_1$. Das von *Čebyšev* 1852 bewiesene „Bertrandsche Postulat" besagt sogar: Im Intervall $]n, 2n]$ liegt für *jedes* $n \in \mathbb{N}_1$ eine Primzahl. Siehe A8.

AUFGABEN UND HINWEISE

**1)** a) Es gelte die Hypothese $H(c_1, c_2, s)$. Sei $a$ reell mit $0 < a < \frac{1}{c_2}$.
Zeigen Sie:
Für unendlich viele $n$ liegt im Intervall $]n, n + a \cdot \log n]$ keine Primzahl. (Unter Voraussetzung des Primzahlsatzes gilt die Behauptung also für $0 < a < 1$.)
Folgender Beweisweg wird vorgeschlagen:

b) Definition: Sei $k \in \mathbb{N}$, $f : \mathbb{N}_k \longrightarrow \mathbb{R}$ eine Funktion. Definiere $\delta f : \mathbb{N}_k \longrightarrow \mathbb{R}$ durch $(\delta f)(n) = f(n+1) - f(n)$.

c) Zeigen Sie: $\delta(af + bg) = a\delta f + b\delta g$ für $a, b \in \mathbb{R}$ und $f, g : \mathbb{N}_k \longrightarrow \mathbb{R}$.

d) Es gelte $(\delta f)(n) \leq (\delta g)(n)$ für $n \geq n_0$. Zeigen Sie:
$f(n) \leq g(n) + (f(n_0) - g(n_0))$ für $n \geq n_0$.

e) Sei $0 < b < 1$ und es gelte

(i) $\lim_{n\to\infty} g(n) = \infty$.

(ii) $(\delta f)(n) \leq b(\delta g)(n)$ für $n \geq n_0$.

Zeigen Sie: Es gibt ein $n_1 \geq n_0$ mit $f(n) < g(n)$ für $n \geq n_1$.

f) Angenommen, die Behauptung unter a) sei falsch. Zeigen Sie:
Dann gibt es ein $n_2$ mit

$$p_{n+1} - p_n < a \log n + a \log(\log n) + a \log \frac{1}{(1-a)c_1}$$

für $n > n_2$ (3.19).

g) Man wähle $b \in \mathbb{R}$ mit $a < b < \frac{1}{c_2}$, setze $f(n) = p_n,\ g(n) = \frac{1}{c_2} n \log n$.
Zeigen Sie:
$(\delta f)(n) < b(\delta g)(n)$ für große $n$, falls die Behauptung unter a) falsch ist. Daraus ergibt sich mit e) ein Widerspruch zu 3.19 a).

**2)** Gegeben seien $k$ (nicht notwendig verschiedene) Ziffern
$a_1, \ldots, a_k \in \{0, 1, \ldots, 9\}$. Zeigen Sie:
Es gibt eine Schranke $s \in \mathbb{N}$, $(s \geq k)$, so dass für jede natürliche Zahl $n \geq s$ eine (im Dezimalsystem) $n$–stellige Primzahl existiert, deren erste $k$

Ziffern $a_1, \ldots, a_k$ sind. Dabei darf der Primzahlsatz, also auch 3.22 als wahr unterstellt werden.

**3)** a) Schätzen sie $\displaystyle\sum_{k=1}^{n} \frac{1}{p_k}$ nach oben und unten ab.

b) Schätzen Sie $\displaystyle\sum_{p \leq x} \frac{1}{p}$ nach oben ab.

**4)** a) Zeigen Sie: $\displaystyle\binom{2n+1}{n} < 4^n$ für $n \in \mathbb{N}_1$.

b) Folgern Sie: $\displaystyle\prod_{p \leq n} p < 4^n$ für $n \in \mathbb{N}_1$.

(Induktion nach $n$, Induktionsanfang $n \leq 2$, man unterscheide beim Induktionsschritt, ob $n$ gerade oder ungerade ist.)

**5)** Zeigen Sie (mit Induktion):

$$\binom{2n}{n} > \frac{4^n}{2\sqrt{n}} \quad \text{für} \quad n \in \mathbb{N}_2.$$

(Es gilt auch $\displaystyle\binom{2n}{n} < \frac{4^n}{\sqrt{2n}}$. Siehe [*Chandrasekharan*] VII §3.)

**6)** Sei $p \in \mathbb{P},\ n \in \mathbb{N}_1$.

a) Zeigen Sie: $v_p\left(\binom{2n}{n}\right)$ ist gleich der Anzahl der ungeraden Zahlen in der Folge $\left[\frac{2n}{p}\right], \left[\frac{2n}{p^2}\right], \left[\frac{2n}{p^3}\right], \ldots$ (in der ja fast alle Glieder Null sind). (3.13,3.14)

b) Folgern Sie: Falls $\frac{2}{3}n < p \leq n$ und $n > 2$ ist, gilt $p \nmid \binom{2n}{n}$.

**7)** a) Zeigen Sie für $p \in \mathbb{P},\ n \in \mathbb{N}_1$:

$p \geq \sqrt{2n} \Longrightarrow v_p\binom{2n}{n} \leq 1;$

b) Wir wissen aus dem Beweis von 3.10 folgendes:
$n < p \leq 2n \Longrightarrow v_p\binom{2n}{n} = 1.$

**8)** Beweisen Sie das sogenannte Bertrandsche Postulat:
*Für jedes $n \in \mathbb{N}_1$ liegt im Intervall $]n, 2n]$ immer eine Primzahl.*

Beweisweg: a) Für $n \leq 72$ prüft man es direkt nach. Ab jetzt setze man $n > 72$ voraus.

b) Schreibe $\binom{2n}{n} = R_n \cdot Q_n$ mit $Q_n,\ R_n \in \mathbb{N}$, wobei alle Primfaktoren von $R_n$ kleiner oder gleich $n$ und die von $Q_n$ größer als $n$ sind. Es genügt, $Q_n > 1$ zu zeigen. Da nach A5 die Zahl $\binom{2n}{n}$ nach unten abgeschätzt ist, müssen Sie nur $R_n$ hinreichend gut nach oben abschätzen.

c) Schreibe $e_p = v_p\binom{2n}{n}$. Dann ist $R_n = \prod_{p \leq n} p^{e_p}$. Benutzen Sie:

(1) $\frac{2}{3}n < p \leq n \Longrightarrow e_p = 0$ (A6 b));

(2) $\sqrt{2n} \le p \left(\le \frac{2}{3}n\right) \Longrightarrow e_p \le 1$ (A7 a))
(beachte $\sqrt{2n} < \frac{2}{3}n$ für $n \ge 6$);

(3) $1 < p \left(< \sqrt{2n}\right) \Longrightarrow p^{e_p} \le 2n$ (3.15 b));

(4) $\prod\limits_{p \le \frac{2}{3}n} p < 4^{\frac{2}{3}n}$ (A4 b));

(5) $\pi(m) \le \dfrac{m}{2}$ für $m \ge 8$.

Folgern Sie:

$$R_n = \prod_{p \le \frac{2}{3}n} p^{e_p} \le \prod_{p \le \frac{2}{3}n} p \cdot \prod_{p < \sqrt{2n}} p^{e_p} < 4^{\frac{2}{3}n} \cdot 2n^{\pi(\sqrt{2n})} \le 4^{\frac{2}{3}n} \cdot (2n)^{\sqrt{\frac{n}{2}}}.$$

Man erhält $Q_n = \dbinom{2n}{n} \cdot R_n^{-1} > \dfrac{4^n}{2\sqrt{n}} \left(4^{\frac{2}{3}n}(2n)^{\sqrt{\frac{n}{2}}}\right)^{-1}$. Jetzt ist es eine Sache der elementaren Analysis, zu zeigen, dass letzter Ausdruck für $n > 72$ nicht kleiner als 1 ist, ja sogar mit $n$ gegen $\infty$ geht. (Setze $x := \sqrt{n}$.)

**9)** Aus dem Bertrandschen Postulat lässt sich leicht folgern:
$m!$ ist für $m \in \mathbb{N}_2$ kein Quadrat und auch keine höhere Potenz.

Dass $m!$ kein Quadrat ist, kann man allerdings auch direkt beweisen, indem man nur einen Teil der o.a. Argumente für den Beweis des Bertrandschen Postulats benutzt:

Setze $n = \left[\dfrac{m}{2}\right]$; dann ist $\dfrac{m!}{(n!)^2} = \left(\begin{array}{c} m \\ n \end{array}\right)$ oder $= \left(\begin{array}{c} m \\ n \end{array}\right) \cdot (n+1)$ ganz. Und es genügt zu zeigen, dass $\dfrac{m!}{(n!)^2}$ kein Quadrat ist. Es ist leicht möglich, nachzuweisen, dass $\left[\dfrac{m}{p^\nu}\right] - 2\left[\dfrac{n}{p^\nu}\right] \in \{0,1\}$ auch für ungerades $m$ gilt. Daraus folgt wie oben $p^{e_p} \le m$ und $e_p \le 1$ für $p > \sqrt{m}$, wo $e_p := v_p\left(\dfrac{m!}{n!^2}\right)$.
Es genügt dann zu zeigen: Es gibt eine Primzahl in $]\sqrt{m},\ m]$.

**10)** Auf wie viele Nullen endet 99! in der Dezimalzahldarstellung?

**11)** Bestimmen Sie die Primfaktorzerlegung von $\binom{300}{150}$.

**12)** Zeigen Sie: Für $p \in \mathbb{P}$, $n \in \mathbb{N}_1$ ist $v_p(n!) < \dfrac{n}{p-1}$. Insbesondere gilt $2^n \nmid n!$ für $n \in \mathbb{N}_1$.

# § 4

# Restklassen, Kongruenz, Restklassenringe von $\mathbb{Z}$

Der Inhalt dieses Paragrafen ist von grundlegender Wichtigkeit.
Lesen Sie ihn notfalls zweimal!

**Definition: 4.1** *Seien $a, m \in \mathbb{Z}$. Die Restklasse von $a$ modulo $m$ ist die aus §0 bekannte Teilmenge $a + m\mathbb{Z}$ von $\mathbb{Z}$. Sie wird auch mit $(a \bmod m)$ bezeichnet. Zum Namen „Restklasse“ siehe 4.9 (vi).)*

**Beispiele: 4.2** a) $(a \bmod 0) = \{a\}$. Wenn hingegen $m \neq 0$ ist, ist $(a \bmod m)$ bekanntlich eine weder nach oben noch nach unten beschränkte Menge.
b) $(0 \bmod m) = m\mathbb{Z}$.
c) $(1 \bmod 2)$ ist die Menge aller ungeraden, $(0 \bmod 2)$ die Menge aller geraden Zahlen.
d) $(4 \bmod 10) = M_+ \cup M_-$, wobei $M_+$ die Menge der natürlichen Zahlen ist, deren letzte Ziffer im Dezimalsystem eine 4 ist, und $M_-$ die Menge der $n \in \mathbb{Z}$, für die $-n$ eine natürliche Zahl ist, deren letzte Ziffer eine 6 ist. $(4 \bmod 10) = \{\ldots - 16, -6, 4, 14, 24, \ldots\}$
e) $(a \bmod 1) = \mathbb{Z}$ für alle $a \in \mathbb{Z}$.

**Satz: 4.3** *Sei* $m \in \mathbb{Z}$. *Dann gilt:*
*a) Für jedes* $a \in \mathbb{Z}$ *ist* $a \in (a \bmod m)$.
*b) Ist* $(a \bmod m) \cap (b \bmod m) \neq \emptyset$, *so ist* $(a \bmod m) = (b \bmod m)$.
*Zwei verschiedene Restklassen modulo m sind also disjunkt.*

**Beweis:** a) $\quad a = a + m \cdot 0$.

b) Ist $c \in (a \bmod m) \cap (b \bmod m)$, so $c = a + mx = b + my$ mit gewissen $x, y \in \mathbb{Z}$. Man erhält $a = b + m(y - x)$, also
$a + mz = b + m(y - x + z) \in (b \bmod m)$, mithin
$(a \bmod m) \subset (b \bmod m)$. Aus Symmetriegründen hat man auch die Inklusion $(b \bmod m) \subset (a \bmod m)$, also $(a \bmod m) = (b \bmod m)$. $\square$

**4.4** Obigen Satz kann man auch wie folgt aussprechen: Zu gegebenem $m \in \mathbb{Z}$ liegt jede Zahl $a \in \mathbb{Z}$ in genau einer der Restklassen modulo $m$. D.h. $\mathbb{Z}$ ist die disjunkte Vereinigung der Restklassen modulo (einem vorgegebenen) $m$.

**4.5** In dem relativ uninteressanten Fall $m = 0$ sind die Restklassen modulo $m$ die 1–elementigen Teilmengen von $\mathbb{Z}$. Andernfalls gilt der

**Satz:** *Wenn* $m \in \mathbb{Z} - \{0\}$ *ist, gibt es genau* $|m|$ *Restklassen modulo* $m$, *nämlich* $(0 \bmod m), (1 \bmod m), \ldots, \ (|m| - 1 \bmod m)$.

**Beweis:** Eine Restklasse $(a \bmod m)$ hat nach 0.18 genau ein Element $r$ mit dem Intervall $[0, |m| - 1]$ gemein. Dann ist
$r \in (r + m\mathbb{Z}) \cap (a + m\mathbb{Z})$, also $(r + m\mathbb{Z}) = (a + m\mathbb{Z})$ wegen Satz 4.3.
Wenn $(r \bmod m) = (r' \bmod m)$ für $r, r' \in [0, |m| - 1]$ ist, so hat
$(r \bmod m)$ die Elemente $r, r'$ mit dem Intervall $[0, |m| - 1]$ gemein. Wegen der Eindeutigkeitsaussage aus 0.18 ist $r = r'$. $\square$

**Definition: 4.6** *Für* $m \in \mathbb{Z}$ *bezeichne* $\mathbb{Z}/m$ *(sprich:* $\mathbb{Z}$ *modulo* $m$*) die Menge aller Restklassen modulo* $m$. *(Andere Bezeichnungen:* $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/(m)$, $\mathbb{Z}_m$.*) (Offenbar ist* $\mathbb{Z}/m = \mathbb{Z}/(-m)$.*)*
*Wenn der sogenannte Modul* $m$ *fixiert ist, schreiben wir häufig*
$\overline{a} = (a \bmod m)$. *Wenn* $m \neq 0$ *ist, sollte man sich die Elemente von* $\mathbb{Z}/m$

*„kreisförmig angeordnet“ vorstellen, z.B. für* $m = 6$*:*

Abb.5

**Definition: 4.7** *Die Abbildung* $\kappa : \mathbb{Z} \longrightarrow \mathbb{Z}/m,\ a \longmapsto (a \bmod m)$ *heißt die kanonische Abbildung von* $\mathbb{Z}$ *nach* $\mathbb{Z}/m$*.*

**Bemerkung: 4.8** Offenbar ist $\kappa$ surjektiv. Da die „Faser“ $\kappa^{-1}(\overline{a}) := \{x \in \mathbb{Z} \mid \kappa(x) = \overline{a}\}$ gerade gleich der Restklasse $a + m\mathbb{Z}$ ist, ist $\kappa$ bijektiv, wenn $m = 0$, aber nicht injektiv, wenn $m \neq 0$ ist.

**Satz: 4.9** *Für* $a, b, m \in \mathbb{Z}$ *sind folgende Aussagen äquivalent:*

*(i)* $(a \bmod m) = (b \bmod m)$*, d.h.* $\kappa(a) = \kappa(b)$*;*

*(ii)* $a \in (b \bmod m)$*;*

*(iii)* $b \in (a \bmod m)$*;*

*(iv)* $(a \bmod m) \cap (b \bmod m) \neq \emptyset$*;*

*(v)* $a - b \in m\mathbb{Z}$*, d.h.* $m | a - b$*.*

*Wenn* $m \neq 0$ *ist, sind diese Aussagen äquivalent zu:*

*(vi) Aus* $a = mq_1 + r_1,\ b = mq_2 + r_2$ *mit* $0 \leq r_i < |m|$ *folgt* $r_1 = r_2$*.*

**Beweis:** „(i) $\Longrightarrow$ (ii)“: $a \in (a \bmod m) = (b \bmod m)$.
„(i) $\Longrightarrow$ (iii)“ geht analog.
„(ii) $\Longrightarrow$ (iv)“: Da $a \in (b \bmod m)$, ist $a \in (a \bmod m) \cap (b \bmod m)$.
„(iii) $\Longrightarrow$ (iv)“ geht analog.
„(iv) $\Longrightarrow$ (i)“ ist Satz 4.3 b).
Damit ist die Äquivalenz von (i) bis (iv) gezeigt.
„(ii) $\Longleftrightarrow$ (v)“: $a \in (b \bmod m) \iff a = b + mz$ für ein $z \iff$ $a - b = mz$ für ein $z \iff a - b \in m\mathbb{Z}$.
„(i) $\Longrightarrow$ (vi)“: $r_1 = a + m(-q_1)$ und $r_2 = a + m(-q_2)$ sind Elemente der Restklasse $a + m\mathbb{Z}$, die ins Intervall $[0, |m| - 1]$ fallen. Wegen der Eindeutigkeitsaussage von Satz 0.18 ist $r_1 = r_2$.
„(vi) $\Longrightarrow$ (v)“: $a - b = m(q_1 - q_2) + r_1 - r_2 = m(q_1 - q_2) \in m\mathbb{Z}$, da $r_1 = r_2$.
□

**Definition: 4.10** *Man sagt, „a ist kongruent zu b modulo m“, und schreibt $a \equiv b$ (mod m), oder $a \equiv b$ $(m)$, wenn $a, b, m$ die äquivalenten Aussagen von 4.9 erfüllen.*

**Feststellung: 4.11** *Die Kongruenzrelation genügt folgenden Gesetzen:*
*a)* $a \equiv a$ *(mod m) für alle* $a \in \mathbb{Z}$ *(Reflexivität);*
*b)* $a \equiv b\ (m) \Longrightarrow b \equiv a\ (m)$ *(Symmetrie);*
*c)* $a \equiv b\ (m),\ b \equiv c\ (m) \Longrightarrow a \equiv c\ (m)$ *(Transitivität);*
*d)* $a \equiv b\ (m) \iff ad \equiv bd\ (md)$ *für* $d \neq 0$.

a), b), c) folgen aus 4.9 (i), d) aus 4.9 (v). □

**4.12** Der Grund dafür, dass man $\mathbb{Z}/m$ betrachtet, ist der, dass man auf dieser Menge in kanonischer Weise eine Addition und eine Multiplikation erklären kann. Dies beruht auf folgendem

**Lemma:** *Wenn* $a \equiv a'(m)$ *und* $b \equiv b'(m)$ *gilt, so ist auch* $a + b \equiv a' + b'\ (m)$ *und* $ab \equiv a'b'\ (m)$.

**Beweis:** Nach Voraussetzung gilt: $m|a-a'$ und $m|b-b'$. Hieraus folgt erstens $m|a - a' + b - b' = a + b - (a' + b')$ und zweitens $m|(a - a')b$ sowie $m|a'(b - b')$, also $m|ab - a'b + a'b - a'b' = ab - a'b'$. □

(Für $m = 2$ erhält man solche Regeln wie: „ungerade + ungerade = gerade", „ungerade · ungerade = ungerade" etc., auf welche der Leser sicher schon zu Schulzeiten gestoßen ist.)

**4.13** Dieses Lemma erlaubt uns die

**Definition:** *Auf $\mathbb{Z}/m$ werden Addition und Multiplikation wie folgt definiert:*
$(a \bmod m) + (b \bmod m) := (a + b \bmod m)$,
$(a \bmod m) \cdot (b \bmod m) =: (ab \bmod m)$.

Aus Lemma 4.12 folgt, dass dies wirklich eine Definition ist. Denn es besagt ja, wenn $(a \bmod m) = (a' \bmod m)$ und
$(b \bmod m) = (b' \bmod m)$ ist, gilt: $(a + b \bmod m) = (a' + b' \bmod m)$ und $(ab \bmod m) = (a'b' \bmod m)$.

**4.14 Satz:** *Mit dieser Addition und dieser Multiplikation ist $\mathbb{Z}/m$ ein Ring.*

Der **Beweis** ist naheliegend: Mit der Bezeichnung $\overline{a} = (a \bmod m)$ gilt z.B. $\overline{a}+(\overline{b}+\overline{c}) = \overline{a}+\overline{(b+c)} = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)}+\overline{c} = (\overline{a}+\overline{b})+\overline{c}$.
Dabei gilt das 3. Gleichheitszeichen aufgrund der Assoziativität der Addition in $\mathbb{Z}$. Die anderen Gleichheitszeichen beruhen auf der Definition der Addition in $\mathbb{Z}/m$.
Auf analoge Weise werden die Assoziativität der Multiplikation, die Kommutativität von Addition und Multiplikation sowie die Distributivität auf die entsprechenden Gesetze in $\mathbb{Z}$ zurückgeführt.
Genauso sieht man schließlich, dass $\overline{0}$ das neutrale Element für die Addition, $\overline{1}$ dasselbe für die Multiplikation und $\overline{-a}$ das zu $\overline{a}$ additiv inverse Element ist. □

**Definition: 4.15** *Der Ring $\mathbb{Z}/m$ heißt auch der Restklassenring von $\mathbb{Z}$ nach $m$.*

**Bemerkungen: 4.16** Für $m = 0$ erhält man mit $\mathbb{Z}/0$ keinen wesentlich von $\mathbb{Z}$ verschiedenen Ring. ($\mathbb{Z}$ und $\mathbb{Z}/0$ sind zueinander „isomorf"; s. 5.6)

$\mathbb{Z}/1$ besteht aus genau einem Element, das sowohl das Null– wie das Einselement ist. $\mathbb{Z}/1$ ist der sogenannte Nullring.
Ist jedoch $m > 1$, so treten interessante und neue Fänomene auf. In $\mathbb{Z}/6$ zum Beispiel ist $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$, obwohl $\overline{2} \neq \overline{0} \neq \overline{3}$ ist. In $\mathbb{Z}/5$ hingegen gilt $\overline{2} \cdot \overline{3} = \overline{1}$, d.h. $\overline{2}$ und $\overline{3}$ sind zueinander (multiplikativ) invers. Da ferner $\overline{1}$ und $\overline{4} = \overline{-1}$ in $\mathbb{Z}/5$ invertierbar (bzgl. der Multiplikation) sind, sieht man, dass $\mathbb{Z}/5$ ein Körper ist.
Diese Fänomene werden im Anschluss an die folgenden Definitionen erschöpfend studiert.

**Definitionen: 4.17** *Sei $A$ ein Ring.*
*a) Ein Element $a \in A$ heißt ein Nullteiler, wenn es ein Element $b \neq 0$ mit $ab = 0$ gibt. (Jedes Element teilt die Null. Nullteiler sind solche, die dies auf nichttriviale Weise tun.) 0 ist ein Nullteiler, wenn $A$ mehr als ein Element hat.*
*b) Ein Element aus $A$, welches kein Nullteiler ist, heißt ein Nichtnullteiler oder regulär.*
*c) $A$ heißt nullteilerfrei, wenn in ihm $1 \neq 0$ ist (d.h. $A$ aus mehr als einem Element besteht (Beweis?)) und in ihm kein Element außer 0 ein Nullteiler ist. Ein nullteilerfreier Ring heißt auch integer oder ein Integritätsring.*
*d) Ein Element $a \in A$ heißt Einheit oder invertierbar, wenn es invertierbar bzgl. der Multiplikation ist, d.h. ein $b \in A$ mit $ab = 1$ existiert.*

**4.18** Zum Verständnis des folgenden Satzes machen wir die Bemerkungen:
a) $\mathrm{ggT}(a, m) = \mathrm{ggT}(a + mz, m)$ für alle $z \in \mathbb{Z}$.
b) Eine Einheit eines Ringes ist kein Nullteiler. Denn aus $ab = 0$ und $ca = 1$ folgt $b = 1 \cdot b = cab = c \cdot 0 = 0$.

**Satz: 4.19** *Sei $m \in \mathbb{N}_2$, $a \in \mathbb{Z}$ und $d = ggT(a, m)$. Dann gilt für die Restklasse $\overline{a} = (a \bmod m)$:*
*a) Wenn $d = 1$ ist, ist $\overline{a}$ eine Einheit in $\mathbb{Z}/m$.*
*b) Wenn $d > 1$ ist, ist $\overline{a}$ ein Nullteiler in $\mathbb{Z}/m$.*

(Beachte, dass die Elemente aus $\mathbb{Z} - \{0, 1, -1\}$ weder Einheiten noch Nullteiler in $\mathbb{Z}$ sind.)

**Beweis:** a) Sei $1 = aa' + mm'$. Dann ist $1 \equiv aa' \pmod{m}$, also $\overline{1} = \overline{a}\,\overline{a'}$ in $\mathbb{Z}/m$.
b) Wenn $d > 1$ ist, ist $1 \leq \frac{m}{d} < m$, folglich $m$ kein Teiler der ganzen Zahl $\frac{m}{d}$. D.h. $\frac{m}{d} \not\equiv 0 \pmod{m}$. Es ist aber $a \cdot \frac{m}{d} = \frac{a}{d} \cdot m \in m\mathbb{Z}$, da $\frac{a}{d} \in \mathbb{Z}$ ist. D.h. $a \cdot \frac{m}{d} \equiv 0 \pmod{m}$, mithin $(a \bmod m) \cdot (\frac{m}{d} \bmod m) = \overline{0}$. □

**Bemerkungen: 4.20** a) Aus dem Beweis von 4.19 a) und aus 1.18 ergibt sich, dass man die zu $\overline{a}$ inverse Restklasse – falls sie existiert – mit Hilfe des euklidischen Algorithmus berechnen kann.
b) In jedem endlichen Ring ist jedes Element entweder ein Nullteiler oder eine Einheit. Siehe hierzu A12.

**Korollar: 4.21** *Für $m \in \mathbb{N}_2$ sind folgende Aussagen äquivalent:*

*(i)* *$\mathbb{Z}/m$ ist nullteilerfrei;*

*(ii)* *$\mathbb{Z}/m$ ist ein Körper;*

*(iii)* *$m$ ist eine Primzahl;*

*(iv)* *die Zahlen $1, 2, \ldots, m-1$ sind zu $m$ teilerfremd.*

**Beweis:** Jede der drei Ausagen (i), (ii), (iii) ist offenbar äquivalent zu (iv); (i) und (ii) wegen 4.5 und 4.19. □

**Bemerkung: 4.22** Die Einheiten eines Ringes bilden bzgl. der Multiplikation eine Gruppe.

**Definitionen: 4.23** *a) Die Gruppe der Einheiten eines Ringes $A$ wird mit $A^*$ bezeichnet und Einheitengruppe von $A$ genannt.*
*b) Die Anzahl der Elemente einer Gruppe $G$ wird auch ihre Ordnung genannt.*

*c) Für $m \in \mathbb{N}_1$ definieren wir $\varphi(m) := \#(\mathbb{Z}/m)^*$, d.h. $\varphi(m)$ ist die Ordnung der Einheitengruppe von $\mathbb{Z}/m$. $\varphi$ heißt Eulersche $\varphi$–Funktion.*
*Der Buchstabe $\varphi$ soll in diesem Buch nur als Bezeichnung dieser Funktion benutzt werden.*
*d) Die Restklassen $(a \bmod m)$ mit $ggT(a, m) = 1$ werden auch die primen (oder teilerfremden) Restklassen modulo $m$ genannt.*

**Bemerkungen: 4.24** a) $\varphi(m)$ ist die Anzahl derjenigen $j \in \mathbb{N}_1$ mit $j \leq m$, die zu $m$ teilerfremd sind.

b) Es ergibt sich z.B. für kleine $m$ die Tabelle

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $\varphi(m)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 |

c) Für jede Primzahl $p$ ist $\varphi(p) = p - 1$.

d) Für $p \in \mathbb{P}$ und $n \in \mathbb{N}_1$ ist $\varphi(p^n) = (p-1)p^{n-1}$. Denn die ganzen Zahlen, die zu $p^n$ nicht teilerfremd sind, sind genau die Vielfachen von $p$. Von diesen gibt es in der Menge $\{1, 2, \ldots, p^n\}$ genau $p^{n-1}$, nämlich $1 \cdot p,\ 2 \cdot p, \ldots, p^{n-1} \cdot p$. Also ist $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$.

e) Später werden wir sehen, wie man $\varphi(m)$ aus der Primfaktorzerlegung von $m$ berechnen kann.

**Bemerkungen: 4.25** a) Die Elemente von $\mathbb{Z}/m$ sind nach unserer Konstruktion gewisse Teilmengen von $\mathbb{Z}$, eben die Restklassen modulo $m$. Man kann $\mathbb{Z}/m$ auch anders auffassen: $\mathbb{Z}/m$ ist die Menge $\mathbb{Z}$ mit einer anderen Gleichheit, nämlich der Kongruenz modulo $m$. Das soll heißen: Eine Aussage $\mathcal{A}(x)$ über Elemente $x \in \mathbb{Z}/m$ ist eine Aussage über ganze Zahlen $x$, die sich nicht ändert, wenn man in ihr $x$ durch eine modulo $m$ kongruente Zahl $x'$ ersetzt. (D.h. aus $x \equiv x' \pmod{m}$ soll die Äquivalenz

$$\mathcal{A}(x) \iff \mathcal{A}(x')$$

folgen.)(Vgl. [*Lorenzen* II]I.2.)

b) Die Begriffe Kongruenz und Restklassenring wendet man wie folgt an. Aus der Gleichheit folgt die Kongruenz – modulo beliebigem $m$, d.h. die

Gleichheit in $\mathbb{Z}/m$. Ferner ist die kanonische Abbildung

$$\kappa : \mathbb{Z} \longrightarrow \mathbb{Z}/m$$

mit Addition und Multiplikation verträglich.
Wenn man also gezeigt hat, dass eine gewisse Kongruenz (d.h. eine Gleichung in einem endlichen Ring) nicht gilt, so kann man folgern, dass die entsprechende Gleichung in $\mathbb{Z}$ erst recht nicht gilt.
*Beispiel:* Ist die natürliche Zahl $n$ zu $-1$ modulo 4 kongruent, d.h. $n = 4 \cdot k + 3$ mit einem $k \in \mathbb{N}$, so ist $n$ nicht als Summe von zwei Quadraten ganzer Zahlen darstellbar. Denn in dem Ring $\mathbb{Z}/4$ gilt $\overline{0}^2 = \overline{2}^2 = \overline{0}$ und $\overline{1}^2 = \overline{3}^2 = \overline{1}$. Also gibt es keine $\overline{x},\ \overline{y} \in \mathbb{Z}/4$ mit $\overline{x}^2 + \overline{y}^2 = \overline{3}$. Wäre nun $x^2 + y^2 = n$ in $\mathbb{Z}$, so müsste $\overline{x}^2 + \overline{y}^2 = \overline{3}$ in $\mathbb{Z}/4$ gelten – und das geht nicht.
Viele der Aufgaben zu diesem Paragrafen beruhen auf diesem Prinzip.

**4.26** Sei $m \in \mathbb{N}_1$. Wenn $k \in \mathbb{N}$ und $\operatorname{ggT}(k, m) > 1$ ist, liegt in der Restklasse $k + m\mathbb{Z}$ höchstens eine Primzahl. Bis auf endlich viele Ausnahmen müssen sich die Primzahlen also auf die primen Restklassen modulo $m$ verteilen. Nach einem berühmten Satz von Dirichlet („Primzahlen in arithmetischen Progressionen") liegen in jeder primen Restklasse modulo $m$ unendlich viele Primzahlen. ([*Serre*] IV und [*Scheid*] VI.5.)

In unserem Buch werden wir nur einige Spezialfälle und Abschwächungen dieses Satzes zeigen. Z.B.:

**Satz: 4.27** *Sei $m \in \mathbb{N}_3$. Es gibt unendlich viele Primzahlen $p$ mit $p \not\equiv 1 \pmod{m}$.*

**Beweis:** Seien $p_1, \ldots, p_n$ (mit $n \geq 0$) Primzahlen mit $p_i \not\equiv 1\ (m)$. Wir konstruieren eine weitere solche Primzahl $p$.
Bilde $N := mp_1 \cdot \ldots \cdot p_n - 1$. Da nach Voraussetzung $m \geq 3$ ist, ist $N > 1$, auch wenn $n = 0$ sein sollte. Jeder Primfaktor von $N$ ist verschieden von allen $p_i,\ i = 1, \ldots, n$, da letztere $N$ nicht teilen. Wären alle Primfaktoren von $N$ zu 1 modulo $m$ kongruent, so auch $N$ selbst, da es ein Produkt von Potenzen seiner Primfaktoren ist. Es ist aber $N \equiv -1 \pmod{m}$ und $-1 \not\equiv 1 \pmod{m}$ wegen $m \geq 3$. Also gibt es mindestens einen Primfaktor $p$ von $N$ mit $p \not\equiv 1 \pmod{m}$. □

**Korollar: 4.28** *Für* $m = 3, 4$ *oder* $6$ *gilt:*
*Es gibt unendlich viele Primzahlen* $p \equiv -1 \pmod{m}$.

**Beweis:** Für diese Zahlen – übrigens auch nur für sie – gibt es genau zwei prime Restklassen modulo $m$, nämlich $1 + m\mathbb{Z}$ und $-1 + m\mathbb{Z}$. □

(Übrigens gilt für Primzahlen $p \geq 5$ :
$p \equiv -1\ (3) \iff p \equiv -1\ (6)$.)

AUFGABEN UND HINWEISE

**1)** Es soll eine Fahne mit einem Muster folgender Art entworfen werden:

```
        *  *  *  *  *
        *  *  *  *  *
        *  *  *  *  *
  *  *  *  *  *  *  *
  *  *  *  *  *  *  *
  *  *  *  *
  *  *  *  *
```

Abb. 6

D.h. $n$ Sterne sollen in zwei Quadrate von $m_1 \times m_1$ bzw. $m_2 \times m_2$ Sternen angeordnet werden, die sich in einem Quadrat von $k \times k$ Sternen überlappen. Dabei soll zwar $n$, aber keine der drei Zahlen $m_1, m_2, k$ ein Vielfaches von 5 sein. (Damit ist z.B. $k = 0$ auch ausgeschlossen.) Ist das möglich?

**2)** a) Ein moderner Bildhauer will eine Skulptur schaffen und dazu ein Vielfaches von 7 Kugeln in 3 Würfeln anordnen:

Abb. 7 a)

Aber in keinem einzelnen Würfel soll die Zahl der Kugeln ein Vielfaches von 7 sein.

b) Als der Bildhauer über seinem Entwurf verzweifelt, schlägt ihm ein Freund vor, einen der Würfel sich von den beiden anderen in je einem Würfel durchdringen zu lassen, wie es hier für nur zwei Würfel gezeichnet ist. Keine Kugel darf allen drei Würfeln angehören.

Abb. 7 b)

Wieder soll die Gesamtzahl der Kugeln ein Vielfaches von 7 sein, aber keiner der 3 Würfel und auch keiner der Durchdringungswürfel soll ein Vielfaches von 7 Kugeln haben. Lässt sich dies eher bewerkstelligen?

**3)** a) Sei $m \in \mathbb{N}$, $m = \sum_{i=0}^{k} a_i 10^i$ mit $a_i \in \mathbb{Z}$. Zeigen Sie:

$$m \equiv \sum_{i=0}^{k} a_i \pmod 9 \quad \text{und} \quad m \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}.$$

b) Leiten Sie daraus die bekannten Kriterien für die Teilbarkeit von in Dezimalschreibweise gegebenen Zahlen durch 3, 9 bzw. 11 ab.
c) Schreiben Sie die natürliche Zahl $n$ im Dezimalsystem mit ungerade vielen Ziffern. Dabei darf die erste Ziffer eine 0 sein. Bilden Sie das Palindrom $n'$ dieser Darstellung. (Das Palindrom von z.B. 01234 ist 43210.) Zeigen Sie: $99|n - n'$.
d) Gilt dies auch, wenn $n$ mit gerade vielen Ziffern geschrieben ist?
e) Seien $n_1, \ldots, n_r$ bis zu zehn natürliche Zahlen. Schreibt man sie im Dezimalsystem, so soll jede der zehn Ziffern in allen Zahlen zusammen genau einmal auftreten. Zeigen Sie, dass $n_1 + \ldots + n_r$ durch 9 teilbar ist.
f) Bei einer Unterhaltung bittet Sie Ihr Gegenüber, Sie mögen eine beliebige 5-stellige (natürliche) Zahl (im Dezimalsystem) – vor ihm verborgen – notieren, die Quersumme von dieser Zahl subtrahieren. Wenn Sie ihm dann beliebige 4 Ziffern der Differenz angeben, so macht er sich anheischig, die fnfte zu nennen. (In der Minderzahl der Fälle kann er allerdings die unbekannte Ziffer nicht genau benennen, sondern nur zwei Alternativen anbieten.)

**4)** Sei $d \in \mathbb{N}_2$. Entwickeln Sie für $d$–adisch geschriebene Zahlen (0.A3) Kriterien für die Teilbarkeit durch 2 (bzw. 3). Die Art eines solchen Kriteriums sollte nur von der Restklasse ($d$ mod 2) (bzw.
($d$ mod 3)) abhängen.

**5)** Von der Schule her ist Ihnen vielleicht die „Neunerprobe“ geläufig. Eine ausgeführte Multiplikation zweier (größerer) Zahlen kann man auf ihre Richtigkeit folgendermaßen testen: Der „Neunerrest“ des Produktes muss gleich dem „Neunerrest“ des Produktes der „Neunerreste“ der Faktoren sein. Von welcher Aussage dieses Paragrafen ist das ein Spezialfall?

**6)** Auf einem Blatt stehen alle natürlichen Zahlen von 1 bis 101 – jede genau einmal – geschrieben. Indem man zwei von ihnen, genannt $x$ und $y$, ausradiert und die Zahl $x^5 + y$ hinzufügt, vermindert man die Anzahl der Zahlen um 1. (Jede Zahl wird so oft gezählt, wie sie auf dem Papier steht.) Indem man dieses (nicht völlig determinierte) Verfahren noch 99 mal wiederholt, bleibt schließlich eine Zahl übrig. Können Sie die letzte Ziffer dieser Zahl angeben, ohne mehr zu wissen, als oben angegeben ist? (Vgl. 7.A9.)

**7)** Angenommen, Sie gießen Ihre Topfpflanzen jeden 2. (bzw. 3., bzw. 4., bzw. 5., bzw. 6.) Tag und beginnen damit an einem Sonntag. Gibt es einen Wochentag, an welchem Sie nie gießen?
Die Antwort sollte mit einem Satz dieses Paragrafen begründet werden.

**8)** Kalendarisches: Nach dem – aus der Mode gekommenen – Julianischen Kalender ist genau dann ein Schaltjahr, wenn die Jahreszahl durch 4 teilbar ist. Nach dem heute gültigen Gregorianischen Kalender ist dies in der Regel auch so, allerdings mit Ausnahme der Jahre, deren Jahreszahl durch 100, aber nicht durch 400 teilbar ist. Diese sind keine Schaltjahre.

a) Zeigen Sie: Für den Julianischen (bzw. Gregorianischen) Kalender gilt (mit $n, m \in \mathbb{N}_1$):

$$\left.\begin{array}{r} n \equiv m (\text{mod } 28) \\ (\text{bzw. } n \equiv m (\text{mod } 400) \end{array}\right\} \Longrightarrow \begin{array}{c} \text{Die Jahre } n \text{ und } m \text{ beginnen} \\ \text{mit demselben Wochentag.} \end{array}$$

b) Angenommen, der Julianische Kalender wäre seit dem Jahre 1 unverändert in Kraft, so wäre der Wochentag, mit dem das Jahr $n$ beginnt, der Tag

$$\left(n + \left[\frac{n-1}{4}\right] \text{ mod } 7\right),$$

wobei (1 mod 7) derjenige Wochentag ist, mit dem das Jahr 1 begann, (2 mod 7) der nächste Wochentag usw. ([ ] ist die Gaußklammer, 3.5.)

Diese Formel kann man auf die Jahre 1901 bis 2100 anwenden. Dabei ist (1 mod 7) der Sonntag, da $1989 \equiv 1$ (mod 28) ist und das Jahr 1989 mit einem Sonntag begann.
Übrigens ist

$$n + \left[\frac{n-1}{4}\right] \equiv 5q + r \equiv -2q + r \ (\text{mod } 7),$$

wenn

$$n = 4q + r \ \text{ mit } \ r \in \{1, 2, 3, 4\}$$

ist.

Überzeugen Sie sich von der Richtigkeit aller Behauptungen.
c) Für den Gregorianischen Kalender ergibt sich: Das Jahr $n$ beginnt mit

dem Wochentag

$$\left(n + \left[\frac{n-1}{4}\right] - \left[\frac{n-1}{100}\right] + \left[\frac{n-1}{400}\right] \mod 7\right).$$

Dabei ist (1 mod 7) der Dienstag, da das Jahr 1991 mit einem Dienstag begann.
Stimmt's?

d) Zeigen Sie: Nach dem Julianischen Kalender fällt im langjährigen Durchschnitt der 13. eines jeden Monats auf jeden Wochentag gleich oft.

e) Dies ist nicht so nach dem Gregorianischen Kalender. Nach [*Forster*], Aufgabe 1.5 fällt er am häufigsten auf den Freitag. Wer dies nachprüfen möchte, sollte – um Arbeit zu sparen – das Jahr am 1. März beginnen lassen.

**9)** Versuchen Sie, die Aussage aus 0. A7 besser zu verstehen, nämlich so, dass es Ihnen leicht fällt, selber Aussagen von solcher Art zu entwickeln.

**10)** Bestimmen Sie die Inversen (bzgl. der Multiplikation) von
(2 mod $m$) für ungerade und von (3 mod $m$) für nicht durch 3 teilbare $m$.

**11)** a) Ist (1777 mod 1855) eine prime Restklasse?
Bestimmen Sie gegebenenfalls das Inverse!
b) Welche Bedeutung haben die beiden in a) genannten Zahlen für die Mathematikgeschichte?

**12)** Sei $A$ ein Ring, $a \in A$. Definiere $h_a : A \longrightarrow A$ durch $x \longmapsto ax$.
a) Was bedeutet es für die Abbildung $h_a$, wenn $a$ eine Einheit, bzw. ein Nichtnullteiler, bzw. ein Nullteiler ist?
b) Zeigen Sie: Wenn $A$ endlich ist, ist jedes Element $a \in A$ entweder eine Einheit oder ein Nullteiler.

**13)** Sei $M$ eine Menge, $R$ ihre Potenzmenge (d.h. die Menge ihrer Teilmengen). Für $X, Y \in R$ definiere man

$$\begin{aligned} X+Y &:= (X \cup Y) - (X \cap Y) \\ XY &:= X \cap Y. \end{aligned}$$

Zeigen Sie: Mit diesen Verknüpfungen ist $R$ ein Ring.
(Hinweis: Betrachten sie Abbildungen $M \longrightarrow \mathbb{Z}/2$.)

**14)** Zeigen Sie: Für $n \in \mathbb{N}_2$ ist die Summe der zu $n$ teilerfremden Zahlen aus $\{1, \ldots, n-1\}$ gleich $\frac{1}{2}n \cdot \varphi(n)$.
(Hinweis: Was bedeutet das für das arithmetische Mittel dieser Zahlen?)

**15)** Seien $x, y \in \mathbb{Z}$. Zeigen Sie:
Ist $3x + 2y$ durch 17 teilbar, so auch $5x + 9y$.

**16)** Gray–Code: Sei $F(= (\mathbb{Z}/2)^{(\mathbb{N})})$ die Menge aller Folgen von Elementen aus $\mathbb{Z}/2$, derart dass fast alle Folgenglieder 0 sind. Sei

$$g : \mathbb{N} \longrightarrow F,\ g(n) := (g_0(n), g_1(n), g_2(n), \ldots)$$

durch

$$g_\nu(n) := \left( \left[ \frac{n + 2^\nu}{2^{\nu+1}} \right] \mathrm{mod} 2 \right)$$

definiert. Zeigen Sie:
a) $g$ ist bijektiv,
b) für jedes $n$ unterscheidet sich $g(n+1)$ von $g(n)$ nur an einer einzigen „Stelle“, d.h. es ist $g_\nu(n) = g_\nu(n+1)$ bis auf genau ein $\nu$.

**17** Bestimmen Sie die beiden (womöglich auch drei) letzten Ziffern von $1995^{1995!+1}$, sowie die letzte von $1998^{1998!}$ im Dezimalsystem.

**18** Seien $x, y, m, n \in \mathbb{Z},\ m, n \geq 1$. Zeigen Sie: Ist $x \equiv y \bmod p^m$, so ist $x^{p^n} \equiv y^{p^n} \bmod p^{m+n}$. (Es genügt, den Fall $n = 1$ zu betrachten, also $p^{m+1} | x^p - y^p$ zu zeigen. Schreiben Sie $x^p - y^p = (x-y)(x^{p-1} + x^{p-2}y + \cdots + y^{p-1})$. Modulo $p^m$ besteht der zweite Faktor aus $p$ zueinander kongruenten Summanden, ist also, da $m \geq 1$, durch $p$ teilbar.) Gilt die Behauptung auch für $m = 0$? Zeigen Sie, dass die Umkehrung nicht gilt.

# § 5

# Zyklische Gruppen

In diesem und dem nächsten Paragrafen wird mehr Algebra als Zahlentheorie getrieben. Jedoch, einerseits erhalten wir auch zahlentheoretische Ergebnisse – z.B. 5.16 und 6.7 –, andererseits werden hier die Grundlagen für eine elegante begriffliche Behandlung der Paragrafen 8 bis 10 gelegt.

**Definition: 5.1** *$G$ sei eine additiv geschriebene abelsche Gruppe, $a \in G$, $m \in \mathbb{N}$. Definiere $ma := \underbrace{a + \ldots + a}_{m-mal}$.*
*Formal besser, definiert man $ma$ induktiv durch $0_{\mathbb{Z}} \cdot a := 0_G$, $(m+1)a := ma + a$. (Dabei ist der Deutlichkeit halber hier mit $0_{\mathbb{Z}}$ die $0$ in $\mathbb{Z}$ und mit $0_G$ diejenige in $G$ bezeichnet. Das werden wir jedoch nur gelegentlich so machen.)*
*Für $m \in \mathbb{Z}$ und $m < 0$ – d.h. $-m > 0$ – definiert man $ma := (-m)(-a) = -(-m)a$. Falls $G$ multiplikativ geschrieben ist, definiert man $a^m := \underbrace{a \cdot \ldots \cdot a}_{m-mal}$ für $m \geq 0$ und $a^m := (a^{-1})^{-m} = (a^{-m})^{-1}$ für $m < 0$.*

**Feststellung: 5.2** *Für das vorgenannte „Produkt“ gilt mit $m, n \in \mathbb{Z}$, $a, b \in G$*

*a)* $1a = a$, *b)* $(mn)a = m(na)$,
*c)* $(m+n)a = ma + na$, *d)* $m(a+b) = ma + mb$.

(Vergleichen Sie diese Gesetze mit denen der Vektorraumdefinition.)

Für $m, n \geq 0$ kann man sich z.B. b) wie folgt klarmachen:

$$(mn)a = \underbrace{a + \ldots + a}_{mn-\text{mal}} =$$

$$\underbrace{\underbrace{(a + \ldots + a)}_{n-\text{mal}} + \underbrace{(a + \ldots + a)}_{n-\text{mal}} + \ldots + \underbrace{(a + \ldots + a)}_{n-\text{mal}}}_{m-\text{mal}}$$

$$= m(na).$$

Für $m, n \geq 0$ sind c) und d) noch leichter zu begreifen. Für d) braucht man die Kommutativität von $G$. Ein formaler Beweis von b) bis d) für $m, n \geq 0$ würde mit vollständiger Induktion erfolgen. Der fleißige Leser, der dies versucht, sollte c) vor b) erledigen.
Für b) und d) kann man den allgemeinen Fall $m, n \in \mathbb{Z}$ auf den speziellen Fall $m, n \in \mathbb{N}$ leicht zurückführen. Für c) behandle man erst den Fall $m, n < 0$ und schreibe dann im allgemeinen Fall $m, n$ als Differenzen natürlicher Zahlen.

Wir überlassen es dem Leser, die entsprechenden Gesetze für eine multiplikativ geschriebene abelsche Gruppe zu formulieren.

**Bemerkung: 5.3** Wenn $G$ nicht abelsch ist, so ist d) falsch. D.h. man hat oft $(ab)^m \neq a^m b^m$ (bei multiplikativer Schreibweise). Man sieht sogar sofort, dass aus $(ab)^2 = a^2 b^2$ in einer Gruppe die Gleichung $ba = ab$ folgt.

**Definition: 5.4** *Eine abelsche Gruppe $G$ heißt zyklisch, wenn es ein $z \in G$ gibt, so dass jedes Element $a \in G$ die Gestalt $a = n \cdot z$ mit einem $n \in \mathbb{Z}$ hat. Ein Element $z$ dieser Art heißt ein Erzeuger der Gruppe.*

**Bemerkung: 5.5** Das Wort „abelsch“ in obiger Definition kann man weglassen. Denn eine nicht notwendig abelsche Gruppe $G$, in der es ein $z$ gibt, so dass (bei multiplikativer Schreibweise) alle Elemente von $G$ von der Form $z^n$ mit $n \in \mathbb{Z}$ sind, ist schon abelsch: Es gilt nämlich

$$z^m \cdot z^n = z^{m+n} = z^{n+m} = z^n \cdot z^m.$$

**Definition: 5.6** *Seien $G, H$ Gruppen. Ein Homomorfismus von $G$ nach $H$ ist eine Abbildung $f : G \longrightarrow H$ mit $f(a+b) = f(a) + f(b)$ für alle $a, b \in G$. Ein Isomorfismus von $G$ nach $H$ ist ein bijektiver Homomorfismus. $G$ und $H$ heißen zueinander isomorf, wenn es einen Isomorfismus von $G$ nach $H$ gibt. Man schreibt dann $G \cong H$.*

**Bemerkungen: 5.7** Sei $f : G \longrightarrow H$ ein Homomorfismus.

a) $f(0) = 0$ (genauer $f(0_G) = 0_H$).
Denn es ist $f(0) = f(0+0) = f(0) + f(0)$. Durch Addition von $-f(0)$ erhält man $0 = f(0)$.

b) $f(-a) = -f(a)$.
Denn $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$.

c) Wenn $f$ bijektiv ist, ist auch die Umkehrabbildung $f^{-1} : H \longrightarrow G$ ein Homomorfismus.
Seien nämlich $a, b \in H$ mit $f^{-1}(a) = a'$, $f^{-1}(b) = b'$, also $f(a') = a$, $f(b') = b$. Dann ist $f(a' + b') = f(a') + f(b') = a + b$, also
$f^{-1}(a + b) = a' + b' = f^{-1}(a) + f^{-1}(b)$.

d) Wegen c) folgt aus $G \cong H$, dass auch $H \cong G$ gilt.
Ebenso gilt: $G \cong G$. Schließlich folgt aus $G \cong H$ und $H \cong K$ auch $G \cong K$.

e) Sei $G$ eine (additiv geschriebene) Gruppe von 2 Elementen 0 und $x \neq 0$. Dann ist $x + x = 0$. Denn aus $x + x = x$ würde $x = 0$ folgen. Es gibt also einen und auch nur einen Isomorfismus

$$\mathbb{Z}/2 \xrightarrow{\cong} G, \;\text{ nämlich }\; \overline{0} \longmapsto 0,\; \overline{1} \longmapsto x.$$

Angewandt auf die Gruppe $\mathbb{Z}^* = \{1, -1\}$ ergibt sich der Isomorfismus

$$\mathbb{Z}/2 \xrightarrow{\cong} \{1, -1\},\; \overline{0} \longmapsto 1,\; \overline{1} \longmapsto -1.$$

**Feststellung: 5.8** *Sei $G$ eine zyklische Gruppe und $z \in G$ ein Erzeuger. Dann ist die Abbildung $F : \mathbb{Z} \longrightarrow G$ mit $F(n) = nz$ ein surjektiver Gruppenhomomorfismus. (Wenn wir von Gruppen reden, ist mit $\mathbb{Z}$ und mit $\mathbb{Z}/m$ jeweils die additive Gruppe gemeint.)*

**Beweis:** Aus 5.2 c) folgt, dass $F$ ein Homomorfismus, und aus der Definition eines Erzeugers, dass $F$ surjektiv ist. $\square$

**Satz: 5.9** *Sei $G$ eine zyklische Gruppe mit Erzeuger $z$. Dann gibt es ein $m \in \mathbb{N}$ und einen Gruppenisomorfismus*

$$f : \mathbb{Z}/m \longrightarrow G$$

*mit $f(1 \; mod \; m) = z$.*
*(Dabei ist $m$ durch $G$ eindeutig bestimmt: $m = 0$, wenn $G$ unendlich ist, ansonsten $m = \#G$.)*

**Beweis:** Betrachte die Abbildung $F : \mathbb{Z} \longrightarrow G$ aus 5.8, also $F(n) = nz$. Sei $K \subset \mathbb{Z}$ der sogenannte Kern von $F$, d.h. $K := \{k \in \mathbb{Z} | F(k) = 0\} = \{k \in \mathbb{Z} | k \cdot z = 0\}$.

*Behauptung 1:* $K$ ist eine Untergruppe von $\mathbb{Z}$.
Denn offenbar ist $0 \in K$, und wenn $a, b \in K$, ist $(a - b)z = az - bz = 0$, also $a - b \in K$.
Nach 1.6 gibt es ein $m \in \mathbb{N}$ mit $K = m\mathbb{Z}$.

*Behauptung 2:* $F(k) = F(k') \iff k \equiv k' \pmod{m}$.
Denn: $F(k) = F(k') \iff kz = k'z \iff (k - k')z = 0 \iff$
$k - k' \in m\mathbb{Z} \iff k \equiv k' \pmod{m}$.

Wegen der Implikation „$\Longleftarrow$“ aus der Behauptung 2 kann man definieren:

$$f\left((k \bmod m)\right) := F(k) = kz;$$

denn, wenn $(k \bmod m) = (k' \bmod m)$ ist, gilt auch $F(k) = F(k')$. Man hat also die Abbildung $f : \mathbb{Z}/m \longrightarrow G$ gefunden. Offenbar ist
$f(1 \bmod m) = z$. Da $F$ ein surjektiver Homomorfismus ist, gilt dies auch für $f$.
Aus der Implikation „$\Longrightarrow$“ der Behauptung 2 folgt schließlich die Injektivität von $f$. $\square$

(Abbildung 5 zeigt, woher zyklische Gruppen ihren Namen haben: $\kappa\acute{\upsilon}\kappa\lambda o\varsigma$ = Kreis.)

**Beispiel: 5.10** $\mathbb{Z}^* \cong \mathbb{Z}/2$ (vgl. 5.7 e)). Allgemeiner sei
$G = \left\{ e^{2\pi i k/m} \middle| \, k \in \mathbb{Z} \right\}$, $m \in \mathbb{N}_1$. Dann ist $\mathbb{Z}/m \cong G$ mittels
$\overline{k} \longmapsto \left(e^{2\pi i/m}\right)^k$.
(Beachte: Hier wird $G$ multiplikativ, $\mathbb{Z}/m$ additiv geschrieben.)

**5.11 Definitionen:** *Sei $G$ eine Gruppe, $a \in G$.*
*a)* $\langle a \rangle := \{k \cdot a \mid k \in \mathbb{Z}\}$ *(bzw. $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ bei multiplikativer Schreibweise).*
*b) Die Ordnung von $a$ ist $ord(a) := \#\langle a \rangle \in \mathbb{N}_1 \cup \{\infty\}$.*

**Bemerkungen: 5.12** a) Für jedes $a \in G$ ist $\langle a \rangle$ eine zyklische Untergruppe von $G$.
b) Wenn es ein $r \in \mathbb{N}_1$ mit $ra = 0$ gibt, ist $\text{ord}(a)$ endlich, und zwar die kleinste der Zahlen $r \in \mathbb{N}_1$ mit $ra = 0$. Wenn es solche $r$ nicht gibt, ist $\text{ord}(a) = \infty$.
c) Wenn $\text{ord}(a) < \infty$ und $ka = 0$ für ein $k \in \mathbb{Z}$ ist, gilt $\text{ord}(a)|k$.
Denn aus 5.9 und seinem Beweis ergibt sich

$$ord(a) \cdot \mathbb{Z} = \{k \in \mathbb{Z} | ka = 0\}.$$

d) Sei $\text{ord}(a) = m < \infty$. Für $k, k' \in \mathbb{Z}$ gilt dann

$$ka = k'a \iff k \equiv k' (\text{mod } m).$$

Denn es ist

$$(k - k')a = 0 \iff k - k' \in m\mathbb{Z}$$

nach c) und der trivialen Umkehrung von c).
e) Eine endliche Gruppe $G$ ist genau dann zyklisch, wenn es ein $z \in G$ mit $\text{ord}(z) = \#G$ gibt.
Denn es ist $\langle z \rangle \subset G$ und $\#G < \infty$. Also gilt $\langle z \rangle = G$ genau dann, wenn $\#\langle z \rangle = \#G$ ist.

**Satz: 5.13** *Sei $G$ eine zyklische Gruppe der Ordnung $m < \infty$ und $z$ ein Erzeuger von $G$, ferner $k \in \mathbb{Z}$. Das Element $kz$ ist genau dann ein Erzeuger von $G$, wenn $ggT(k, m) = 1$ ist.*
*Insbesondere ist $\varphi(m)$ die Anzahl der Elemente aus $G$, die (jedes für sich) Erzeuger von $G$ sind.*

**Beweis:** Wegen Satz 5.9 dürfen wir $G = \mathbb{Z}/m$ und $z = (1 \bmod m)$ annehmen. Dann ist offenbar $kz = (k \bmod m)$.
Wenn $kz$ ein Erzeuger ist, gibt es insbesondere ein $k' \in \mathbb{Z}$, so dass $k'kz = z$, d.h. $k'k \equiv 1 \pmod{m}$ ist. Mithin gibt es $k', m' \in \mathbb{Z}$ mit $1 = kk' + mm'$. D.h. es ist $\mathrm{ggT}(k, m) = 1$.
Umgekehrt folgt aus $\mathrm{ggT}(k, m) = 1$, dass es ein $k' \in \mathbb{Z}$ mit
$k'k \equiv 1 \pmod{m}$ also $k'kz = z$ gibt. Für jedes $n \in \mathbb{Z}$ ist dann
$(nk')(kz) = nz$ und somit $\langle kz \rangle = \langle z \rangle = G$.
Eine Restklasse modulo $m$ ist also genau dann ein Erzeuger der additiven Gruppe $\mathbb{Z}/m$, wenn sie eine prime Restklasse modulo $m$ ist. Und deren Anzahl ist $\varphi(m)$. □

**Satz: 5.14** *Sei $G$ eine zyklische Grupe der Ordnung $m < \infty$ mit einem Erzeuger $z$ und $H$ eine Untergruppe. Dann ist $H$ ebenfalls zyklisch, und es gibt einen Teiler $d$ von $m$, derart dass $dz$ ein Erzeuger von $H$ und $\#H = m/d$ ist. Insbesondere gilt: $\#H|m$.*

**Beweis:** Betrachte die folgende Teilmenge $M := \{a \in \mathbb{Z} | az \in H\}$ von $\mathbb{Z}$. Diese Menge ist eine Untergruppe von $\mathbb{Z}$. Denn es ist $0z = 0 \in H$, also $0 \in M$, und mit $a, b \in M$ gilt $(a-b)z = az - bz \in H$, also $a - b \in M$. Deshalb gibt es ein $d \in \mathbb{N}$ mit $M = d\mathbb{Z}$.
Wegen $m \in M$ gilt $d|m$.
Jedes Element von $G$, also erst recht jedes Element von $H$ ist von der Form $az$ mit einem $a \in \mathbb{Z}$. Und deshalb ist
$H = \{az | a \in M\} = \{az | a \in d\mathbb{Z}\} = \{b(dz) | b \in \mathbb{Z}\} = \langle dz \rangle$.
Die verschiedenen Vielfachen von $dz$ in $G$ sind $1 \cdot dz,\ 2 \cdot dz,$
$\ldots, (m/d) \cdot dz = mz = 0$. Also gilt $\#H = m/d$. □

**Korollar: 5.15** *Zu jedem Teiler $n > 0$ von $m$ besitzt eine zyklische Gruppe der Ordnung $m$ genau eine Untergruppe der Ordnung $n$.*

**Beweis:** Sei $G = \langle z \rangle$ und $d = m/n$. Dann ist $\langle dz \rangle$ eine Untergruppe von $G$ der Ordnung $m/d = n$.
Nach 5.14 ist aber $H = \langle dz \rangle$, wenn $H$ eine Untergruppe der Ordnung $m/d$ ist. □

**Korollar: 5.16** *Für jedes $m \in \mathbb{N}_1$ gilt* $\sum_{d \in \mathbb{N}, d|m} \varphi(d) = m$.

**Beweis:** Zu jedem positiven Teiler $d$ von $m$ gibt es genau eine Untergruppe $H_d$ von $\mathbb{Z}/m$ der Ordnung $d$. Definiere
$E_d = \{x \in G | \langle x \rangle = H_d\}$. Nach 5.13 ist $\# E_d = \varphi(d)$.
Nun ist jedes $x \in \mathbb{Z}/m$ der Erzeuger der Untergruppe $\langle x \rangle$, liegt also in genau einem $E_d$ mit $d > 0,\ d|m$. Mithin ist

$$m = \#(\mathbb{Z}/m) = \sum_{d|m, d \in \mathbb{N}} \# E_d = \sum_{d|m, d \in \mathbb{N}} \varphi(d). \qquad \square$$

## AUFGABEN UND HINWEISE

**1)** Seien $G$ eine endliche zyklische Gruppe, $H_1, H_2$ Untergruppen der Ordnung $d_1, d_2$. Zeigen Sie:

$$H_1 \subset H_2 \iff d_1 | d_2.$$

**2)** a) Seien $m, n \in \mathbb{N}_1$ zueinander teilerfremd. Zeigen Sie:
Es gibt ein $k \in \mathbb{N}_1$ mit $m | n^k - 1$.
b) Sei $p$ eine Primzahl. Die Folge $(x_n)$ sei durch $x_0 = p$,
$x_{n+1} = 2x_n + 1$, definiert. Zeigen Sie:
Die Folge $(x_n)$ kann nicht nur aus Primzahlen bestehen.

**3)** *Sei $G$ eine endliche Gruppe der Ordnung $p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ mit $p_i \in \mathbb{P}$, $\alpha_i \in \mathbb{N}_1$, ferner $z$ ein Erzeuger von $G$ und $x \in G$ mit*
$p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_r^{\alpha_r - 1} x = 0$.
*Zeigen Sie:* $z + x$ *ist ein Erzeuger von* $G$.

**4)** *Ein Zahlenrätsel:*
*$GAUSS$ ist ein Primfaktor von $BRAHMAGUPTA$, wenn vier der vorkommenden 10 Buchstaben für die Ziffer 0, sechs für die Ziffer 1 stehen und beide Zahlen in Binärschreibweise mit $B = G = 1$ geschrieben sind. Bestimmen Sie sämtliche Lösungen.*

# § 6

# Untergruppen, Faktorgruppen, Ideale, Restklassenringe und Homomorfismen

Hier werden die Konstruktionen von §4 verallgemeinert.

*Sei im folgenden $G$ eine (additiv geschriebene) abelsche Gruppe, $H$ eine Untergruppe.*

**Definition: 6.1** *Sei $a \in H$. Die Nebenklasse von $a$ modulo $H$, auch mit ($a$ mod $H$) bezeichnet, ist die Teilmenge $a + H = \{a + h | h \in H\}$ von $G$.*

**6.2** Analog zu 4.3 gilt der

**Satz:** *a) Für jedes $a \in G$ ist $a \in (a \text{ mod } H)$.*
*b) Gilt $(a \text{ mod } H) \cap (b \text{ mod } H) \neq \emptyset$, so ist $(a \text{ mod } H) = (b \text{ mod } H)$.*
*c) Jedes $a \in G$ liegt in genau einer Nebenklasse modulo $H$.*
*d) Jede Nebenklasse modulo $H$ hat so viele Elemente wie $H$.*

**Beweis:** a) ist trivial.
b) Sei etwa $a + h_1 = b + h_2$ mit $h_i \in H$, so ist $a + h = b + h + h_2 - h_1 \in b + H$

für jedes $h \in H$. Somit ist $a + H \subset b + H$. Die Inklusion $b + H \subset a + H$ ist genauso zu beweisen.
c) folgt aus a), b).
d) Die Abbildung $H \longrightarrow a + H$, $h \longmapsto a + h$ ist bijektiv. Sie ist nämlich surjektiv nach Definition von $a + H$. Und da aus $a + h_1 = a + h_2$ in der Gruppe $G$ die Gleichung $h_1 = h_2$ folgt, ist die Abbildung auch injektiv. □

**Definition: 6.3** *Mit $[G : H]$ wird die Anzahl der Nebenklassen modulo $H$ bezeichnet. Sie heißt Index von $H$ (in $G$).*

**Satz: 6.4** *Es ist $\#G = [G : H] \cdot \#H$.*
*(Dies gilt auch, falls $\#G = \infty$ ist, wenn man*
*$\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty$ für $n \in \mathbb{N}_1$ definiert. Es ist auch richtig im Sinne des Produktes von möglicherweise unendlichen Kardinalzahlen.)*
*Insbesondere gilt $\#H \mid \#G$, wenn $G$ endlich ist.*

**Beweis:** Es gibt nach Definition $[G : H]$ Nebenklassen, die alle so viele Elemente wie $H$ haben. □

**Korollar: 6.5** *a) Für $x \in G$, $G$ endlich, gilt ord$(x) \mid \#G$.*
*b) Insbesondere ist $(\#G) \cdot x = 0$.*

**Beweis:** a) $\text{ord}(x) = \#\langle x\rangle$ und $\langle x\rangle$ ist eine Untergruppe von $G$.
b) Dies folgt aus a) und 5.12 d). □

**6.6** Wir erhalten das zahlentheoretische

**Korollar** (*Euler*):
*Sei $k \in \mathbb{Z}$ teilerfremd zu $m \in \mathbb{N}_1$. Dann ist $k^{\varphi(m)} \equiv 1 \pmod m$.*

**Beweis:** Nach 4.19 und 4.22 ist ($k$ mod $m$) ein Element der (multiplikativ geschriebenen) Einheitengruppe $(\mathbb{Z}/m)^*$ von $\mathbb{Z}/m$. Diese hat $\varphi(m)$ Elemente. Wende 6.5 b) an. □

**6.7** Speziell für eine Primzahl $p$ erhalten wir das (historisch ältere)

**Korollar** („Kleiner Satz“ von *Fermat)*:
*a)* *Wenn* $p \nmid k$*, so ist* $k^{p-1} \equiv 1 \pmod{p}$*.*
*b)* *Für beliebige* $k \in \mathbb{Z}$ *ist* $k^p \equiv k \pmod{p}$*.*

**Beweis:** a) Gilt wegen 6.6 und $\varphi(p) = p - 1$.
b) folgt für $k \not\equiv 0 \pmod{p}$ aus a) und ist für $k \equiv 0 \pmod{p}$ trivial. □

Eines unserer Ziele wird es sein, für gewisse $m$ zu zeigen, dass die Einheitengruppe $(\mathbb{Z}/m)^*$ zyklisch ist. Wir sind jetzt in der Lage, ein Kriterium für das Zyklischsein einer endlichen abelschen Gruppe zu beweisen:

**Satz: 6.8** *Sei* $G$ *eine abelsche Gruppe der Ordnung* $m < \infty$*. Für jeden positiven Teiler* $d$ *von* $m$ *gebe es höchstens* $d$ *Elemente* $x \in G$ *mit* $dx = 0$*. Dann ist* $G$ *zyklisch.*

**Beweis:** Für $d|m$ sei $\psi(d) := \#\{x \in G \mid \operatorname{ord} x = d\}$. Zu zeigen ist $\psi(m) > 0$.
Da jedes $x \in G$ eine Ordnung hat, die $m$ teilt, ist

$$(1) \qquad \sum_{d \in \mathbb{N}, d|m} \psi(d) = m.$$

Sei $d > 0$ ein Teiler von $m$ mit $\psi(d) > 0$, d.h. es existiere ein $x \in G$ der Ordnung $d$. Die zyklische Gruppe $\langle x \rangle$ hat $d$ Elemente, und für $y \in \langle x \rangle$ gilt $dy = 0$. Deshalb gehören nach Voraussetzung alle $z$ mit $dz = 0$ zu $\langle x \rangle$, insbesondere alle der Ordnung $d$. D.h. alle $z$ der Ordnung $d$ sind Erzeuger von $\langle x \rangle$. Von diesen gibt es gemäß 5.13 genau $\varphi(d)$ Stück.
Deshalb gilt $\psi(d) = \varphi(d)$, wenn $\psi(d) > 0$ ist.
Nach 5.16 ist aber

$$(2) \qquad \sum_{d \in \mathbb{N}, d|m} \varphi(d) = m \qquad .$$

Aus (1), (2) und den Ungleichungen $\psi(d) \leq \varphi(d)$ folgt $\psi(d) = \varphi(d)$ für alle positiven Teiler $d$ von $m$.
Insbesondere ist $\psi(m) = \varphi(m) > 0$, was zu zeigen war. □

**Definition: 6.9** *a) Mit $G/H$ wird die Menge der Nebenklassen modulo $H$ bezeichnet.*
*b) Die kanonische Abbildung $\kappa : G \longrightarrow G/H$ wird durch $\kappa(a) = a + H$ definiert.*

**6.10** Analog zu 4.9 erhalten wir den

**Satz:** *Für $a, b \in G$ sind folgende Aussagen äquivalent:*

(i) $(a \; mod \; H) = (b \; mod \; H)$, d.h. $\kappa(a) = \kappa(b)$;

(ii) $a \in (b \; mod \; H)$;

(iii) $b \in (a \; mod \; H)$;

(iv) $(a \; mod \; H) \cap (b \; mod \; H) \neq \emptyset$;

(v) $a - b \in H$.

Der Beweis stimmt mit dem von 4.9 fast buchstäblich überein. □

**Definition: 6.11** *Man sagt, „$a$ ist kongruent zu $b$ modulo $H$“, und schreibt $a \equiv b \; (mod \; H)$ oder $a \equiv b \; (H)$, wenn $a, b, H$ die äquivalenten Aussagen von 6.10 erfüllen.*

**Feststellung: 6.12** *Die Kongruenzrelation genügt offenbar folgenden Gesetzen:*
*a)* $a \equiv a \; (mod \; H)$,
*b)* $a \equiv b \; (mod \; H) \Longrightarrow b \equiv a \; (mod \; H)$,
*c)* $a \equiv b \; (mod \; H), \;\; b \equiv c \; (mod \; H) \;\Longrightarrow a \equiv c \; (mod \; H)$.
*d) Ist $H'$ eine weitere Untergruppe von $G$ mit $H \subset H'$, so gilt die Implikation*

$$a \equiv b \; (mod \; H) \quad \Longrightarrow \quad a \equiv b \; (mod \; H').$$

*e)* $a \equiv a' \; (mod \; H), \; b \equiv b' \; (mod \; H) \quad \Longrightarrow \quad a + b \equiv a' + b' \; (mod \; H)$.

**6.13** Wie in 4.13 können wir wegen 6.12 e) auf der Menge $G/H$ eine Addition definieren:

$$(a \bmod H) + (b \bmod H) := (a + b \bmod H).$$

**Feststellungen: 6.14** *Mit der oben angegebenen Addition ist $G/H$ eine abelsche Gruppe. $H = (0 \bmod H)$ ist das neutrale Element, und $(-a \bmod H)$ ist zu $(a \bmod H)$ invers. Ferner ist $\kappa : G \longrightarrow G/H$ ein Homomorfismus, der sogenannte kanonische Homomorfismus.*

**Definition: 6.15** *$G/H$, mit der oben angegebenen Addition, heißt die Faktorgruppe (oder Restklassengruppe) von $G$ modulo $H$ (oder von $G$ nach $H$).*

**Feststellung: 6.16** *Wenn $G$ zyklisch ist, so ist es auch jede Faktorgruppe $G/H$ von $G$. Ist $z$ ein Erzeuger von $G$, so ist $(z \bmod H)$ ein solcher von $G/H$.*

**Beweis:** Wenn $G = \{nz \mid n \in \mathbb{Z}\}$ gilt, dann erst recht
$G/H = \{nz + H \mid n \in \mathbb{Z}\} = \{n\,(z \bmod H) \mid n \in \mathbb{Z}\}$. □

**Bemerkung: 6.17** Zusammen mit 5.14 ergibt sich: Ist $G$ eine zyklische Gruppe, $H$ eine Untergruppe, so sind $H$ sowie $G/H$ ebenfalls zyklisch. Die Umkehrung ist i.a. falsch. Beachte jedoch 7.14.

**6.18 Bemerkungen**(für den nicht abelschen Fall, die in diesem Buch nicht gebraucht werden):
Man muss ein wenig vorsichtig sein, will man obige Betrachtungen auf nicht (notwendig) kommutative Gruppen verallgemeinern. Man hat dann zwischen Linksnebenklassen $aH$ und Rechtsnebenklassen $Ha$ zu unterscheiden (multiplikative Schreibweise!).
Satz 6.2 behält seine Gültigkeit, wenn man ihn entweder auf Linksnebenklassen oder auf Rechtsnebenklassen anwendet. Hingegen kann $aH \cap Hb \neq \emptyset$ sein

und trotzdem $aH \neq Hb$ gelten.
Es gibt ebenso viele Rechts- wie Linksnebenklassen nach $H$. Die Abbildung $aH \longmapsto Ha^{-1} = \{x^{-1} \mid x \in aH\}$ gibt eine bijektive Zuordnung.
(Hingegen wird durch $aH \longmapsto Ha$ keine Abbildung definiert; denn aus $aH = bH$ folgt *nicht* allgemein $Ha = Hb$!)
Man kann also den Index $[G : H]$ mit Links- oder mit Rechtsnebenklassen definieren.

Satz 6.4 bleibt erhalten und auch das Korollar 6.5. Insbesondere ist $x^{\#G} = 1$ (multiplikative Schreibweise) für $x \in G$.

Satz 6.8 gilt ohne die Voraussetzung, $G$ sei abelsch.

Satz 6.10 gilt für Linksnebenklassen, wenn man (v) durch $b^{-1}a \in H$ ersetzt. Für Rechtsnebenklassen gilt er, wenn man (v) durch $ab^{-1} \in H$ ersetzt.
Auf $G/H$ kann man genau dann eine kanonische Gruppenstruktur erklären, wenn $aH = Ha$ für alle $a \in G$ gilt. In diesem Falle heißt $H$ ein Normalteiler von $G$. Jede Untergruppe einer abelschen Grupe ist ein Normalteiler.

Im folgenden wollen wir eine wichtige Beziehung zwischen den Begriffen Faktorgruppe und Gruppenhomomorfismus (5.6) beschreiben.

**Definition: 6.19** *Sei $f : G \longrightarrow H$ ein Gruppenhomomorfismus. Der Kern von $f$ ist die Menge*

$$Ker(f) := \{a \in G \mid f(a) = 0_H\}.$$

*Das Bild von $f$ ist die Menge*

$$Im(f) := f(G) := \{f(a) \mid a \in G\}.$$

**Bemerkungen: 6.20** a) Ker$(f)$ ist eine Untergruppe von $G$ und Im$(f)$ eine solche von $H$.
Denn wegen $f(0_G) = 0_H$ (5.7) ist $0_G \in$Ker$(f)$, $0_H \in$ Im$(f)$. Und wegen $f(a - b) = f(a) + f(-b) = f(a) - f(b)$ ist sowohl Ker$(f)$ als auch Im$(f)$ gegen Differenzenbildung abgeschlossen.
b) Für $a, b \in G$ gilt $f(a) = f(b)$ genau dann, wenn $f(a - b) = 0$, d.h. $a - b \in$ Ker$(f)$ ist. Insbesondere ist $f$ genau dann injektiv, wenn Ker$(f) = \{0\}$ ist.

**6.21 Satz** *(Homomorfiesatz, Verallgemeinerung von 5.9):*
*Sei $f : G \longrightarrow H$ ein Homomorfismus abelscher Gruppen und $U \subset G$ eine Untergruppe von $G$ mit $U \subset Ker(f)$. Dann gibt es einen eindeutig bestimmten Homomorfismus $g : G/U \longrightarrow H$ derart, dass das Diagramm*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\kappa"'] & & H \\ & G/U \arrow[ur, "g"'] & \end{tikzcd}$$

*kommutativ ist, d.h. $f = g \circ \kappa$ gilt. Hierbei ist $\kappa$ die kanonische Abbildung. Wenn $U$ =Ker(f) ist, ist $g$ injektiv. D.h. es gibt einen Isomorfismus $G/Ker(f) \cong Im(f)$.*

**Beweis:** Seien $a, b \in G$. So gilt $a \equiv b$ (mod Ker$(f)$) genau dann, wenn $f(a) = f(b)$ ist (6.20 b). Da $U \subset \mathrm{Ker}(f)$, folgt aus $a \equiv b$ (mod $U$), dass $a \equiv b$ (mod Ker$(f)$), d.h. $f(a) = f(b)$ ist. Deshalb ist die Abbildung $g : G/U \longrightarrow H$ durch $g((a \bmod U)) := f(a)$ wohldefiniert. Da mithin $g$ vermittels $f$ definiert ist, sieht man sowohl, dass $g$ ein Homomorfismus, als auch, dass $g \circ \kappa = f$ ist. Ferner folgt $\mathrm{Im}(f) = \mathrm{Im}(g)$.
Die Eindeutigkeit von $g$ folgt so: Wenn $g' \circ \kappa = f$ ist, so ist
$g'(a \bmod U) = g' \circ \kappa(a) = f(a)$; d.h. $g' = g$.
Sei jetzt $U = \mathrm{Ker}(f)$ und $g((a \bmod U)) = g((b \bmod U))$, d.h.
$f(a) = f(b)$. Dann ist $a - b \in \mathrm{Ker}(f) = U$, also
$(a \bmod U) = (b \bmod U)$. Somit ist $g$ injektiv und bildet $G/\ \mathrm{Ker}(f)$ bijektiv, also isomorf auf $\mathrm{Im}(g) = \mathrm{Im}(f)$ ab. □

**6.22 Bemerkung** (für den nichtabelschen Fall, die ebenfalls in diesem Buch nicht gebraucht wird):
Seien in 6.19ff $G$ und $H$ nicht notwendig abelsch. Dann ist Ker$(f)$ ein Normalteiler. Satz 6.21 bleibt richtig, wenn man zusätzlich voraussetzt, $U$ sei ein Normalteiler.

Wie sieht die Sache bei Ringen aus? Ganz ähnlich, da diese ja bezüglich der Addition Gruppen sind.

**Definition: 6.23** *Ein Ideal eines Ringes $A$ ist eine Teilmenge $I$ von $A$ mit folgenden Eigenschaften:*

*1) $I$ ist bzgl. der Addition eine Untergruppe von $A$;*
*2) für $a \in A$ und $x \in I$ gilt $ax \in I$.*

**Bemerkung: 6.24** Eine Untergruppe $H$ der additiven Gruppe von $\mathbb{Z}$ ist schon ein Ideal. Denn für $a \in \mathbb{Z}$, $x \in H$ gilt $ax = \pm(x + x + \ldots + x)$.
Die Ideale von $\mathbb{Z}$ sind also die Mengen $m\mathbb{Z}$.

**Definitionen: 6.25** *a) Ein Ringhomomorfismus ist eine Abbildung von Ringen:*

$$f : A \longrightarrow B \quad \textit{mit}$$

*(i) $f(a + b) = f(a) + f(b)$, d.h. $f$ ist ein Homomorfismus der additiven Gruppen,*

*(ii) $f(ab) = f(a) \cdot f(b)$;*

*(iii) $f(1_A) = 1_B$.*

*b) Der Kern eines solchen Ringhomomorfismus ist*

$$\mathit{Ker}(f) := \{a \in A \mid f(a) = 0_B\}.$$

*b) Das Bild von $f$ ist*

$$\mathit{Im}(f) := f(A) = \{f(a) \mid a \in A\}.$$

*d) Ein Isomorfismus von Ringen ist ein bijektiver Ringhomomorfismus.*

**Bemerkungen: 6.26** a) Der Kern eines Ringhomomorfismus $f : A \longrightarrow B$ ist ein Ideal von $A$.
Denn zunächst stimmt der Kern von $f$ als Ringhomomorfismus mit dem von $f$ als Homomorfismus der additiven Gruppen überein, ist also eine Untergruppe der additiven Gruppe von $A$.
Wenn ferner $x \in Ker(f)$ und $a \in A$ ist, gilt
$f(ax) = f(a) \cdot f(x) = f(a) \cdot 0 = 0$, also $ax \in Ker(f)$.
b) Das Bild eines Ringhomomorfismus $f : A \longrightarrow B$ ist ein Unterring von

$B$ .
c) Die kanonische Abbildung $\kappa : \mathbb{Z} \longrightarrow \mathbb{Z}/m$ ist ein Ringhomomorfismus mit dem Kern $m\mathbb{Z}$.

**Satz: 6.27** *Sei $I$ ein Ideal des Ringes $A$. In der Faktorgruppe (der additiven Gruppen) $A/I$ kann man (auf kanonische Weise) eine Multiplikation $(A/I) \times (A/I) \longrightarrow A/I$ einführen, derart dass*
*1) $A/I$ ein Ring und*
*2) der kanonische Gruppenhomomorfismus $\kappa : A \longrightarrow A/I$ ein Ringhomomorfismus wird.*

**Beweis:** Die Vorschrift

$$(a \bmod I) \cdot (b \bmod I) := (ab \bmod I)$$

ist wohldefiniert. Seien nämlich $a \equiv a' \pmod I$ und $b \equiv b' \pmod I$. Dann ist $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$, da $a - a',\ b - b' \in I$ und $I$ ein Ideal ist. Es folgt $ab \equiv a'b' \pmod I$.

Die Ringgesetze in $A/I$ folgen unmittelbar aus ihrer Gültigkeit in $A$.

Offenbar ist $(1 \bmod I)$ ein neutrales Element für die Multiplikation in $A/I$.

Die Abbildung $\kappa : A \longrightarrow A/I,\ \ \kappa(a) = (a \bmod I)$ ist bekanntlich (6.14) ein Homomorfismus der additiven Gruppen. Nach der oben gegebenen Definition der Multiplikation in $A/I$ und weil $(1 \bmod I)$ die Eins in $A/I$ ist, ist $\kappa$ auch ein Ringhomomorfismus. □

**6.28** Sei $I$ ein Ideal von $\mathbb{Z}$. Dann ist $I = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$, und es ist $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m$.

**6.29 Satz** (Homomorfiesatz für Ringe): *Sei $f : A \longrightarrow B$ ein Ringhomomorfismus und $I$ ein Ideal von $A$ mit $I \subset Ker(f)$. Dann gibt es einen eindeutig bestimmten Ringhomomorfismus $g : A/I \longrightarrow B$ derart, dass das Diagramm*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\kappa"'] & & B \\ & A/I \arrow[ur, "g"'] & \end{tikzcd}$$

*kommutativ ist, d.h.* $f = g \circ \kappa$ *gilt. Hierbei ist* $\kappa$ *die kanonische Abbildung. Wenn* $I = Ker(f)$ *ist, ist* $g$ *injektiv. D.h. es gibt einen Isomorfismus* $A/Ker(f) \cong Im(f)$*.*

**Beweis:** Aus dem entsprechenden Satz und Beweis über abelsche Gruppen (6.21) wissen wir bereits, dass man $g(a \bmod I) = f(a)$ definieren muss und dass dies wohldefiniert ist. Ferner ist $g$ ein Homomorfismus für die additiven Gruppen und $f = g \circ \kappa$. Schließlich ist noch $g((a \bmod I) \cdot (b \bmod I)) = g(ab \bmod I) = f(ab) = f(a) \cdot f(b) =$
$g(a \bmod I) \cdot g(b \bmod I)$ und $g(1_A \bmod I) = f(1_A) = 1_B$, also $g$ ein Ringhomomorfismus. Das beweist den Satz. □

**Korollar: 6.30** *Seien* $m, n \in \mathbb{N}$, $m|n$. *Dann wird durch*

$$(a \ mod \ n) \longmapsto (a \ mod \ m)$$

*ein surjektiver Ringhomomorfismus*

$$\mathbb{Z}/n \longrightarrow \mathbb{Z}/m$$

*definiert.*

**Beweis:** Seien $\kappa : \mathbb{Z} \longrightarrow \mathbb{Z}/n$ und $\kappa' : \mathbb{Z} \longrightarrow \mathbb{Z}/m$ die kanonischen Homomorfismen. Nach 6.29 gibt es genau einen Homomorfismus $g : \mathbb{Z}/n \longrightarrow \mathbb{Z}/m$, so dass

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\kappa'} & \mathbb{Z}/m \\ {\scriptstyle\kappa}\searrow & & \nearrow{\scriptstyle g} \\ & \mathbb{Z}/n & \end{array}$$

kommutativ ist. Aus $g \circ \kappa = \kappa'$ folgt

$$g(a \bmod n) = g(\kappa(a)) = \kappa'(a) = (a \bmod m). \qquad \square$$

AUFGABEN UND HINWEISE

**1)** Seien $k \in \mathbb{Z}$ und $G$ eine abelsche Gruppe. Man betrachte die Abbildung $f_k : G \longrightarrow G,\ a \longmapsto ka$. Zeigen Sie:
a) $f_k$ ist ein Homomorfismus.
b) Wenn $\#G = m < \infty$ und $k$ zu $m$ teilerfremd ist, ist $f_k$ bijektiv.

**2)** Nach A1 b) gilt für eine abelsche Gruppe $G$ ungerader (endlicher) Ordnung: Jedes Element von $G$ ist von der Form $2a$, mit einem $a \in G$. Bemerkenswerterweise gilt dies auch für „nichtassoziative Gruppen“, sogenannte Loops.
Ein Loop ist eine Menge $L$ zusammen mit einer Verknüpfung

$$L \times L \longrightarrow L, \quad (a, b) \longmapsto ab,$$

für die folgendes gilt:
Zu jedem $a$ und jedem $b$ gibt es eindeutig bestimmte $x$ und $y$ mit

$$xa = ay = b.$$

Jede Gruppe ist natürlich ein Loop.

Wenn $M$ eine endliche Menge mit einer Verknüpfung ist, kann man eine vollständige Multiplikationstafel aufstellen:

| | $a$ | $b$ | $c$ | $\ldots$ |
|---|---|---|---|---|
| $a$ | $aa$ | $ab$ | $ac$ | $\ldots$ |
| $b$ | $ba$ | $bb$ | $bc$ | $\ldots$ |
| $c$ | $ca$ | $cb$ | $cc$ | $\ldots$ |
| . | . | . | . | $\ldots$ |
| . | . | . | . | $\ldots$ |
| . | . | . | . | $\ldots$ |

$M$ ist nun genau dann ein Loop, wenn in jeder Spalte und in jeder Zeile der Multiplikationstafel (der Produkte) von $M$ jedes Element von $M$ genau einmal steht. (Die erste Zeile z.B. in obiger Multiplikationstafel ist: $(aa, ab, ac, \ldots)$.) D.h. eine endliche Menge mit Verknüpfung ist ein Loop genau dann, wenn die Multiplikationstafel ein sogenanntes lateinisches Quadrat ist.
Ein Beispiel für ein kommutatives Loop ist $L = \{a, b, c\}$ mit der Tafel

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $b$ | $a$ | $c$ |
| $b$ | $a$ | $c$ | $b$ |
| $c$ | $c$ | $b$ | $a$ |

Prüfen Sie nach, dass $L$ nicht assoziativ ist.
Was bedeutet die Kommutativität eines Loops für seine Multiplikationstafel?
Die Aussage, die Sie beweisen mögen, lautet:
Sei $L$ ein endliches, kommutatives Loop mit ungerade vielen Elementen. Dann ist jedes Element von $L$ von der Form $xx$. (D.h. in der Multiplikationstafel steht in der Diagonale jedes Element mindestens einmal, also genau einmal.)
Dies lässt sich leicht beweisen, indem man überlegt, wie oft ein Element von $L$ überhaupt in der Multiplikationstafel auftritt und wie oft es außerhalb der Diagonale auftreten kann, wenn $L$ kommutativ ist.
Ein anderes Argument geht so: Zu $a \in A$ definiere eine Abbildung

$$\alpha : L \longrightarrow L\ ,\quad \alpha(x) = y\ ,\ \text{wenn}\ \ xy = a.$$

(Wegen der Loop–Eigenschaft ist $\alpha$ wohldefiniert.)
Zu zeigen ist: Es gibt ein $x$ mit $\alpha(x) = x$, d.h. es gibt einen sogenannten Fixpunkt von $\alpha$.
Da $L$ kommutativ ist, ist $\alpha^2 := \alpha \circ \alpha = id_L$, d.h. $\alpha$ ist eine sogenannte Involution auf $L$. Zu zeigen bleibt nun folgendes allgemeine Lemma (das auch in einer Aufgabe zu §12 eine Rolle spielen wird):

Ist $\alpha$ eine Involution auf einer endlichen Menge $M$ und $M^\alpha$ die Menge aller Fixpunkte, so gilt

$$\#M \equiv \#M^\alpha \pmod 2.$$

(Mit etwas Kenntnis über Operationen von Gruppen auf Mengen kann man allgemeiner zeigen: Wenn $\alpha^{p^n} = id_M$ mit $p \in \mathbb{P},\ n \in \mathbb{N}$ gilt, so ist

$$\#M \equiv \#M^\alpha \pmod p.$$

Vielleicht versuchen Sie, direkt zu zeigen: Die Menge $\{\alpha^r x \mid r \in \mathbb{N}\}$ hat unter o.a. Voraussetzung die Mächtigkeit $p^m$ mit einem $m \in \mathbb{N}$ .)

**3)** a) Seien $a \in \mathbb{Z},\ n \in \mathbb{N}_1$ und $p$ ein ungerader Primfaktor von $a^{2^n} + 1$.
Zeigen Sie: $p \equiv 1 \pmod{2^{n+1}}$ (*Euler*). (Vgl. 10. A4.)
(Hinweis: Bestimmen Sie die Ordnung von ($a$ mod $p$) in $(\mathbb{Z}/p)^*$.)
b) Seien $a, n \in \mathbb{N}_2$. Zeigen Sie: $n|\varphi(a^n - 1)$.

**4)** Zeigen Sie: Ist $G$ eine Gruppe von Primzahlordnung, so ist $G$ zyklisch.
(Sie dürfen voraussetzen, $G$ sei abelsch, obwohl dies nicht nötig ist.)

**5)** Lieber Leser, haben Sie schon ein Möbiusband gesehen? So sieht es aus:

Abb. 8 a)

Es lässt sich leicht aus einem länglichen rechteckigen Papierstreifen zusammenkleben:

Abb. 8 b)

(Kleben Sie die beiden Schmalseiten so zusammen, dass $a$ mit $a'$ und $b$ mit $b'$ zusammenfällt!)
Mathematisch gesehen, ist ein Möbiusband eine berandete nichtorientierbare Fläche im $\mathbb{R}^3$.
Und nun Ihre Aufgabe: Nehmen Sie einen rechteckigen Papierstreifen mit den Seitenlängen 1 und $n \in \mathbb{N}_1$. Teilen Sie diesen mit Bleistiftstrichen auf jeder Seite in $n$ Quadrate der Seitenlänge 1, so dass Sie insgesamt $2n$ Felder erhalten. Diese $2n$ Felder sollen mit den Elementen von $\mathbb{Z}/2n$ bezeichnet werden, verschiedene Felder mit verschiedenen Restklassen. Anschließend sollen Sie den Papierstreifen geeignet zusammenkleben. Dabei soll folgendes erreicht werden: Für jedes $k$ sollen die Restklassen ($k$ mod $2n$) und ($k+1$ mod $2n$) benachbarte Felder bezeichnen. (Ein kleiner Käfer soll vom Feld $\overline{k}$ zum Feld $\overline{k+1}$ gelangen können, indem er nur einen Bleistiftstrich – oder die Klebekante – überquert und vom Rande fernbleibt.)

Was bedeutet es für die Felder $\overline{m}$ und $\overline{m'}$, wenn $\lambda(\overline{m'}) = \lambda(\overline{m})$ für die „kanonische“ Abbildung (6.30)

$$\lambda : \mathbb{Z}/2n \longrightarrow \mathbb{Z}/n$$

gilt?
(Da der Papierstreifen „länglich“ sein sollte, darf $n$ nicht zu klein sein, oder die Quadrate müssen durch Rechtecke ersetzt werden.)

**6)** Äquivalenzrelationen und Äquivalenzklassen:
Seien $M$ eine Menge und $\sim$ eine (zweistellige) Relation auf dieser Menge; d.h.

für $a, b \in M$ gilt entweder „$a \sim b$“ oder „nicht $a \sim b$“, welch letzteres „$a \not\sim b$“ geschrieben wird. (Beispiele für Relationen sind $\equiv \pmod m$, $|$ , $\leq$.)

Definitionen: a) Die Relation $\sim$ heißt eine Äquivalenzrelation, wenn gilt:

(i) $a \sim a$ (für alle $a \in M$) (Reflexivität);

(ii) $a \sim b \Longrightarrow b \sim a$ (Symmetrie);

(iii) $a \sim b,\ b \sim c \Longrightarrow a \sim c$ (Transitivität).

(Äquivalent zu diesen Forderungen sind:

(i) $a \sim a$;

(ii') $a \sim b,\ a \sim c \Longrightarrow b \sim c$ (Komparativität).)

b) Eine Äquivalenzklasse bezüglich einer Äquivalenzrelation $\sim$ ist eine *nichtleere* Teilmenge $C \subset M$ mit folgenden beiden Eigenschaften:

(iv) $a, b \in C \Longrightarrow a \sim b$;

(v) $a \in C,\ b \in M, a \sim b \Longrightarrow b \in C$.

Sei nun $\sim$ eine Äquivalenzrelation auf $M$. Zeigen Sie:
Jedes Element von $M$ liegt in genau einer Äquivalenzklasse bezüglich $\sim$. Durch $a \longmapsto \{b \in M \mid a \sim b\}$ wird eine kanonische Abbildung

$$\kappa : M \longrightarrow M/\!\sim$$

definiert, wobei $M/\!\sim$ die Menge der Äquivalenzklassen bezüglich $\sim$ bezeichnet.
Zeigen Sie ferner:
Wenn $f : M \longrightarrow N$ eine beliebige Abbildung von Mengen ist, so wird durch

$$a \sim b :\Longleftrightarrow f(a) = f(b) \quad (\text{für } a, b \in M)$$

eine Äquivalenzrelation auf $M$ definiert.
Für *diese* Äquivalenzrelation gilt: Es gibt eine eindeutig bestimmte und injektive Abbildung

$$\varphi : M/\!\sim \longrightarrow N,$$

so dass das Diagramm

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\kappa}\searrow & & \nearrow{\scriptstyle\varphi} \\ & M/\sim & \end{array}$$

kommutativ ist.

**7)** Ein Kartenspiel für 2 Spieler: Sei $n \in \mathbb{N}_1$ und $M$ eine Teilmenge einer Gruppe mit $\#M = 2n$. Es seien $2n$ Spielkarten mit Namen der Elemente dieser Menge bezeichnet. Jeder Spieler erhält die Hälfte der Karten. Die Spieler spielen abwechselnd, indem jeder entweder eine Karte auf den Tisch rechts neben die dort eventuell schon liegenden Karten legt, oder indem er die aufliegenden Karten durch diejenige Karte ersetzt, die dem Produkt der aufliegenden Karten (in festgelegter Reihenfolge) entspricht. In letzterem Fall vermehrt er seine Karten – wenn es kein leeres Produkt ist. Verloren hat derjenige Spieler, der zuerst keine Karten mehr hat. Zeigen Sie, daß der anfangende Spieler verliert, wenn der zweite die richtige (Verhinderungs-)Strategie anwendet. (Die Menge $M$ ist beiden Spielern bekannt.)

# § 7

# Direkte Produkte, Chinesischer Restsatz

**Definition: 7.1** *Seien* $G_1, \ldots, G_n$ *(bzw.* $A_1, \ldots, A_n$*) endlich viele Gruppen (bzw. Ringe). Das direkte Produkt* $\prod_{i=1}^{n} G_i = G_1 \times \ldots \times G_n$ *(bzw.* $\prod_{i=1}^{n} A_i = A_1 \times \ldots \times A_n$*) ist als Menge das kartesische Produkt. Die Verknüpfungen* $+, \cdot$ *sind komponentenweise definiert:*

$$\begin{array}{lcrcl} (x_1, \ldots, x_n) & + & (y_1, \ldots, y_n) & := & (x_1 + y_1, \ldots, x_n + y_n), \\ (x_1, \ldots, x_n) & \cdot & (y_1, \ldots, y_n) & := & (x_1 \cdot y_1, \ldots, x_n \cdot y_n). \end{array}$$

*Bei additiv geschriebenen abelschen Gruppen schreibt man auch* $\bigoplus_{i=1}^{n} G_i = G_1 \oplus \ldots \oplus G_n$ *statt* $G_1 \times \ldots \times G_n$ *und spricht von direkter Summe.*

Man sieht sofort, dass $\prod_{i=1}^{n} G_i \left( \prod_{i=1}^{n} A_i \right)$ wieder eine Gruppe (ein Ring) ist. Das neutrale Elemente von $\prod_{i=1}^{n} G_i$ ist $(0_{G_1}, \ldots, 0_{G_n})$, wo $0_{G_i}$ das neutrale Element von $G_i$ bezeichnet, das multiplikativ neutrale Element von $\prod_{i=1}^{n} A_i$ ist

$(1_{A_1}, \ldots, 1_{A_n})$.

**Bemerkung: 7.2** Ein Ringhomomorfismus von $A$ nach $B$ ist insbesondere ein Homomorfismus für die additiven Gruppen der Ringe. Deshalb ist $f(0) = 0$. Hingegen folgt $f(1_A) = 1_B$ nicht allgemein aus $f(ab) = f(a) \cdot f(b)$. Z.B. erfüllt $f : A \longrightarrow A \times B,\ \ a \longmapsto (a, 0)$ die Eigenschaften (i) und (ii) von 6.25 a), aber nicht (iii), es sei denn, $B$ ist isomorf zum Nullring.

**Feststellung: 7.3** *Seien $f_1, \ldots, f_n$ Gruppen- (Ring-) Homomorfismen*

$$f_i : B \longrightarrow A_i,$$

*so erhält man auf kanonische Weise einen Gruppen- (Ring-) Homomorfismus*

$$(f_1, \ldots, f_n) :\ B \longrightarrow \prod_{i=1}^{n} A_i$$

*durch*

$$(f_1, \ldots, f_n)(x) := (f_1(x), \ldots, f_n(x))\,.$$

*Hierfür gilt:* $\mathrm{Ker}(f_1, \ldots, f_n) = \bigcap_{i=1}^{n} \mathrm{Ker} f_i$.

Dass dieses beides so ist, liegt an der Definition des direkten Produktes.

**7.4 Satz** (Chinesischer Restsatz, *Sun Tsu*, *Chhin Chiu–Shao*):
*Seien $m_1, \ldots, m_n \in \mathbb{N}_1$ paarweise teilerfremd. (D.h. für $i \neq j$ sei $ggT(m_i, m_j) = 1$.) Die kanonischen Homomorfismen*

$$\kappa_i : \mathbb{Z} \longrightarrow \mathbb{Z}/m_i$$

*induzieren auf kanonische Weise einen surjektiven Homomorfismus:*

$$\mathbb{Z} \longrightarrow \prod_{i=1}^{n} (\mathbb{Z}/m_i)$$

*und einen Isomorfismus*

$$G : \mathbb{Z}/m_1 \cdot \ldots \cdot m_n \xrightarrow{\cong} \prod_{i=1}^{n} (\mathbb{Z}/m_i).$$

**Beweis:** Betrachte den oben definierten Homomorfismus

$$F := (\kappa_1, \ldots, \kappa_n) : \mathbb{Z} \longrightarrow \prod_{i=1}^{n} (\mathbb{Z}/m_i).$$

Sein Kern besteht nach 7.3 aus allen $a \in \mathbb{Z}$, für die $m_1|a$, $m_2|a, \ldots$ und $m_n|a$ gilt. Dies ist aber (wegen 2.6) gleichbedeutend mit $m_1 \cdot \ldots \cdot m_n|a$, da die $m_i$ paarweise teilerfremd sind. Somit ist

$$\operatorname{Ker} F = m_1 \cdot \ldots \cdot m_n \mathbb{Z}.$$

Nach dem Homomorfiesatz (6.29) wird also durch $F$ ein *injektiver* Homomorfismus induziert:

$$G : \ \mathbb{Z}/m_1 \cdot \ldots \cdot m_n \longrightarrow \prod_{i=1}^{n} (\mathbb{Z}/m_i)$$

Da „Start" und „Ziel" von $G$ die gleiche endliche Anzahl von Elementen haben, nämlich $m_1 \cdot \ldots \cdot m_n$, ist $G$ auch surjektiv. Und hieraus folgt die Surjektivität der Abbildung $\mathbb{Z} \to \prod_{i=1}^{n} (\mathbb{Z}/m_i)$. □

**Korollar: 7.5** *Seien $m_1, \ldots, m_n$ paarweise teilerfremde ganze Zahlen $\neq 0$ und $a_1, \ldots, a_m \in \mathbb{Z}$ beliebig. Dann hat das Kongruenzsystem*

$$x \equiv a_i \pmod{m_i} \qquad (i = 1, \ldots, n)$$

*eine Lösung, d.h. es gibt ein $x \in \mathbb{Z}$, welches alle $n$ angegebenen Kongruenzen erfüllt. Die Lösung ist bis auf Kongruenz modulo $m_1 \cdot \ldots \cdot m_n$ eindeutig bestimmt.*

**Beweis:** Die Existenzaussage folgt aus der Surjektivität, die Eindeutigkeitsaussage aus der Injektivität der Abbildung $G$. □

Wie man die Lösung obigen Kongruenzsystems konkret und schnell berechnen kann, wird in A16 angegeben.

**Feststellung: 7.6** *Seien $A_1, \ldots, A_n$ Ringe. Ein Element $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$ ist genau dann eine Einheit in $A_1 \times \ldots \times A_n$, wenn jedes $a_i$ Einheit in $A_i$ ist. Mit anderen Worten:*

$$(A_1 \times \ldots \times A_n)^* = A_1^* \times \ldots \times A_n^*.$$

Dies liegt daran, dass die Multiplikation komponentenweise definiert ist.

**Korollar: 7.7** *Seien $m_1, m_2 \in \mathbb{N}_1$ zueinander teilerfremd. Dann ist*

$$\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2).$$

**Beweis:** Es ist

$$\mathbb{Z}/m_1m_2 \cong (\mathbb{Z}/m_1) \times (\mathbb{Z}/m_2),$$

also

$$(\mathbb{Z}/m_1m_2)^* \cong (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*.$$

Aus der Gleichheit der Elementezahlen letztgenannter Mengen folgt die Behauptung. □

**Korollar: 7.8** *Sei $m \in \mathbb{N}_1$ und $m = p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ die Primfaktorzerlegung von $m$ mit paarweise verschiedenen $p_1, \ldots, p_n$ und mit $r_i \geq 1$. Dann ist*

$$\varphi(m) = (p_1 - 1)p_1^{r_1-1} \cdot \ldots \cdot (p_n - 1)p_n^{r_n-1} = m \cdot \prod_{p \in \mathbb{P},\, p|m} \left(1 - \frac{1}{p}\right).$$

**Beweis:** Die erste Gleichung ergibt sich aus 4.24 d), wo $\varphi(p^r)$ berechnet wurde, und 7.7.
Die zweite Gleichung folgt aus $(p-1)p^{r-1} = p^r(1 - 1/p)$. □

**Bemerkung: 7.9** Die zweite Formel für $\varphi(m)$ benötigt offenbar etwas weniger Information über $m$ als die erste. (Man muss nur die Primzahlen kennen, die $m$ teilen, und braucht $v_p(m)$ nicht genauer zu bestimmen.) Bis heute ist kein schnelleres Verfahren, $\varphi(m)$ zu bestimmen, bekannt. Ist $m$ ein Produkt zweier verschiedener Primzahlen, so kann man aus $m$ und $\varphi(m)$ durch das Lösen einer quadratischen Gleichung diese Primfaktoren bestimmen. Wie?

**7.10** Wenn man beim Chinesischen Restsatz die multiplikative Struktur vergisst, erhält man das

**Korollar:** *Seien $G_1, \ldots, G_n$ endliche zyklische Gruppen mit paarweise teilerfremden Ordnungen. Dann ist $G_1 \times \ldots \times G_n$ zyklisch.*
*Wenn jeweils $z_i$ ein Erzeuger von $G_i$ ist, so ist $(z_1, \ldots, z_n)$ ein solcher von $G_1 \times \ldots \times G_n$ – und natürlich umgekehrt.*

**Beweis:** Wir haben Isomorfismen $g_i : \mathbb{Z}/m_i \xrightarrow{\cong} G_i$ mit $g_i(\overline{1}) = z_i$. Also gibt es einen Isomorfismus:

$$g : (\mathbb{Z}/m_1) \times \ldots \times (\mathbb{Z}/m_n) \xrightarrow{\cong} G_1 \times \ldots \times G_n,$$
$$g(a_1, \ldots, a_n) = (g_1(a_1), \ldots, g_n(a_n)) \,.$$

Diesen Isomorfismus verkette man mit dem Isomorfismus

$$f : \mathbb{Z}/m_1 \cdot \ldots \cdot m_n \xrightarrow{\cong} (\mathbb{Z}/m_1) \times \ldots \times (\mathbb{Z}/m_n),$$

für den $f(\overline{1}) = (\overline{1}, \ldots, \overline{1})$ gilt, und man erhält die Behauptungen. □

**Bemerkung: 7.11** Man kann die Sache auch vom anderen Ende her betrachten. Sei $G$ eine zyklische Gruppe mit $\#G = m_1 \cdot \ldots \cdot m_n$, wo die $m_i$ paarweise teilerfremde natürliche Zahlen sind. Dann ist $G \cong \mathbb{Z}/m_1 \cdot \ldots m_n \cong (\mathbb{Z}/m_1) \times \ldots \times (\mathbb{Z}/m_n)$. D.h. $G$ ist „direkt zerlegbar“ (auf nicht triviale Weise), wenn mindestens 2 der $m_i$ größer als 1 sind.

**Bemerkungen: 7.12** Sei $G_1 \times G_2$ ein direktes Produkt zweier abelscher Gruppen $G_1, G_2$. Dann ist $G_1 \times \{0\} = \{(x, 0) \mid x \in G_1\}$ eine zu $G_1$ isomorfe Untergruppe von $G_1 \times G_2$. Ferner ist die Projektion $p_2 : G_1 \times G_2 \longrightarrow G_2 \quad (x, y) \longmapsto y$ ein surjektiver Homomorfismus mit dem Kern $G_1 \times \{0\}$. Nach dem Homomorfiesatz erhält man die Isomorfie $(G_1 \times G_2)/(G_1 \times \{0\}) \cong G_2$. Die beiden Untergruppen $G_1 \times \{0\}$ und $\{0\} \times G_2$ haben die Eigenschaften $(G_1 \times \{0\}) \cap (\{0\} \times G_2) = \{0_{G_1 \times G_2}\}, \quad (G_1 \times \{0\}) + (\{0\} \times G_2) = G_1 \times G_2$.

Hiervon gibt es eine Umkehrung:

**Lemma: 7.13** *Seien $H_1, H_2$ Untergruppen einer abelschen Gruppe $G$ mit*

$$H_1 \cap H_2 = \{0\}, \quad H_1 + H_2 = G.$$

*Dann ist $G \cong H_1 \times H_2$. Genauer gilt: Die Abbildung*

$$f : H_1 \times H_2 \longrightarrow G, \quad (a, b) \longmapsto a + b$$

*ist ein Isomorfismus.*

**Beweis:** Offenbar ist $f$ ein Homomorfismus. Aus $H_1 + H_2 = G$ folgt, dass $f$ surjektiv ist.
Die Injektivität von $f$ erhält man aus $H_1 \cap H_2 = \{0\}$ wie folgt: Seien $a \in H_1$, $b \in H_2$ und $(a,b) \in \mathrm{Ker}(f)$, d.h. $a + b = f(a,b) = 0$. Dann ist $a = -b \in H_2$, somit $a \in H_1 \cap H_2$. Deshalb ist $a$ und damit $b$ gleich Null. $\mathrm{Ker}(f) = \{0\}$ heißt aber, dass $f$ injektiv ist. □

**Satz: 7.14** *Seien $G$ eine endliche abelsche Gruppe, $H$ eine Untergruppe, so dass folgendes gilt:*
*1) $ggT(\#H, [G : H]) = 1$, 2) $H$ und $G/H$ sind zyklisch.*

*a) Dann ist $G$ zu $H \times (G/H)$ isomorf, also zyklisch.*
*b) Ein Element $z \in G$ ist ein Erzeuger von $G$ genau dann, wenn $(z \bmod H)$ ein solcher von $G/H$ und $[G : H] \cdot z$ ein solcher von $H$ ist.*
(Dieser Satz wird nur in §9 gebraucht.)

**Beweis:** a) Es genügt, folgendes zu zeigen:
*Behauptung:* In $G$ existiert ein Element $x$ der Ordnung $[G : H]$.
Wenn dies richtig ist, gilt nämlich für $H' := \langle x \rangle$ zunächst $H \cap H' = \{0\}$. Denn die Ordnung der Gruppe $H \cap H'$ teilt die beiden teilerfremden Zahlen $\#H$ und $\#H' = [G : H]$. Nach 7.13 ist deshalb $H + H'$ zu $H \times H'$ isomorf, hat also $\#H \cdot [G : H] = \#G$ Elemente und muss deshalb schon die ganze Gruppe $G$ sein. D.h. es ist
$G = H + H' \cong H \times H'$. (Offenbar ist $H' \cong G/H$.)

Da $H$ und $H' \cong G/H$ zyklisch von teilerfremden Ordnungen sind, ist $G$ zyklisch nach 7.10.

*Beweis der Behauptung*: Sei $x' \in G$ so gewählt, dass $\overline{x'} = x' + H$ ein Erzeuger der zyklischen Gruppe $G/H$ ist. Mit $m := [G/H]$ gilt $m\overline{x'} = \overline{0}$, d.h. $z := mx' \in H$.

Da $m$ zu $\#H$ teilerfremd ist, gibt es ein $m' \in \mathbb{Z}$ mit $m'm \equiv 1 \pmod{\#H}$, also $mm'z = z$ wegen $z \in H$.

Wir behaupten: $x := x' - m'z$ hat die Ordnung $m = [G : H]$.

Denn $mx = mx' - mm'z = mx' - z = 0$, also $\mathrm{ord}\,(x) | m$. Da andererseits $x + H = x' + H$ ist, also $m$ die kleinste positive ganze Zahl mit $mx \in H$ ist, ist $kx \neq 0$ für $1 \leq k \leq m - 1$, d.h. $\mathrm{ord}(x) = m$.

b) „$\Longrightarrow$“ Nach 6.16 ist $(z \bmod H)$ ein Erzeuger von $G/H$, und nach 5.14 ist $[G:H]\cdot z$ ein solcher von $H$.
„$\Longleftarrow$“ Da $G/H$ von $(z \bmod H)$ erzeugt wird, sind $z+H$, $2z+H, \ldots, [G:H]\cdot z+H = H$ die Nebenklassen nach $H$. Ihre Vereinigung ist $G$. Da nach Voraussetzung jedes Element von $H$ ein Vielfaches von $[G:H]\cdot z$ ist, ist jedes Element von $G$ von der Form

$$k\cdot z + m\cdot[G:H]\cdot z = n\cdot z$$

mit gewissen $k,m,n\in\mathbb{Z}$. D.h. $z$ ist ein Erzeuger von $G$. □

**Satz: 7.15** *Seien $G_1,\ldots,G_n$ endliche abelsche Gruppen der Ordnungen $m_1,\ldots,m_n$. Wenn $G_1\times\ldots\times G_n$ zyklisch ist, so ist auch jedes $G_i$ zyklisch, und die $m_1,\ldots,m_n$ sind paarweise teilerfremd.*

**Beweis:** Die $G_i$ sind isomorf zu Untergruppen von $G_1\times\ldots\times G_n$ (vgl. 7.12), also zyklisch nach 5.14.
Sei jetzt $i,j\in\{1,\ldots,n\}$, $i\neq j$. Dann ist auch $G_i\times G_j$ isomorf zu einer Untergruppe von $G_1\times\ldots\times G_n$, also zyklisch. Sei $d := \mathrm{ggT}(m_i,m_j)$ und $k := \dfrac{m_i\cdot m_j}{d}$ (das sogenannte kleinste gemeinsame Vielfache). Dann ist

$$k\cdot(a,b) = \left(\frac{m_j}{d}m_i a,\ \ \frac{m_i}{d}m_j b\right) = (0,0) = 0$$

für alle $a\in G_i$, $b\in G_j$. Ein Erzeuger $z$ von $G_i\times G_j$ hat aber die Ordnung $m_i\cdot m_j$. Es folgt $m_i\cdot m_j \,\Big|\, \dfrac{m_i m_j}{d}$, also $d=1$. □

**Korollar: 7.16** *Sei $p\in\mathbb{P}$, $n\in\mathbb{N}_1$. Dann ist die additive Gruppe von $\mathbb{Z}/p^n$, also erst recht der Ring $\mathbb{Z}/p^n$ nicht direkt zerlegbar. D.h. wenn $\mathbb{Z}/p^n\cong G_1\times G_2$ mit abelschen Gruppen $G_i$ ist, so ist $G_1$ oder $G_2$ trivial, d.h. besteht nur aus einem Element.*

**Beweis:** Andernfalls müsste es teilerfremde ganze Zahlen $m_1,m_2>1$ mit $m_1\cdot m_2 = p^n$ geben. □

**Korollar: 7.17** *Sind $m_1,m_2\in\mathbb{N}_1$ nicht teilerfremd, so gibt es keinen surjektiven Gruppenhomomorfismus*

$$f:\mathbb{Z}\longrightarrow\mathbb{Z}/m_1\times\mathbb{Z}/m_2.$$

**Beweis:** Einerseits ist $f(\mathbb{Z}) \cong \mathbb{Z}/\mathrm{Ker}(f)$ zyklisch, andererseits $\mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ nicht zyklisch. □

## AUFGABEN UND HINWEISE

**1)** Drei Busse fahren jeder auf einer Rundstrecke. Die erste Rundstrecke habe 24, die zweite 31 und die dritte 35 Stationen. Jeder Bus benötigt von jeder Station zur nächsten (genau) 2 Minuten Fahrzeit und hält an jeder Station (genau) $\frac{1}{2}$ Minute lang. Die drei Rundstrecken haben zwei Stationen $A$ und $B$ gemeinsam.
Frage: Ist es bei entsprechendem Streckennetz möglich, dass die drei Busse gleichzeitig in der Station $A$ starten, aber nie gleichzeitig in der Station $B$ halten?

**2)** Zwei Zahnräder mit $m$ bzw. $n$ Zähnen greifen ineinander. Geben Sie eine – hinreichende und notwendige – Bedingung an das Zahlenpaar $(m, n)$ dafür an, dass nach genügend vielen Umdrehungen jeder Zahn des ersten Rades in jede „Zahnlücke“ des anderen Rades gegriffen hat.

Abb. 9

**3)** Betrachten Sie eine Torusfläche (Oberfläche eines Fachrradschlauches). Zerlegen Sie diese durch $n$ „Breiten–" und $m$ „Längenkreise" in $n \cdot m$ Karos.

Abb. 10

Denken Sie sich den Torus als Schachbrett mit den Karos als Feldern. (Die auf normalen Schachbrettern übliche Schwarz–Weiß–Färbung der Felder ist nur dann möglich, wenn $m$ und $n$ beide gerade sind.) Seien nun $n, m$ teilerfremd. Zeigen Sie:
Wenn auf diesem exotischen Schach„brett" außer den beiden Königen nur noch ein weißer Läufer steht, ist der schwarze König matt. (D.h. der Läufer bedroht jedes Feld, wenn höchstens noch eine weitere Figur auf dem „Brett" steht.)

**4)** Man kann sich eine kompliziertere Karierung des Torus vorstellen: $n$ ausgezeichnete Breitenkreise, aber eine geschlossene Kurve $C$, die – leicht schräg zu den Längenkreisen – jeden Breitenkreis $m$–mal schneidet. (Sie „schraubt" sich um den Torus $m$–mal herum. Auf dem entstehenden Karomuster bedroht ein Turm jedes Feld.)
Bezeichnen Sie die $m \cdot n$ Karos so mit den Elementen von $\mathbb{Z}/mn$, dass man von

($k$ mod $mn$) zu ($k+1$ mod $mn$) durch Überschreiten eines der ausgezeichneten Breitenkreise gelangt, ohne $C$ zu überqueren. Bei dem kanonischen Ringhomomorfismus

$$\mathbb{Z}/mn \longrightarrow \mathbb{Z}/n$$

haben zwei Elemente das gleiche Bild genau dann, wenn die entsprechenden Felder zwischen denselben Breitenkreisen liegen. Vgl. 6. A5.

**5)** Ein Element $e$ eines Ringes $A$ heißt idempotent, wenn $e^2 = e$ ist. Zeigen Sie:
a) Wenn $e$ idempotent ist, dann auch $1 - e$.
b) In einem direkten Produkt von Ringen $A_1 \times A_2$ sind (1,0) und (0,1) idempotent.
c) Wenn $e \in A$ idempotent ist, gibt es einen Isomorfismus
$f : A_1 \times A_2 \xrightarrow{\cong} A$ mit $f(1,0) = e$. Ferner sind die Ideale $f(A_1 \times 0)$ und $f(0 \times A_2)$ von $A$ durch $e$ eindeutig bestimmt. Ist $e = 1$ bzw. $e = 0$, so ist $A_2$ bzw. $A_1$ isomorf zum Nullring $\mathbb{Z}/1$.

**6)** Finden Sie alle Lösungen des Zahlenrätsels

$$CHINA \cdot CHINA = *****CHINA.$$

Die Buchstaben sind durch Ziffern des Dezimalsystems zu ersetzen (gleiche Buchstaben durch gleiche Ziffern), die Sternchen durch beliebige Ziffern. Die Zahlen dürfen mit Nullen beginnen. Z.B. ist

$$00000 \cdot 00000 = 0000000000$$

eine Lösung. Die Lösungen sollten nicht durch Probieren gefunden werden, sondern mit Hilfe von A5 und Sätzen dieses Paragrafen. Ihre Methode sollte im Prinzip auf Darstellungen in jedem $d$–adischen Ziffernsystem anwendbar sein. Für $d = 7$ z.B. sollten Sie die Lösungen ohne weiteres Rechnen sofort angeben können.

**7)** Finden Sie eine natürliche Zahl, welche bei der Division durch 6, 5, 4, 3 die Reste 5, 4, 3, 2 lässt (*Brahmagupta*).

**8)** Es gibt eine Verallgemeinerung des Chinesischen Restsatzes auf allgemeine (kommutative) Ringe. Vgl. z.B. [*Brüske, Ischebeck, Vogel*], 1.9 und viele andere Bücher über (kommutative) Algebra.

**9) a)** Zeigen Sie, dass die nach dem „Spiel“ aus 4.A6 übrigbleibende Zahl modulo 30 eindeutig bestimmt ist.

**b)** Sei $p > 3$ eine Primzahl. Zeigen Sie $n^p \equiv n \pmod{6p}$ für jede ganze Zahl $n$.

**10)** a) Für welche $n$ ist $\varphi(n)$ ungerade?
b) Gibt es etwa nur endlich viele $n$, für welche $\varphi(n)$ nicht durch 3 teilbar ist? (4.28)
c) Für welche $n$ ist $\varphi(n) = 2$ ?

**11)** a) Zeigen Sie: Für alle $n \in \mathbb{N}_1$ ist $\varphi(n) > \frac{1}{2}\sqrt{n}$.
(Hinweis: Für ungerade $n$ ist sogar $\varphi(n) \geq \sqrt{n}$. Wenden Sie 7.8 an.)
b) Folgern Sie: $\lim_{n\to\infty} \varphi(n) = \infty$.
Mit anderen Worten: Zu $a \in \mathbb{N}$ gibt es nur endlich viele $n \in \mathbb{N}_1$ mit $\varphi(n) \leq a$.

**12)** Seien $m, n \in \mathbb{N}_1$. Zeigen Sie: Die kanonische Abbildung (vgl. 9.9 Beweis)

$$(\mathbb{Z}/mn)^* \longrightarrow (\mathbb{Z}/m)^*$$

ist surjektiv.
(Dies folgt ziemlich direkt aus der Zerlegung von $\mathbb{Z}/mn$ in Faktoren der Form $\mathbb{Z}/p^r$. Ein mehr „rechnerischer“ Beweis geht so:
Schreiben Sie $n = n_1 n_2$, so dass jeder Primfaktor von $n_1$ auch ein solcher von $m$ ist und dass $n_2$ zu $m$ teilerfremd ist. Betrachten Sie die Abbildungen

$$(\mathbb{Z}/mn)^* \longrightarrow (\mathbb{Z}/mn_1)^* \longrightarrow (\mathbb{Z}/m)^*$$

gesondert. Man kann $n_1$ ohne Primfaktorzerlegung durch iteriertes Berechnen von ggT's bestimmen. Wie?)

**13)** Eine natürliche Zahl heißt quadratfrei, wenn sie nicht durch das Quadrat einer Primzahl teilbar ist.

Zeigen Sie: Ist $m \in \mathbb{N}_2$ quadratfrei, so gilt $a^{\varphi(m)+1} \equiv a \pmod{m}$ für *alle* $a \in \mathbb{Z}$. Diese Kongruenz gilt sogar modulo $6m$, wenn alle Primfaktoren von

$m$ größer als 3 sind; vgl. A9.

**14)** Zeigen Sie folgende Verallgemeinerung von 3.3: Es gibt beliebig große Lücken zwischen aufeinanderfolgenden quadratfreien Zahlen.

(Gehen Sie davon aus, dass der Beweis nicht allzu schwer, aber verschieden von dem für 3.3 ist, und den Chinesischen Restsatz benutzt.)

**15)** Sei $G$ eine (additiv geschriebene) abelsche Gruppe der Ordnung $m = p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ mit verschiedenen Primzahlen $p_i$, und $r_i \in \mathbb{N}_1$. Ferner sei definiert:

$$G_i \;:=\; \{x \in G \,|\, p_i^{r_i} x = 0\}.$$

Zeigen Sie:

a) Jedes $G_i$ ist eine Untergruppe von $G$.

b) Es gibt einen naheliegenden Isomorfismus

$$f : \bigoplus_{i=1}^{n} G_i \longrightarrow G$$

(Für die Injektivität kann man A1, für die Surjektivität 7.4 benutzen.)

Insbesondere erhält man $\#G_i = p_i^{r_i}$.

c) Gibt es zu jedem $i = 1, \ldots, n$ höchstens $p_i^{r_i - 1}$ Elemente $x \in G$ mit $p_i^{r_i - 1} = 0$, so sind alle $G_i$ und damit auch $G$ zyklisch. Vgl. 6.8.

**16)** Auf folgende Weise kann man ein Kongruenzsystem zu paarweise teilerfremden Moduln lösen. Mit den Bezeichnungen von 7.5 setze man $M := \prod_{i=1}^{n} m_i$ und $m_i' := M/m_i$. Dann ist $m_i$ zu $m_i'$ teilerfremd, und somit gibt es $x_i \in \mathbb{Z}$ mit $m_i' x_i \equiv a_i \pmod{m_i}$. Für $j \neq i$ ist hingegen $m_i' x_i \equiv 0 \pmod{m_j}$. Also erfüllt

$$x := \sum_{i=1}^{n} m_i' x_i$$

das Kongruenzsystem aus 7.5.

**17)** Der große Fritz stellte dem kleinen Moritz die Aufgabe, die Primfaktorzerlegung der Zahl 1040519177 zu finden. Er glaubte, auf diese Weise eine Weile Ruhe vor ihm zu haben; denn Maple und Mathematica gab es noch nicht. Leider hatte er sich vom kleinen Moritz überreden lassen, den Wert der $\phi$-Funktion dieser Zahl zu verraten. Und so dauerte seine Ruhe nicht lange. (Moritz besaß eine Primzahltafel und Fritz hatte sich auf zwei Primfaktoren beschränkt.)

*In den folgenden Aufgaben sollen Sie die grundlegenden Aussagen über die zahlentheoretischen Funktionen beweisen. Diese sind Abbildungen:*

$$f : \mathbb{N}_1 \longrightarrow \mathbb{C}.$$

*Sie sind für die analytische Zahlentheorie wichtig.*

**18)** a) Seien $f$, $g$ zahlentheoretische Funktionen und $a \in \mathbb{C}$, so definiert man

$$(f+g)(n) := f(n) + g(n) \text{ und } (af)(n) = a(f(n)).$$

Auf diese Weise wird die Menge $\mathcal{Z}$ der zahlentheoretischen Funktionen zu einem (unendlichdimensionalen) $\mathbb{C}$–Vektorraum.

b) Wir definieren eine Multiplikation „$*$“, die sogenannte Faltung (oder das Dirichlet-Produkt) auf $\mathcal{Z}$ wie folgt:

$$(f * g)(n) := \sum_{ab=n} f(a)g(b) = \sum_{a|n} f(a)g(n/a)$$

Dabei seien $a$, $b$ Variable für natürliche Zahlen.

Zeigen Sie: $\mathcal{Z}$ zusammen mit „$+$“ und „$*$“ ist ein kommutativer Ring.

(Die neutralen Elemente sind die Nullfunktion 0 und die Funktion $\varepsilon$, definiert durch $\varepsilon(1) = 1$, $\varepsilon(n) = 0$ für $n \in \mathbb{N}_2$. Zur Assoziativität der Multiplikation zeige man

$$f * (g * h)(n) = \textstyle\sum_{abc=n} f(a)g(b)h(c)\,).$$

c) Zeigen Sie: $\mathcal{Z}$ ist nullteilerfrei.

(Seien $a$ und $b$ minimal in $\mathbb{N}_1$ mit $f(a) \neq 0$, bzw. $g(b) \neq 0$. Dann ist $(f * g)(ab) = f(a)g(b)$.)

**19)** (Diese Aufgabe können Sie überschlagen.)

Im folgenden Paragrafen werden Polynome als unendliche formale Summen

$$\sum_{i=0}^{\infty} a_i X^i$$

eingeführt, wobei $a_i = 0$ bis auf endlich viele $i$ sein soll. Wenn man auf diese letzte Bedingung verzichtet, also $a_i \neq 0$ auch für unendlich viele $i$ zulässt, spricht man von einer formalen Potenzreihe. (Das Adjektiv „formal" wird verwendet, da von Konvergenz nicht die Rede ist. Eine formale Potenzreihe definiert i.a. keine Funktion.) Die formalen Potenzreihen über einem Ring $A$ bilden mit der in 8.4 definierten Addition und Multiplikation ebenfalls einen Ring $A[[X]]$.

Man kann auch Potenzreihen in mehreren, ja unendlich vielen Variablen betrachten.

Zeigen Sie: Der formale Potenzreihenring $\mathbb{C}[[X_i \mid i \in \mathbb{N}_1]]$ in abzählbar unendlich vielen Variablen ist isomorf zum oben definierten Ring $\mathcal{Z}$.

(Sei $p_n$ die $n$-te Primzahl. Man ordne der zahlentheoretischen Funktion $f$ die Potenzreihe

$$\sum f(p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}) X_1^{r_1} \cdot X_2^{r_2} \cdot \ldots \cdot X_m^{r_m} \quad \text{zu.}$$

„Summiert" wird über alle „endlichen" Monome.)

**20)** Seien $f$, $g \in \mathcal{Z}$ und $s \in \mathbb{C}$ so, dass die beiden Reihen (sog. Dirichletreihen)

$$\sum_{n=1}^{\infty} f(n)/n^s \text{ und } \sum_{n=1}^{\infty} g(n)/n^s$$

absolut konvergieren mit den Grenzwerten $F$ bzw. $G$.

Zeigen Sie: Dann konvergiert

$$\textstyle\sum_{n=1}^{\infty} (f * g)(n)/n^s \text{ gegen } FG.$$

**21)** Zeigen Sie: Eine zahlentheoretische Funktion $f$ ist genau dann eine Einheit in $\mathcal{Z}$, wenn $f(1) \neq 0$ ist.

(Um die bezüglich „$*$“ inverse Funktion $g$ zufinden, bestimmen Sie zunächst $g(1)$. Dann kann man $g(n)$ aus den $g(d)$ mit den echten Teilern $d$ von $n$ errechnen.)

**22)** Sei $\iota_0$ die durch $\iota_0(n) = 1$ für alle $n \in \mathbb{N}_1$ definierte (konstante) zahlentheoretische Funktion. Für $f \in \mathcal{Z}$ ist dann

$$(\iota_0 * f)(n) = \textstyle\sum_{a|n} f(a).$$

Man nennt $Sf := \iota_0 * f$ auch die summatorische Funktion von $f$. Es ist $S\varepsilon = \iota_0$ und $S\varphi = id_{\mathbb{N}_1}$ gemäß 5.16.

Die Möbiusfunktion $\mu$ ist definiert als die zu $\iota_0$ bezüglich „$*$“ inverse zahlentheoretische Funktion. Natürlich ist

$$\mu * (Sf) = f, \text{ d.h. } \sum_{a|n} \mu(n/a) Sf(a) = f$$

(Möbiussche Umkehrformel), ferner

$$\sum_{a|n} \mu(a) = \begin{cases} 1 & \text{für} \quad n = 1 \\ 0 & \text{sonst} \end{cases} \qquad \text{und} \ \ \mu(1) = 1.$$

Zeigen Sie für eine Primzahl $p$ :

a) $\mu(p) = -1$,
b) $\sum_{i=0}^{j} \mu(p^i) = 0$ für $j \geq 1$
c) $\mu(p^j) = 0$ für $j \geq 2$.
Wie man $\mu(n)$ aus einer Primfaktorzerlegumg von $n$ berechnen kann, sollen Sie in A25 zeigen.

**23)** Seien $m, n \in \mathbb{N}_1$ zueinander teilerfremd. Zeigen Sie: Zu jedem Teiler $d > 0$ von $mn$ gibt es eindeutig bestimmte $a, b \in \mathbb{N}_1$ mit

$$d = ab, \quad a \mid m, \quad b \mid n.$$

(Natürlich sind dann auch $a$, $b$ zueinander teilerfremd.)

**24)** Eine zahlentheoretische Funktion $f$ heißt multiplikativ, wenn

$$f(1) = 1 \text{ und } f(mn) = f(m)f(n) \text{ für } \textit{teilerfremde } m,\ n$$

gilt. Sie heißt streng multiplikativ, wenn

$$f(1) = 1 \text{ und } f(mn) = f(m)f(n) \text{ für } \textit{alle } m,\ n$$

gilt.

Die Eulersche Funktion $\varphi$ ist multiplikativ, die Funktionen $\varepsilon$ und $\iota_0$ sind sogar streng multiplikativ.

Eine multiplikative Funktion ist durch ihre Werte auf den Primzahlpotenzen, eine streng multiplikative Funktion schon durch ihre Werte auf den Primzahlen bestimmt.

Zeigen Sie: Die multiplikativen zahlentheoretischen Funktionen bilden eine Untergruppe der Einheitengruppe $\mathcal{Z}^*$ von $\mathcal{Z}$.

(Seien $f$, $g$ multiplikativ. Zeigen Sie die Multiplikativität von $f * g$ mit A23. Sei $h$ bezüglich „$*$" zu $f$ invers. Definieren Sie

$$h'(p_1^{r_1} \cdot \ldots \cdot p_m^{r_m}) := h(p_1^{r_1}) \cdot \ldots \cdot h(p_m^{r_m}).$$

für verschiedene Primzahlen $p_1, \ldots, p_m$. Zunächst sieht man $h' * f = \varepsilon$ , d.h. $h' = h$ für Primzahlpotenzen. Aber man weiß, dass $h' * f$ multiplikativ ist.)

**25)** Da Sie jetzt wissen, dass $\mu$ multiplikativ ist, können Sie $\mu(n)$ aus der Primfaktorzerlegung von $n$ berechnen.

Obwohl $\iota_0$ sogar streng multiplikativ ist, gilt dies nicht für die inverse Funktion $\mu$. Auch ist die Faltung streng multiplikativer Funktionen nicht immer streng multiplikativ.

**26)** Bestimmen Sie die letzten 100 Stellen von $1997^{1997!}$ im Dezimalsystem. Wieviele weitere Stellen können Sie noch ganz einfach bestimmen?

# § 8

# Polynomringe, $(\mathbb{Z}/p)^*$

*Sei im folgenden $A$ ein Ring.*

**Definition: 8.1** *Ein Polynom über $A$ in einer „Unbestimmten" $X$ ist ein „Ausdruck"*

$$a_0 + a_1 X + a_2 X^2 \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{\infty} a_i X^i$$

*mit $a_i \in A$, wo $a_i = 0$ für $i > n$ ist.*
*Das heißt, formal gesehen ist ein Polynom eine Folge $(a_0, a_1, a_2, \ldots) = (a_i)_{i \in \mathbb{N}}$ mit der Eigenschaft $a_i = 0$ für „fast alle $i$", d.h. für alle $i \in \mathbb{N}$ mit nur endlich vielen Ausnahmen.*

*Insbesondere gilt $\sum\limits_{i=0}^{\infty} a_i X^i = \sum\limits_{i=0}^{\infty} b_i X^i$ genau dann, wenn $a_i = b_i$ für alle $i$ ist.*

*Die $a_i$ heißen die Koeffizienten des Polynoms $\sum\limits_{i=0}^{\infty} a_i X^i$.*

**Bemerkung: 8.2** Jedes Polynom $f := \sum\limits_{i=0}^{\infty} a_i X^i$ definiert eine Abbildung:

$$A \longrightarrow A, \quad b \longmapsto \sum_{i=0}^{\infty} a_i b^i =: f(b).$$

Wenn nun etwa $A$ endlich ist, aber aus mindestens 2 Elementen besteht, gibt es einerseits nur endlich viele Abbildungen $A \longrightarrow A$, nämlich $(\#A)^{\#A}$ viele, andererseits unendlich viele Polynome. In diesem Falle definieren mehrere Polynome dieselbe Abbildung. Man darf also Polynome über $A$ nicht mit Abbildungen $A \longrightarrow A$ identifizieren.

Anders ausgedrückt, die Gleichheit zweier polynomialer Abbildungen – als Abbildungen – gibt nicht das Recht zum „Koeffizientenvergleich".

**8.3** *Mit $A[X]$ wird die Menge aller Polynome über $A$ in der Unbestimmten $X$ bezeichnet. $A[X]$ heißt der Polynomring über $A$ (in einer Unbestimmten).*

**Feststellung: 8.4** *$A[X]$ wird zu einem Ring, wenn man Addition und Multiplikation „wie üblich" definiert:*

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i,$$

$$\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) := \sum_{k=0}^{\infty} \left( \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k.$$

*(Dabei sind $a_i + b_i$ und $\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j$ durch die Verknüpfungen in $A$ definiert.)*
*Die neutralen Elemente sind gegeben durch:*

$$\sum_{i=0}^{\infty} a_i X^i = 0 \iff a_i = 0 \quad \textit{für alle} \quad i$$

$$\sum_{i=0}^{\infty} a_i X^i = 1 \iff a_0 = 1, \quad a_i = 0 \quad \textit{für alle} \quad i \geq 1.$$

Der Beweis ist einfach und ein wenig langweilig. Er wird dem Leser überlassen.

**Feststellung: 8.5** *Seien* $f, g \in A[X]$, $b \in A$. *Dann ist*
$(f+g)(b) = f(b) + g(b)$ *und* $(fg)(b) = f(b)g(b)$. *(Siehe 8.2 zur Definition von* $f(b)$.*) Mit anderen Worten: Die Abbildung*
$A[X] \longrightarrow A, \quad f \longmapsto f(b)$ *ist ein Ringhomomorfismus.*

**Beweis:** Addition und Multiplikation in $A[X]$ sind gerade so definiert, dass dies gilt. □

**Definition: 8.6** *Sei* $f = \sum_{i=0}^{\infty} a_i X^i \in A[X]$. *Wir definieren* grad*(*$f$*), den Grad von* $f$*, durch*

$$\begin{array}{rcl} \mathrm{grad}(0) & = & -\infty \quad \textit{und} \\ \mathrm{grad}(f) & = & \mathrm{Max}\,\{i \in \mathbb{N} | a_i \neq 0\} \quad \textit{für} \quad f \neq 0. \end{array}$$

*Wenn* $\mathrm{grad}(f) = n \geq 0$ *ist, heißt* $a_n$ *der Leitkoeffizient (oder der höchste Koeffizient) von* $f$.

**Feststellung: 8.7** *Seien* $f, g \in A[X]$ *(und* $A$ *nicht isomorf zum Nullring).*
*a)* *Es ist* $\mathrm{grad}(fg) \leq \mathrm{grad}(f) + \mathrm{grad}(g)$. *(Hierbei wird definiert:*
$n - \infty = -\infty + n = -\infty$ *und* $-\infty \leq n$ *für alle* $n \in \mathbb{N} \cup \{-\infty\}$.*)*
*b)* *Wenn* $f \neq 0$ *und der Leitkoeffizient von* $f$ *kein Nullteiler in* $A$ *ist, gilt sogar:* $\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g)$. *In diesem Falle ist (wenn auch* $g \neq 0$ *ist) der Leitkoeffizient von* $fg$ *das Produkt der Leitkoeffizienten von* $f$ *und von* $g$.
*c)* *Wenn* $A$ *ein Integritätsring – etwa ein Körper – ist, dann ist auch* $A[X]$ *ein Integritätsring.*
*d)* $\mathrm{grad}(f \pm g) \leq \mathrm{Max}\{\mathrm{grad}\, f, \mathrm{grad}\, g\}$.
*e)* *Wenn* $\mathrm{grad}\, f \neq \mathrm{grad}\, g$ *ist, gilt*
$\mathrm{grad}(f \pm g) = \mathrm{Max}\{\mathrm{grad}\, f, \mathrm{grad}\, g\}$.

Der einfache Beweis wird dem Leser überlassen.

**Bemerkung: 8.8** Die Polynome vom Grad $\leq 0$, die „konstanten" Polynome, bilden einen Unterring von $A[X]$, der zu $A$ isomorf ist.
*Wir fassen* $A$ *auf kanonische Weise als diesen Unterring auf.*

**8.9 Satz** (Division mit Rest):
*Seien $f, g \in A[X]$. Der Leitkoeffizient von $f$ sei eine Einheit in $A$. Dann gibt es eindeutig bestimmte $q, r \in A[X]$ mit*
1) $g = f \cdot q + r$,
2) $\mathrm{grad}(r) < \mathrm{grad}(f)$.

**Beweis:** a) Zur Existenz von $q$ und $r$: Es ist $g = f \cdot 0 + g$, also die Menge $\{r' \in A[X] \mid \exists q' \in A[X] \text{ mit } g = fq' + r'\}$ nicht leer. Wähle aus ihr ein $r$ von kleinstmöglichem Grad. (Jede nichtleere Teilmenge von $\{-\infty\} \cup \mathbb{N}$ besitzt ein kleinstes Element.) Es gibt dann ein $q \in A[X]$ mit $g = fq + r$.
Es bleibt $\mathrm{grad}(r) < \mathrm{grad}(f)$ zu zeigen. Aus der Annahme, es wäre $\mathrm{grad}(r) \geq \mathrm{grad}(f)$, erhielte man wie folgt einen Widerspruch zur Minimalität von $\mathrm{grad}(r)$:
Sei $m := \mathrm{grad}(r)$, $n := \mathrm{grad}(f)$, $a_n$ der Leitkoeffizient von $f$, $b_m$ der von $r$. Da $a_n$ nach Voraussetzung eine Einheit und $m - n \geq 0$ nach Annahme ist, kann man das Polynom $a_n^{-1} b_m X^{m-n} \cdot f$ bilden, welches gleichen Grad und gleichen Leitkoeffizienten wie $r$ hat. Dann hat $r' := r - a_n^{-1} b_m X^{m-n} \cdot f$ einen echt kleineren Grad als $r$. Da aber
$g = (q + a_n^{-1} b_m X^{m-n}) \cdot f + r'$ ist, ergibt sich der gewünschte Widerspruch.
b) Zur Eindeutigkeit: Sei $g = fq + r = fq' + r'$ mit $\mathrm{grad}(r) < \mathrm{grad}(f)$ und $\mathrm{grad}(r') < \mathrm{grad}(f)$. Dann folgt $r - r' = (q' - q)f$. Wäre nun $q' \neq q$, so folgte $\mathrm{grad}((q' - q) \cdot f) \geq \mathrm{grad}(f)$ nach 8.7 b). Da aber $\mathrm{grad}(r - r') \leq \mathrm{Max}\{\mathrm{grad}(r), \mathrm{grad}(r')\} < \mathrm{grad}(f)$ ist, ergäbe sich ein Widerspruch. Somit ist $q' - q = 0$ und damit auch $r = r'$. □

**Bemerkung: 8.10** Wenn $A$ ein Körper ist, hat jedes $f \in A[X] - \{0\}$ als Leitkoeffizienten eine Einheit.

**Definition: 8.11** *Ein Element $\alpha \in A$ heißt eine Nullstelle (oder Wurzel) von $f \in A[X]$, wenn $f(\alpha) = 0$ ist.*

**Korollar: 8.12** *Wenn $\alpha$ eine Nullstelle von $f \in A[X]$ ist, gibt es ein Polynom $g \in A[X]$ mit*
$$f = (X - \alpha) \cdot g.$$

**Beweis:** $X - \alpha = -\alpha + 1 \cdot X + 0X^2 + \ldots$ hat den Leitkoeffizienten 1 und den Grad 1. Nach 8.9 gibt es $g, r \in A[X]$ mit $f = (X - \alpha)g + r$ und $\mathrm{grad}\, r < 1$.

Somit ist $r \in A$. Deshalb erhalten wir

$$0 = f(\alpha) = (\alpha - \alpha)g(\alpha) + r(\alpha) = r,$$

d.h. $r = 0$. □

Behauptung.

**Korollar: 8.13** *Über einem Integritätsring hat ein Polynom vom Grade $n \geq 0$ höchstens $n$ verschiedene Nullstellen.*

**Beweis:** Sei $f \neq 0$ ein Polynom kleinsten Grades, das mehr Nullstellen hat als sein Grad angibt. Seien etwa $\text{grad}(f) = n$ und $\alpha_1, \ldots, \alpha_{n+1}$ verschiedene Nullstellen von $f$. Dann gibt es ein Polynom $g$ vom Grade $n-1$ mit

$$f = (x - \alpha_{n+1})g.$$

Da $(\alpha_i - \alpha_{n+1})g(\alpha_i) = 0$, aber $\alpha_i \neq \alpha_{n+1}$ für $i \leq n$ ist, sind $\alpha_1, \ldots, \alpha_n$ verschiedene Nullstellen von $g$, welches den Grad $n-1$ hat. Dies ist ein Widerspruch zur Minimalität von $n$. □

**Korollar: 8.14** *Seien $A$ ein unendlicher Integritätsring und $f, g \in A[X]$. Wenn dann $f(a) = g(a)$ für alle $a \in A$ gilt, ist $f = g$.*

**Beweis:** Dann ist nämlich $(f - g)(a) = 0$ für unendlich viele $a$, d.h. $f - g$ hat unendlich viele Nullstellen, muss also das Nullpolynom sein.

□

**8.15** Nun zum wichtigsten Ergebnis dieses Paragrafen:

**Satz:** *Seien $K$ ein Integritätsring und $G$ eine endliche Untergruppe der Einheitengruppe $K^*$. Dann ist $G$ zyklisch.*

*Insbesondere ist $K^*$ zyklisch, wenn $K$ ein endlicher Körper ist. Speziell ist $(\mathbb{Z}/p)^*$ zyklisch.*

**Beweis:** Nach Satz 6.8 genügt es, folgendes zu zeigen:

Für jeden positiven Teiler $d$ von $\#G$ gibt es höchstens $d$ Elemente $\alpha \in G$ mit $\alpha^d = 1$.

Dies gilt aber deshalb, weil das Polynom $X^d - 1 \in K[X]$ höchstens $d$ Nullstellen hat. □

**8.16** Obiger Satz formuliert sich explizit folgendermaßen:

**Korollar:** *Sei $p$ eine Primzahl. Es gibt ein $r \in \mathbb{Z}$, so dass jede der Zahlen $1, 2, \ldots, p-1$ Rest von genau einer der Potenzen $r^0, r^1, \ldots, r^{p-2}$ von $r$ bei Division durch $p$ ist.*

**Definition: 8.17** *Ein solches $r$ heißt eine Primitivwurzel modulo $p$.*

**8.18** Wenn $r$ eine Primitivwurzel modulo $p$ und $r \equiv r' \pmod{p}$ ist, dann ist auch $r'$ eine Primitivwurzel modulo $p$.

Man kann Primitivwurzeln durch endliches Probieren in $\{1, 2, \ldots, p-1\}$ finden. Bis auf Kongruenz modulo $p$ gibt es nach 5.13 genau $\varphi(p-1)$ Primitivwurzeln modulo $p$.

Zum Testen ob eine Zahl eine Primitivwurzel ist, benutzt man das folgende

**Lemma: 8.19** *Sei $p$ eine Primzahl und $r \in \mathbb{Z}$ nicht durch $p$ teilbar. Genau dann ist $r$ eine Primitivwurzel modulo $p$, wenn für jeden Primfaktor $q$ von $p-1$*

$$r^{(p-1)/q} \not\equiv 1 \pmod{p} \text{ ist.}$$

**Beweis:** Genau dann, wenn die Ordnung von $\overline{r} := (r \bmod p)$ in $(\mathbb{Z}/p)^*$ gleich $p-1$ ist, ist $r$ eine Primitivwurzel modulo $p$. Im anderen Falle ist sie ein echter Teiler von $p-1$, d.h. ein Teiler einer der Zahlen $(p-1)/q$, wo $q$ ein Primfaktor von $p-1$ ist. □ **8.20** Ein weiteres zahlentheoretisches

Ergebnis erhalten wir als Korollar zu folgendem

**Satz:** *Sei $K$ ein endlicher Körper. Das Produkt aller Elemente aus $K^*$ ist* $-1$.

**Beweis:** Sei $x \in K^*$. Wenn $x \neq x^{-1}$ ist, so gibt es zu $x$ in dem Produkt $\prod_{z \in K^*} z$ genau einen weiteren Faktor $y$ (nämlich $y = x^{-1}$) mit $xy = 1$. Also ist

$$\prod_{x \in K^*} x = \prod_{\substack{x \in K^* \\ x = x^{-1}}} x.$$

Nun bedeutet $x = x^{-1}$, dass $x^2 = 1$, d.h. dass $x$ eine Nullstelle des Polynoms $X^2 - 1 = (X-1)(X+1)$ ist. Die einzigen $x \in K^*$ mit $x = x^{-1}$ sind also 1 und $-1$ (bzw. nur 1, wenn $1 = -1$ wie z.B. in $\mathbb{Z}/2$ ist). Also ist $\prod_{x \in K^*} x = 1 \cdot (-1) = -1$. $\square$

**8.21 Korollar** (Satz von *Wilson*): *Eine Zahl $m \in \mathbb{N}_2$ ist genau dann prim, wenn $(m-1)! \equiv -1$ (mod $m$) ist. Genauer gilt:*

$$(m-1)! \equiv \begin{cases} 2 & \text{wenn } m = 4 \\ -1 & \text{wenn } m \in \mathbb{P} \\ 0 & \text{sonst} \end{cases}$$

**Beweis:** 1. Fall: $m = 4$. Klar.
2. Fall: $m \in \mathbb{P}$. Dann ist
$((m-1)! \bmod m) = \prod_{x \in (\mathbb{Z}/m)^*} x = (-1 \bmod m)$ nach 8.20.
3. Fall: Sei $m > 4$ nicht prim, etwa $m = kn$ mit $1 < k < m$. Wenn $k \neq n$ ist, sind $k$ und $n$ verschiedene Faktoren in $1 \cdot 2 \cdot \ldots \cdot (m-1)$, also $m = k \cdot n \mid (m-1)!$.

Wenn $k = n$ ist, kann $n = 2$ wegen $n^2 = m > 4$ nicht gelten.
Mit $2 < n$ ist auch $2n < n^2 = m$, also $2n^2 = n \cdot 2n \mid (m-1)!$ und deshalb $m = n^2 \mid (m-1)!$. $\square$

AUFGABEN UND HINWEISE

**1)** Seien $p, q$ ungerade Primzahlen mit $p = 2q + 1$.
a) Wie viele Erzeuger hat $(\mathbb{Z}/p)^*$ ?

Sei $r \in \mathbb{N}$ mit $2 \leq r \leq q$. Zeigen Sie:
b) $r^q \equiv \pm 1 \pmod{p}$.
c) Entweder $r$ oder $-r$ ist eine Primitivwurzel modulo $p$. Dies hängt davon ab, welche der beiden Kongruenzen in b) gilt. In welcher Weise?

**2)** *Eine Legende:* Leonhard Euler, dem große Frömmigkeit nachgesagt wird, kam dennoch eines Nachts in die Situation, mit dem Teufel ein Spiel spielen zu müssen.
Euler holte ein Säckchen mit Bohnen und stellte 23 Becher im Kreis auf, 22 weiße und einen schwarzen. In letzteren legte er eine Bohne.
Die Spielregel war nun folgende: Der erste Spieler nehme eine Bohne und gebe sie in den Becher links neben dem schwarzen. Der zweite Spieler nehme 2 Bohnen und gebe nacheinander je eine in die links anschließenden beiden Becher. Dann nehme der erste Spieler 4 Bohnen und lege nacheinander je eine in die links anschließenden 4 Becher, u.s.w. Jeder Spieler nehme, wenn die Reihe an ihm ist, so viele Bohnen, wie sich bereits in allen Bechern zusammen befinden, und lege, anschließend an den zuletzt „bedienten“ Becher, in die folgenden Becher im Kreis herum immer je eine Bohne.

(Dabei wird er sehr bald den Kreis der 23 Becher mehr als einmal umrunden.)

Abb. 11

Verloren hat nun derjenige Spieler, der die *letzte* der Bohnen, die er bei einem Spielzug zu verteilen hat, in den schwarzen Becher gibt.
Der Teufel begann.

Fragen: Hatte das Spiel überhaupt ein Ende? Wer gewann (gegebenenfalls)?

Das Spiel hatte mehr als eine viertel Stunde gedauert. Der Teufel verlangte ein zweites Spiel, in dem diesmal Euler anfangen sollte und in dem die Zahl der Becher – um das Spiel abzukürzen – drastisch vermindert werden sollte.
Frage: Wie viele Becher entfernte Euler, um erstens das Spiel zu gewinnen und es zweitens sogar – sehr zum Ärger des Teufels – etwa doppelt so lange

dauern zu lassen wie das erste? (Gemeint ist, dass insgesamt – zusammen mit der Bohne, die zu Beginn im schwarzen Becher lag – doppelt so viele Bohnen benötigt wurden wie beim ersten Spiel.)

Schließlich änderte der Teufel die Regel dahingehend ab, dass derjenige verloren haben sollte, dessen letzte der gerade zu verteilenden Bohnen im Becher rechts neben (d.h. vor) dem schwarzen landete. Was geschah?

**3)** a) Man suche ein Vielfaches von 7, welches bei der Division durch 2, 3, 4, 5 und 6 jedesmal den Rest 1 lässt. (*Ibn al–Haitam*)
b) Mit welchem Satz des Paragrafen kann man a) und unendlich viele analoge Aufgaben sofort (d.h. ohne weitere Rechnung) lösen?

**4)** Sei $p$ eine ungerade Primzahl, $p = 2m + 1$.
a) Zeigen Sie:

$$(-1)^m (m!)^2 \equiv -1 (\text{mod}\, p).$$

(Berechnen Sie $\prod_{x \in (\mathbb{Z}/p)^*} x$ . Vgl. 8.21.)
b) Folgern Sie: Wenn $p \equiv 1 \pmod 4$ ist, so ist $-\overline{1}$ in $\mathbb{Z}/p$ ein Quadrat.

**5)** a) Welche Nullstellen hat das Polynom $X^2 - X$ in $\mathbb{Z}/6$ ?
(Vgl. 7. A5)
b) Welche Nullstellen hat das Polynom $X^2$ in $\mathbb{Z}/9$ ?

**6)** Sei $G$ eine endliche Untergruppe der Einheitengruppe eines Integritätsringes. Insbesondere ist $G$ zyklisch. Wir wollen die Summe ihrer Erzeuger bestimmen.

a) Ist $G$ nicht trivial, d.h. $G \neq \{1\}$, so ist die Summe aller Elemente von $G$ gleich 0. (Sei $v \in G - \{1\}$. Zeigen Sie: $v \cdot \sum_{u \in G} u = \sum_{u \in G} u$.)

b) Ist $\#G$ eine Primzahl $p$, so wird $G$ von jedem ihrer von 1 verschiedenen Elemente erzeugt. Deren Summe ist also nach a) gleich -1.

c) Sei jetzt $\#G = p^n$ mit einer Primzahl $p$ und $n > 1$. Seien ferner $v \in G$ von der Ordnung $p^r$ mit $1 \leq r < n$ und $z \in G$. Zeigen Sie: Genau dann ist $z$ ein Erzeuger von $G$, wenn $vz$ ein solcher ist.

Schließen Sie wie in a), dass die Summe der Erzeuger in diesem Falle gleich 0 ist.

d) Sei schließlich allgemein

$$\#G = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

mit verschiedenen Primzahlen $p_1, \ldots, p_r$ und $\alpha_i \in \mathbb{N}_1$. Für die Summe $S$ der Erzeuger von $G$ gilt dann:

1) Ist mindestens ein $\alpha_i > 1$, so ist $S = 0$.

2) Gilt $\alpha_1 = \ldots = \alpha_r = 1$, so ist $S = (-1)^r$.

(Zerlegen Sie die zyklische Gruppe $G$ nach dem chinesischen Restsatz:

$$G = G_1 \times \ldots \times G_r \quad \text{mit} \quad \#G_i = p_i^{\alpha_i},$$

und fassen Sie die $G_i$ als Untergruppen von $G$ auf. Sei $s_i$ die Summe der Erzeuger von $G_i$. Zeigen Sie $S = s_1 \cdot \ldots \cdot s_r$.)

e) Speziell für $\mathbb{Z}/p$ ergibt sich:

Sei $S$ die Summe der (paarweise nicht kongruenten) Primitivwurzeln modulo der Primzahl $p$ und $\mu$ die Möbiussche Funktion. Dann gilt

$$S \equiv \mu(p-1) \pmod{p}.$$

# § 9

# $(\mathbb{Z}/p^n)^*$

*In diesem Paragrafen sei $p$ eine Primzahl.*
Wir werden folgendes zeigen: Ist $p \neq 2$, so ist $(\mathbb{Z}/p^n)^*$ zyklisch für alle $n \in \mathbb{N}$. Hingegen ist $(\mathbb{Z}/2^n)^*$ für $n \geq 3$ nicht zyklisch, aber isomorf zu $(\mathbb{Z}/2) \times (\mathbb{Z}/2^{n-2})$.

Wir wollen Satz 7.14 anwenden und beginnen damit, eine Untergruppe $E_n$ von $(\mathbb{Z}/p^n)^*$ auszuzeichnen, die sich für $p > 2$ als zyklisch herausstellen wird.

**Definition: 9.1** *Sei $n \in \mathbb{N}_1$. Die Restklassen $(1 + x \ mod\ p^n)$ mit $x \in p\mathbb{Z}$ heißen 1–Einheiten von $\mathbb{Z}/p^n$. Mit $E_n$ sei die Menge der 1–Einheiten von $\mathbb{Z}/p^n$ bezeichnet.*

**Bemerkungen: 9.2** a) Jede 1–Einheit ist eine Einheit in $\mathbb{Z}/p^n$. Denn wegen $p|x$ ist $1 + x$ zu $p$ und damit zu $p^n$ teilerfremd.
b) $(a \mod p^n) \in \mathbb{Z}/p^n$ ist eine 1–Einheit genau dann, wenn $a \equiv 1 \pmod p$ gilt.
Denn $a \equiv 1 + x \pmod{p^n}$ für ein $x \in p\mathbb{Z}$ bedeutet $a \in 1 + x + p^n\mathbb{Z} \subset 1 + p\mathbb{Z}$. Die Umkehrung ist nach Definition klar.
c) Jedes Element aus $(\mathbb{Z}/2^n)^*$ ist eine 1–Einheit.

**Lemma: 9.3** *Die Menge $E_n$ der 1–Einheiten ist eine Untergruppe von $(\mathbb{Z}/p^n)^*$ der Ordnung $p^{n-1}$.*

**Beweis:** Zunächst ist $(1 \bmod p^n) \in E_n$. Ferner gilt $(1+x)(1+y) = 1 + x + y + xy$. Und mit $x, y \in p\mathbb{Z}$ ist auch $x + y + xy \in p\mathbb{Z}$. Also ist $E_n$ gegenüber Multiplikation abgeschlossen. Schließlich, da $(\mathbb{Z}/p^n)^*$ endlich ist, hat $(1 + x \bmod p^n)$ eine endliche Ordnung, etwa $k > 0$. Dann ist $(1 + x \bmod p^n)^{-1} = (1 + x \bmod p^n)^{k-1} \in E_n$.
Die Anzahl der 1–Einheiten ist gleich der Zahl der Restklassen $(x \bmod p^n)$, wo $x \in p\mathbb{Z}$ ist, also gleich $\dfrac{p^n}{p} = p^{n-1}$. □

**Lemma: 9.4** *Für $k \in \mathbb{N}$ mit $1 \leq k \leq p-1$ gilt $p \mid \begin{pmatrix} p \\ k \end{pmatrix}$.*

**Beweis:** Es ist $\binom{p}{k} = p!/k!(p-k)!$. Offenbar teilt $p$ den Zähler, aber nicht den Nenner dieses Bruches, da $k,\ p-k \leq p-1$ vorausgesetzt ist. □

**Lemma: 9.5** *Sei $p > 2$, $m \in \mathbb{N}_1$ und $x \in p^m\mathbb{Z} - p^{m+1}\mathbb{Z}$. Dann ist $(1+x)^p - 1 \in p^{m+1}\mathbb{Z} - p^{m+2}\mathbb{Z}$. Mit anderen Worten: Es gilt*

$$(1+x)^p = 1 + y \quad \textit{für ein} \quad y \in p^{m+1}\mathbb{Z} - p^{m+2}\mathbb{Z}.$$

**Beweis:** Wegen $\binom{p}{1} = p$ gilt: $(1+x)^p = 1 + px + \binom{p}{2}x^2 + \ldots + x^p$. Setze $B := \binom{p}{2}x^2 + \ldots + x^p$.

Nach Voraussetzung ist $v_p(x) = m$, also $v_p(px) = m + 1$.
*Behauptung:* $v_p(B) \geq m + 2$.
*Beweis hierfür:* Sei $2 \leq k \leq p - 1$. Dann ist

$$\begin{array}{rcl} v_p\left(\binom{p}{k} x^k\right) & = & v_p\left(\binom{p}{k}\right) + k \cdot v_p(x) \geq 1 + k \cdot m \\ & = & 1 + (k-1)m + m \geq 2 + m, \quad \text{da } \ k-1,\ m \geq 1. \end{array}$$

Ferner ist $v_p(x^p) = p \cdot v_p(x) = pm = m + (p-1)m \geq m+2$, da $m \geq 1,\ \ p-1 \geq 2$. (Genau hier wird $p > 2$ gebraucht.)
Jeder Summand in $B$ ist also durch $p^{m+2}$ teilbar, also auch $B$ selbst.

Es ist $px$ durch $p^{m+1}$, aber nicht durch $p^{m+2}$ teilbar. Hingegen ist $B$ durch $p^{m+2}$ teilbar. Es folgt, dass $y := px + B = (1+x)^p - 1$ zwar durch $p^{m+1}$, aber nicht durch $p^{m+2}$ teilbar ist. □

**Korollar: 9.6** *Sei $p > 2$, $r \in \mathbb{N}_1$. Wenn $x \in p^r\mathbb{Z} - p^{r+1}\mathbb{Z}$ ist, so ist $(1 + x)^{p^k} - 1 \in p^{r+k}\mathbb{Z} - p^{r+k+1}\mathbb{Z}$ für alle $k \in \mathbb{N}_1$.*

**Bemerkung: 9.7** Es ist $-2 \in 2\mathbb{Z} - 2^2\mathbb{Z}$, aber $(1-2)^2 - 1 = 0 \in 2^k\mathbb{Z}$ für alle $k \in \mathbb{N}$.

**Satz: 9.8** *Sei $p > 2$. Die Gruppe $E_n$ der 1–Einheiten in $(\mathbb{Z}/p^n)^*$ ist zyklisch. Für $n > 1$ ist $(1 + x \mod p^n)$ mit $x \in p\mathbb{Z}$ ein Erzeuger von $E_n$ genau dann, wenn $x \notin p^2\mathbb{Z}$ ist.*

**Beweis:** Sei $x \in p\mathbb{Z} - p^2\mathbb{Z}$. Nach 9.6 ist $(1+x)^{p^{n-1}} - 1 \in p^n\mathbb{Z}$, d.h. $(1+x)^{p^{n-1}} \equiv 1 \pmod{p^n}$. Die Ordnung von $(1 + x \bmod p^n)$ in der Gruppe $E_n$ ist also ein Teiler von $p^{n-1}$. Aber für jeden echten Teiler $p^k$ von $p^{n-1}$ – d.h. für $k < n-1$ – ist $(1+x)^{p^k} - 1 \notin p^n\mathbb{Z}$ ebenfalls gemäß 9.6, also $(1+x)^{p^k} \not\equiv 1 \pmod{p^n}$.
Da somit bzgl. der Multiplikation $\operatorname{ord}(1 + x \bmod p^n) = p^{n-1} = \#E_n$ gilt, ist $E_n$ zyklisch mit dem Erzeuger $(1 + x \bmod p^n)$.

Wenn nun $y \in p^2\mathbb{Z}$ ist, gilt $(1+y)^{p^{n-2}} \equiv 1 \pmod{p^n}$ nach 9.6, d.h. $(1 + y \bmod p^n)$ ist kein Erzeuger von $E_n$. □

**Lemma: 9.9** *Durch $(a \bmod p^n) \longmapsto (a \bmod p)$ wird eine Abbildung $(\mathbb{Z}/p^n)^* \longrightarrow (\mathbb{Z}/p)^*$ definiert. Diese Abbildung ist ein surjektiver Gruppenhomomorfismus mit dem Kern $E_n$. Deshalb gilt:*

$$(\mathbb{Z}/p^n)^*/E_n \cong (\mathbb{Z}/p)^*.$$

**Beweis:** Wegen $p^n\mathbb{Z} \subset p\mathbb{Z}$ erhält man mit dem Homomorfiesatz (6.29) einen Ringhomomorfismus $f' : \mathbb{Z}/p^n \longrightarrow \mathbb{Z}/p$, definiert durch $(a \bmod p^n) \longmapsto (a \bmod p)$.
*Behauptung:* Jeder Ringhomomorfismus $g' : A \longrightarrow B$ bildet $A^*$ in $B^*$ ab, induziert also einen Gruppenhomomorfismus $g : A^* \longrightarrow B^*$.
*Beweis hierfür:* Wenn $u \in A^*$, d.h. $u \cdot v = 1_A$ für ein $v \in A$ ist, erhält man $g'(u) \cdot g'(v) = g'(u \cdot v) = g'(1_A) = 1_B$. Damit ist auch $g'(u)$ eine Einheit in $B$.
Gemäß dieser Behauptung induziert $f'$ einen Gruppenhomomorfismus $f : (\mathbb{Z}/p^n)^* \longrightarrow (\mathbb{Z}/p)^*$, dessen Kern offenbar $E_n$ ist.
Ferner gilt $\operatorname{Im}(f) = (\mathbb{Z}/p)^*$, d.h. $f$ ist surjektiv. Denn, wenn
$(a \bmod p) \in (\mathbb{Z}/p)^*$, d.h. $\operatorname{ggT}(a, p) = 1$ ist, ist auch $\operatorname{ggT}(a, p^n) = 1$, d.h. $(a \bmod p^n) \in (\mathbb{Z}/p^n)^*$. Somit ist dann
$(a \bmod p) = f(a \bmod p^n) \in \operatorname{Im}(f)$.
Mit Hilfe des Homomorfiesatzes 6.21 erhalten wir nun die Isomorfie $(\mathbb{Z}/p^n)^*/E_n \cong (\mathbb{Z}/p)^*$. □

**Satz: 9.10** *Sei $p > 2$ und $n \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^n)^* \cong (\mathbb{Z}/(p-1)) \times (\mathbb{Z}/p^{n-1})$, also zyklisch.*

**Beweis:** Nach 9.8 ist $E_n$ zyklisch, nach 9.9 ist $(\mathbb{Z}/p^n)^*/E_n$ isomorf zu $(\mathbb{Z}/p)^*$, welches nach 8.16 zyklisch ist. Da schließlich $\mathrm{ggT}(\#E_n,\ \#(\mathbb{Z}/p)^*) = \mathrm{ggT}(p^{n-1},\ p-1) = 1$ gilt, folgt unser Satz aus 7.14a). □

**9.11** Wir wollen die Struktur von $(\mathbb{Z}/2^n)^*$ bestimmen. Zunächst gilt $(\mathbb{Z}/2)^* = \{(1 \bmod 2)\}$ und $(\mathbb{Z}/4)^* = \{(1 \bmod 4),\ (-1 \bmod 4)\}$. Diese beiden Gruppen sind trivialerweise zyklisch.

**9.12 Lemma** (vgl. 9.5): *Sei $n \in \mathbb{N}_2$ und $x \in 2^n\mathbb{Z} - 2^{n+1}\mathbb{Z}$. Dann ist $(1+x)^2 - 1 \in 2^{n+1}\mathbb{Z} - 2^{n+2}\mathbb{Z}$.*

**Beweis:** Es ist $(1+x)^2 = 1+2x+x^2$. Aus $v_2(x) = n \geq 2$ folgt $v_2(2x) = n+1$ und $v_2(x^2) = 2n \geq n+2$. Somit ist $v_2\left((1+x)^2 - 1\right) = n+1$. □

**Korollar: 9.13** *Für $n \in \mathbb{N}_2$ ist $(5 \bmod 2^n)$ Erzeuger einer zyklischen Untergruppe der Ordnung $2^{n-2}$ von $(\mathbb{Z}/2^n)^*$. Insbesondere gilt für $\alpha, \beta \in \mathbb{Z}$:*

$$(5 \bmod 2^n)^\alpha \equiv (5 \bmod 2^n)^\beta \iff \alpha \equiv \beta \pmod{2^{n-2}}.$$

**Satz: 9.14** *Sei $n \in \mathbb{N}_2$. Die Abbildung*

$$\begin{array}{rcl} f : (\mathbb{Z}/2) \times (\mathbb{Z}/2^{n-2}) & \longrightarrow & (\mathbb{Z}/2^n)^* \\ \Big((\varepsilon \bmod 2), (\alpha \bmod 2^{n-2})\Big) & \longmapsto & (-1 \bmod 2^n)^\varepsilon \cdot (5 \bmod 2^n)^\alpha \end{array}$$

*ist ein Gruppenisomorfismus. (Links steht das direkte Produkt der additiven Gruppen.) Insbesondere ist $(\mathbb{Z}/2^n)^*$ für $n \geq 3$ nicht zyklisch.*

**Beweis:** Zunächst ist – mit 9.13 – klar, dass $f$ ein wohldefinierter Gruppenhomomorfismus ist.
Die Gruppen $(\mathbb{Z}/2) \times (\mathbb{Z}/2^{n-2})$ und $(\mathbb{Z}/2^n)^*$ haben jeweils $2^{n-1}$ Elemente, da $\varphi(2^n) = (2-1) \cdot 2^{n-1}$ ist. Deshalb genügt es, folgendes zu zeigen:
*Behauptung:* $\mathrm{Ker}(f) = \{0\} = \{((0 \bmod 2), (0 \bmod 2^{2n-2}))\}$.

*Beweis hierfür:* Wenn $\Big((\varepsilon \bmod 2), (\alpha \bmod 2^{n-2})\Big) \in \operatorname{Ker}(f)$ ist und $\varepsilon, \alpha$ (ohne Einschränkung der Allgemeinheit) $\geq 0$ gewählt sind, gilt $(-1)^\varepsilon \cdot 5^\alpha \equiv 1 \pmod{2^n}$. Hieraus folgt $(-1)^\varepsilon \equiv 1 \pmod 4$, also
$\varepsilon \equiv 0 \pmod 2$. Dann folgt aber auch $5^\alpha \equiv 1 \pmod{2^n}$, d.h.
$\alpha \equiv 0 \pmod{2^{n-2}}$.
Dass $(\mathbb{Z}/2^n)^*$ nicht zyklisch ist, ergibt sich aus 7.15. □

**9.15 Korollar** (zu 9.10 und 9.14): *Sei $m \in \mathbb{N}_1$. Die Gruppe $(\mathbb{Z}/m)^*$ ist genau dann zyklisch, wenn $m$ eine der folgenden Zahlen ist: $1,\ 2,\ 4,\ p^n,\ 2p^n$ mit $p \in \mathbb{P} - \{2\}$ und $n \in \mathbb{N}$.*

**Beweis:** Sei $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ mit paarweise verschiedenen $p_i \in \mathbb{P}$ und $\alpha_i \in \mathbb{N}_1$. Dann gilt nach dem Chinesischen Restsatz (7.4) und nach 7.6 die Isomorfie

$$(\mathbb{Z}/m)^* \cong \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\alpha_i})^* .$$

Nach 7.15 ist also $(\mathbb{Z}/m)^*$ genau dann zyklisch, wenn alle $(\mathbb{Z}/p_i^{\alpha_i})^*$ es sind und zusätzlich $\operatorname{ggT}\big(\varphi(p_i^{\alpha_i}),\ \varphi(p_j^{\alpha_j})\big) = 1$ für $i \neq j$ gilt. Wenn aber $p_i,\ p_j$ ungerade sind und $\alpha_i,\ \alpha_j > 0$, so ist 2 ein gemeinsamer Teiler von $\varphi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i - 1}$ und $\varphi(p_j^{\alpha_j})$. Der Rest ist klar. □

**Definition: 9.16** *Falls $(\mathbb{Z}/m)^*$ zyklisch ist, heißt $r \in \mathbb{Z}$ eine Primitivwurzel modulo $m$, wenn $(r \bmod m)$ ein Erzeuger von $(\mathbb{Z}/m)^*$ ist.*

**Bemerkung: 9.17** Sei $p$ eine ungerade Primzahl, $n \in \mathbb{N}_2$. Dann gibt es bis auf Kongruenz modulo $p^n$ (bzw. $2p^n$) genau
$\varphi(p-1) \cdot (p-1)p^{n-2}$ Primitivwurzeln modulo $p^n$ (bzw. $2p^n$).

**9.18** Nur für spezielle Primzahlen $p$ gibt es „vernünftige" Methoden, Primitivwurzeln modulo $p$ zu finden. Im allgemeinen ist man auf systematisches Probieren angewiesen. Hat man hingegen bereits eine solche gefunden, so ist es nicht mehr so aufwendig, eine Primitivwurzel modulo $p^n$ bzw. $2p^n$ zu bestimmen.

**Satz: 9.19** *Seien $p > 2$, $n \in \mathbb{N}_2$ und $r \in \mathbb{Z}$.*
*a) Genau dann ist $r$ eine Primitivwurzel modulo $p^n$, wenn $r$ eine solche modulo $p$ ist und $r^{p-1} \not\equiv 1 \pmod{p^2}$ gilt.*
*b) Insbesondere ist eine Primitivwurzel modulo $p^2$ schon eine modulo $p^n$ – und umgekehrt.*

**Beweis:** a) Nach 7.14 b) ist $z = (r \bmod p^n)$ ein Erzeuger von $(\mathbb{Z}/p^n)^*$ genau dann, wenn $(z \bmod E_n)$ ein Erzeuger von $(\mathbb{Z}/p^n)^*/E_n$ und $z^{p-1}$ ein solcher von $E_n$ ist.
Der Homomorfismus

$$(\mathbb{Z}/p^n)^* \longrightarrow (\mathbb{Z}/p)^*$$

bildet $z$ auf $(r \bmod p)$ ab und hat den Kern $E_n$. Also ist $(z \bmod E_n)$ genau dann ein Erzeuger von $(\mathbb{Z}/p^n)^*/E_n$, wenn $(r \bmod p)$ ein solcher von $(\mathbb{Z}/p)^*$ ist. Andererseits ist $z^{p-1} = (r^{p-1} \bmod p^n)$ nach 9.8 ein Erzeuger von $E_n$ genau dann, wenn $r^{p-1} - 1 \notin p^2\mathbb{Z}$ ist.
b) folgt aus a). □

**9.20** a) Seien nun $p > 2$ und $r$ eine Primitivwurzel modulo $p$. Wenn $r^{p-1} \not\equiv 1 \pmod{p^2}$ ist, ist $r$ eine Primitivwurzel modulo $p^n$. Andernfalls ist aber $r + p$ eine solche. Denn

$$(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + p^2(\ldots) \equiv 1 + (p-1)r^{p-2}p \not\equiv 1 \pmod{p^2},$$

da $p - 1$, $r \notin p\mathbb{Z}$ sind.

b) Ist $r$ eine Primitvwurzel modulo $p^n$, so ist die ungerade der beiden Zahlen $r$, $r+p^2$ eine Primitivwurzel modulo $2p^n$. Dies sieht man an der „chinesischen" Zerlegung

$$(\mathbb{Z}/2p^n)^* \cong (\mathbb{Z}/2)^* \times (\mathbb{Z}/p^n)^*.$$

## AUFGABEN UND EIN HINWEIS

**1)** Bestimmen Sie eine Primitivwurzel modulo 121 und alle 11–ten Potenzen in $(\mathbb{Z}/121)^*$.

**2)** Sei $p$ eine der Primzahlen 2, 3, 5, 11. Zeigen Sie:
Es gibt keine $x,\ y,\ z \in \mathbb{Z}$ mit

$$x^p + y^p = z^p \quad \text{und} \quad p \nmid xyz.$$

(Für $p = 2$ ist dies trivial. Sonst rechnen Sie modulo $p^2$.)
Dies ist der sogenannte erste Fall der Fermat–Vermutung für die Exponenten 2, 3, 5, 11. Siehe: 15. A7.

**3)** Sei $m \in \mathbb{N}$ so gewählt, dass $(\mathbb{Z}/m)^*$ zyklisch ist. Bestimmen Sie das Produkt aller Erzeuger dieser Gruppe.
(Für alle von 3, 4 und 6 verschiedenen $m$ ergibt sich das „gleiche“ Ergebnis.)
Man kann diese Aufgabe leicht direkt bearbeiten. Sie sollten jedoch versuchen, sie mit 4. A14 (und 7. A10) in Zusammenhang zu bringen.

**4)** Sei $p$ eine Primzahl, $n \in \mathbb{N}_1$. Für $a, b \in \mathbb{Z}$ gelte $a \equiv b \pmod{p^n}$. Zeigen Sie: $a^{p^k} \equiv b^{p^k} \pmod{p^{n+k}}$.

**5)** Ein Zahlenrätsel im Quintalsystem:

$$EMMY^{EMMY} = * \ldots * EMMY.$$

Finden Sie eine nichttriviale Lösung.
(Im Quintalsystem ist die Grundzahl 5 statt 10 im Dezimal– bzw. 2 im Binärsystem. „$* \ldots *$“ bedeutet beliebig viele beliebige Ziffern. Trivial ist die Lösung $EMMY = 0001$.)

**6)** 64 (allgemeiner $2^m$) Menschen stehen im Kreis. Sie zählen (sich) reihum ab:

$$1, 2, 1, 2, \ldots \ .$$

Jeder, der 2 gerufen hat, verlässt den Kreis. Nach einer Runde bleiben 32 (bzw. $2^{m-1}$) übrig. Diese wiederholen das Verfahren usw.

Überlegen Sie: Wenn man auf naheliegende Weise die Menschen mit Elementen von $\mathbb{Z}/64$ (bzw. $\mathbb{Z}/2^m$) „benennt“, bleiben für $k \leq 6$ (bzw. $k \leq m$) nach $k$ Runden noch diejenigen übrig, deren „Namen“ von der Form $(1 + 2^k r \bmod 64)$ (bzw. $(1 + 2^k r \bmod 2^m)$) sind.

**7)** Seien $q$ und $p := 2q + 1$ Primzahlen. Zeigen Sie: Es gibt keine $n$, $m \in \mathbb{N}$, für die $2^n = p^m + 1$ wäre. (Welche Ordnung hat $(2 \bmod p)$ in $(\mathbb{Z}/p)^*$ mindestens? Was folgt daraus für $n$? Mit 9.14 folgt $p \equiv -1 \pmod{2^q}$.) (Vgl. [Schroeder] S.160f.)

# § 10

# Das quadratische Reziprozitätsgesetz

*In diesem Paragrafen bezeichne $p$ eine ungerade Primzahl.*

Es geht um die Lösbarkeit der Kongruenz

$$(1) \qquad x^2 \equiv a \pmod{p}.$$

Zu gegebenem $p$ alle $a$ zu finden, für die (1) lösbar ist, ist eine endliche Aufgabe, da es nur auf die Restklasse von $a$ modulo $p$ ankommt. Das „reziproke" Problem, nämlich zu gegebenem $a$ alle Primzahlen $p$ zu finden, für die (1) lösbar ist, wird durch das quadratische Reziprozitätsgesetz auf eine endliche Aufgabe zurückgeführt. Dieses Gesetz gibt einen einfachen Zusammenhang zwischen der Lösbarkeit von $x^2 \equiv q \pmod{p}$ und der von $x^2 \equiv p \pmod{q}$ an, wo $q$ eine weitere Primzahl $\neq 2$ ist. Daraus wird sich ergeben, dass bei gegebenem $a$ die Lösbarkeit von (1) nur von der Restklasse modulo $4a$ abhängt, in welcher die Primzahl $p$ liegt. Darüberhinaus erlaubt es, über die Lösbarkeit von (1) bei gegebenen $a$ und $p$ durch einen schnellen Algorithmus zu entscheiden.

**Bemerkungen: 10.1** a) Betrachte die Abbildung
$\tau : (\mathbb{Z}/p)^* \longrightarrow (\mathbb{Z}/p)^*, \ \ a \longmapsto a^2$.
Offenbar ist $\tau$ ein Homomorfismus. (Vgl. 6. A1.) Die Menge der Quadrate in $(\mathbb{Z}/p)^*$, nämlich $\mathrm{Im}(\tau)$, ist also eine Untergruppe von $(\mathbb{Z}/p)^*$.

b) Es gilt $\mathrm{Ker}(\tau) = \{$ Nullstellen von $X^2 - 1$ in $\mathbb{Z}/p\} = \{\overline{1}, -\overline{1}\}$. Da $\mathrm{Ker}(\tau)$ somit genau 2 Elemente besitzt, besteht $\mathrm{Im}(\tau) \cong (\mathbb{Z}/p)^*/\mathrm{Ker}(\tau)$ aus $\dfrac{1}{2}\#(\mathbb{Z}/p)^* = \dfrac{p-1}{2}$ Elementen. D.h. es gibt genau $\dfrac{p-1}{2}$ Quadrate in $(\mathbb{Z}/p)^*$. (Im Körper $\mathbb{Z}/p$ gibt es deshalb – einschließlich 0 – genau $\frac{p+1}{2}$ Quadrate.) $(\mathbb{Z}/p)^*/\ \mathrm{Im}(\tau)$ ist also eine Gruppe der Ordnung 2. Jede solche Gruppe ist isomorf zu $\mathbb{Z}^* = \{1, -1\}$, und zwar durch einen eindeutig bestimmten Isomorfismus (5.7 e).

c) Wenn man diesen Isomorfismus

$$(\mathbb{Z}/p)^*/\mathrm{Im}(\tau) \longrightarrow \{1, -1\}$$

mit dem kanonischen Homomorfismus

$$(\mathbb{Z}/p)^* \longrightarrow (\mathbb{Z}/p)^*/\mathrm{Im}(\tau)$$

verkettet, erhält man den Homomorfismus

$$(\mathbb{Z}/p)^* \longrightarrow \{1, -1\},$$

$$x \longmapsto \begin{cases} 1, & \text{wenn } x \text{ Quadrat in } (\mathbb{Z}/p)^*, \\ -1, & \text{wenn } x \text{ kein solches ist.} \end{cases}$$

d) Wenn $z$ ein Erzeuger von $(\mathbb{Z}/p)^*$, d.h. $z$ die Restklasse einer Primitivwurzel ist, so sind die geraden Potenzen von $z$, also die Elemente $z^2,\ z^4, \ldots, z^{p-1} = \overline{1}$ die Quadrate in $(\mathbb{Z}/p)^*$. Die Nichtquadrate sind somit von der Form $z^{2k-1}$ mit $k \in \mathbb{Z}$ bzw. $k = 1, 2, \ldots, (p-1)/2$.

**Definition: 10.2** *Für $p \in \mathbb{P} - \{2\}$ und $a \in \mathbb{Z}$ sei definiert:*

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \textit{wenn } p|a \\ 1, & \textit{wenn } p \nmid a \textit{ und } (a \bmod p) \textit{ ein Quadrat in } (\mathbb{Z}/p)^* \textit{ ist} \\ -1, & \textit{wenn } p \nmid a \textit{ und } (a \bmod p) \textit{ kein Quadrat in } (\mathbb{Z}/p)^* \textit{ ist.} \end{cases}$$

*Die Abbildung $\left(\frac{*}{*}\right) : \mathbb{Z} \times (\mathbb{P} - \{2\}) \longrightarrow \mathbb{Z}$ heißt das Legendre–Symbol.*
*Eine Zahl $a \in \mathbb{Z}$ heißt quadratischer Rest (bzw. quadratischer Nichtrest) modulo $p$, wenn $\left(\frac{a}{p}\right) = 1$ (bzw. $\left(\frac{a}{p}\right) = -1$) ist.*

**Feststellung: 10.3** *Die Abbildung*

$$(\mathbb{Z}/p)^* \longrightarrow \{1, -1\}, \quad (a \ mod \ p) \longmapsto \left(\frac{a}{p}\right)$$

*ist offenbar der in 10.1c) angegebene Gruppenhomomorfismus. Es folgt also*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

*zunächst für den Fall $p \nmid ab$. Im Falle $p|ab$ gilt diese Gleichung jedoch trivialerweise auch.*

**10.4 Satz** (*Euler*): *Für alle $a \in \mathbb{Z}$ gilt*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

**Beweis:** Dies ist trivial für $p \mid a$. Ist nun die Restklasse $\overline{a}$ ein Quadrat in $(\mathbb{Z}/p)^*$, $\overline{a} = x^2$, so gilt $\overline{a}^{(p-1)/2} = x^{p-1} = \overline{1}$ nach dem kleinen Satz von Fermat (6.7). Ist andererseits $\overline{a}$ kein Quadrat in $(\mathbb{Z}/p)^*$ und $z$ ein Erzeuger von $(\mathbb{Z}/p)^*$, so ist $\overline{a}$ von der Form $z^{2k+1}$, also $\overline{a}^{(p-1)/2} = z^{(p-1)\cdot k+(p-1)/2} = z^{(p-1)/2} \neq \overline{1}$. Wegen $\left(z^{(p-1)/2}\right)^2 = \overline{1}$ kann $z^{(p-1)/2}$ nur gleich $-\overline{1}$, der anderen Nullstelle von $X^2 - \overline{1}$ sein. □

**Korollar: 10.5** $\left(\frac{-1}{p}\right) \equiv p \ (mod \ 4)$, also

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{wenn} \quad p \equiv 1 \pmod{4} \\ -1 & \text{wenn} \quad p \equiv -1 \pmod{4} \end{cases}$$

**Beweis:** Aus der Kongruenz $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$ folgt offenbar (wegen $p > 2$) die Gleichheit

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Und $\frac{p-1}{2}$ ist gerade bzw. ungerade, je nachdem, ob $p \equiv 1 \pmod{4}$ oder $p \equiv -1 \pmod{4}$ ist. □

**Korollar: 10.6** *Es gibt unendlich viele Primzahlen $p$ mit $p \equiv 1 \pmod 4$.*

**Beweis:** Seien $p_1, \ldots, p_n$ mit $n \geq 0$ endlich viele solche. Sei $q$ ein Primfaktor von $(2 \cdot p_1 \cdot \ldots \cdot p_n)^2 + 1$. Es ist $q \neq 2$ und $q \neq p_i$ für $i = 1, \ldots, n$. Wegen $(2 \cdot p_1 \cdot \ldots \cdot p_n)^2 \equiv -1 \pmod q$ ist -1 ein Quadrat modulo $q$, d.h. $\left(\frac{-1}{q}\right) = 1$, d.h. $q \equiv 1 \pmod 4$. □

**10.7** Jede ungerade Primzahl ist modulo 4 entweder zu 1 oder zu -1 kongruent. Nach 4.28 und obigem Korollar gibt es von jeder der beiden Sorten unendlich viele.

**Bemerkung: 10.8** Sei $n = \dfrac{p-1}{2}$. Die Elemente

$$-\overline{n},\ \overline{-n+1}\,, \ldots,\ -\overline{1},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{n}$$

sind untereinander verschieden und machen ganz $(\mathbb{Z}/p)^*$ aus $(\overline{a} = (a \bmod p))$. Für $\overline{a} \in (\mathbb{Z}/p)^*$ gilt: Zu jedem $i \in \{1, \ldots, n\}$ gibt es ein $i' \in \{1, \ldots, n\}$ mit $\overline{a}\overline{i} = \pm\overline{i'}$.

**10.9 Lemma** (*Gauß*): *Zu $a \in \mathbb{Z} - p\mathbb{Z}$ seien $e_1, \ldots, e_n \in \{1, -1\}$ so bestimmt, dass für $i \in \{1, \ldots, n\}$*

$$\overline{a}\overline{i} = e_i \overline{i'}$$

*mit geeigneten $i' \in \{1, \ldots, n\}$ gilt. Dann ist*

$$\left(\frac{a}{p}\right) = e_1 \cdot \ldots \cdot e_n.$$

**Beweis:** Seien $i, j \in \{1, \ldots, n\}$. Mit $\overline{i} \neq \overline{j}$ ist auch $\overline{i'} \neq \overline{j'}$. Denn aus $\overline{a}\overline{i} = \pm\overline{a}\overline{j}$ und $\overline{a} \in (\mathbb{Z}/p)^*$ folgt $\overline{i} = \pm\overline{j}$. Da aber $-\overline{j} \notin \{\overline{1}, \ldots, \overline{n}\}$ ist, bleibt $\overline{i} = \overline{j}$ übrig.
Somit folgt

$$\prod_{i=1}^{n} \overline{i} = \prod_{i=1}^{n} \overline{i'}$$

und deshalb

$$\overline{a}^n \prod_{i=1}^{n} \overline{i} = \prod_{i=1}^{n} (\overline{a}\overline{i}) = \prod_{i=1}^{n} (\overline{e_i}\overline{i'}) = \overline{e_1 \cdot \ldots \cdot e_n} \prod_{i=1}^{n} \overline{i'} = \overline{e_1 \cdot \ldots \cdot e_n} \prod_{i=1}^{n} \overline{i}.$$

Also $\overline{a}^n = \overline{e_1 \cdot \ldots \cdot e_n}$, d.h. $a^n \equiv e_1 \cdot \ldots \cdot e_n \pmod{p}$.

Mit 10.4 folgt die Behauptung. $\square$

**Satz: 10.10** *Es gilt*

$$\begin{aligned} \left(\frac{2}{p}\right) &= \begin{cases} 1 & \textit{wenn} \quad p \equiv \pm 1 \pmod{8} \quad \textit{ist}, \\ -1 & \textit{wenn} \quad p \equiv \pm 3 \pmod{8} \quad \textit{ist} \end{cases} \\ &= (-1)^{(p^2-1)/8}. \end{aligned}$$

**Beweis:** a) Zur 1. Gleichung: Sei $p = 2n+1$.
1. Fall: $n = 4m$ oder $n = 4m+1$. (D.h. $p \equiv 1 \pmod 8$ oder $p \equiv 3 \pmod 8$.) In diesem Falle ist $e_i = 1$ für $1 \leq i \leq 2m$, da $2 \cdot 1,\ 2 \cdot 2,\ \ldots,\ 2 \cdot 2m \in \{1, 2, \ldots, n\}$. Hingegen ist $e_i = -1$ für $2m+1 \leq i \leq n$, da $2(2m+1),\ 2(2m+2), \ldots, 2n \in \{n+1, \ldots, 2n\}$, also $2\overline{(2m+1)},\ 2\overline{(2m+2)}, \ldots, 2\overline{n} \in \{-\overline{n}, -\overline{(n-1)}, \ldots, -\overline{1}\}$ gilt. In diesem Falle ist demnach $e_1 \cdot \ldots \cdot e_n = (-1)^{n-2m} = (-1)^n$.

2. Fall: $n = 4m+2$ oder $n = 4m+3$. (D.h. $p \equiv 5 \pmod 8$ oder $p \equiv 7 \pmod 8$.) Analog zum ersten Fall erhält man:
$e_i = 1$ für $1 \leq i \leq 2m+1$ und $e_i = -1$ für $2m+2 \leq i \leq n$. Es ergibt sich

$$e_1 \cdot \ldots \cdot e_n = (-1)^{n-2m-1} = (-1)^{n-1}.$$

Aus obigen Ergebnissen erhalten wir schließlich

1. für $p \equiv 1 \pmod 8$, d.h. $p = 8m+1$, $n = \dfrac{p-1}{2} = 4m$ :

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{4m} = 1 \ ;$$

2. für $p \equiv -1 \pmod 8$, d.h. $p = 8m+7$, $n = 4m+3$ :

$$\left(\frac{2}{p}\right) = (-1)^{n-1} = (-1)^{4m+2} = 1 \ ;$$

3. für $p \equiv 3 \pmod 8$, d.h. $p = 8m + 3$, $n = 4m + 1$:

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{4m+1} = -1;$$

4. für $p \equiv -3 \pmod 8$, d.h. $p = 8m + 5$, $n = 4m + 2$:

$$\left(\frac{2}{p}\right) = (-1)^{n-1} = (-1)^{4m+1} = -1.$$

b) Zur zweiten Gleichung:

1. $p = 8m \pm 1 \Longrightarrow p^2 - 1 = 64m^2 \pm 16m + 1 - 1$

$$= 8(8m^2 \pm 2m) \Longrightarrow \frac{p^2-1}{8} \quad \text{ist gerade.}$$

2. $p = 8m \pm 3 \Longrightarrow p^2 - 1 = 64m^2 \pm 48m + 9 - 1$

$$= 8(8m^2 \pm 6m + 1) \Longrightarrow \frac{p^2-1}{8} \quad \text{ist ungerade.}$$ □

**10.11 Theorem** (Quadratisches Reziprozitätsgesetz, *Gauß*):
*Seien $p, q$ verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

**Beweis:** Sei $p = 2n + 1$, $q = 2m + 1$. Wir bestimmen $\left(\frac{q}{p}\right)$ nach Gauß' Lemma. Es ist $\left(\frac{q}{p}\right) = (-1)^N$, wenn $N$ die Elementezahl der Menge

$$X := \{x \in \{1, \dots, n\} \mid e_x = -1\}$$

ist. Dabei ist $e_x \in \{1, -1\}$ so zu wählen, dass eine Kongruenz der Form

$$(*) \qquad qx \equiv e_x \cdot u \pmod p$$

mit einem $u \in \{1, \ldots, n\}$ besteht. D.h. ein $x \in \{1, \ldots, n\}$ gehört genau dann zu $X$, wenn es ein $y \in \mathbb{Z}$ mit

$$qx - py \in \{-1, -2, \ldots, -n\}, \quad \text{d.h.}$$

$$py - qx \in \{1, \ldots, n\}$$

gibt. Wenn es ein solches $y$ gibt, ist es eindeutig durch $x$ bestimmt, z.B. weil $e_x$ und $u$ in der Kongruenz $(*)$ eindeutig bestimmt sind. Wir nennen es $y_x$.

$X$ ist gleichmächtig zu der Menge

$$X' := \left\{(x, y) \in \mathbb{Z}^2 \ \mid \ 1 \le py - qx \le n, \ \ 1 \le x \le n\right\}.$$

Eine bijektive Abbildung $X \longrightarrow X'$ wird durch $x \longmapsto (x, y_x)$ gegeben. Aus $1 \le py - qx \le n$ und $1 \le x \le n$ folgt einerseits $1 \le y$, andererseits

$$y \le \frac{qx + n}{p} \le \frac{(q+1)n}{2n+1} < \frac{q+1}{2} = m + 1.$$

Deshalb ist

$$X' = \left\{(x, y) \in \mathbb{Z}^2 \ \mid \ 1 \le x \le n, \ \ 1 \le y \le m, \ \ 1 \le py - qx \le n\right\}.$$

Wir haben

$$\left(\frac{q}{p}\right) = (-1)^N \quad \text{mit} \quad N = \#X'.$$

Aus Symmetriegründen ist

$$\left(\frac{p}{q}\right) = (-1)^M \quad \text{mit} \quad M = \#Y', \text{ wo}$$

$$Y' = \left\{(x, y) \in \mathbb{Z}^2 \ \mid \ 1 \le x \le n, \ \ 1 \le y \le m, \ \ 1 \le qx - py \le m\right\}$$

gilt.

Da $1 \le py - qx \le n$ äquivalent mit $-n \le qx - py \le -1$ ist, sind $X'$ und $Y'$ disjunkt.

Für $1 \le x \le n < \frac{p}{2}$ ist $qx$ nicht durch $p$ teilbar, also $qx - py \ne 0$. Deshalb gilt

$$X' \cup Y' = \left\{(x, y) \in \mathbb{Z}^2 \ \mid \ 1 \le x \le n, \ \ 1 \le y \le m, \ \ -n \le qx - py \le m\right\}$$

und $X' \cap Y' = \emptyset$.
Die beiden Mengen

$$Z_1 := \big\{(x,y) \in \mathbb{Z}^2 \;\mid\; 1 \le x \le n,\;\; 1 \le y \le m,\;\; qx - py < -n\big\}$$

und

$$Z_2 := \big\{(x,y) \in \mathbb{Z}^2 \;\mid\; 1 \le x \le n,\;\; 1 \le y \le m,\;\; qx - py > m\big\}$$

sind gleichmächtig. Eine bijektive Abbildung $Z_1 \longrightarrow Z_2$ wird durch

$$(x,y) \longmapsto (x',y') := (n+1-x,\; m+1-y)$$

gegeben. Denn es ist

$$\begin{aligned}
qx' - py' - m &= q(n+1-x) - p(m+1-y) - m \\
&= q \cdot \frac{p+1}{2} - qx - p \cdot \frac{q+1}{2} + py - m \\
&= -qx + py - m + \frac{q}{2} - \frac{p}{2} \\
&= -qx + py - m + \frac{q-1}{2} - \frac{p-1}{2} \\
&= -(qx - py + n).
\end{aligned}$$

Nun ist $\{1,\ldots,n\} \times \{1,\ldots,m\}$ die disjunkte Vereinigung der Mengen $X', Y', Z_1$ und $Z_2$, also $m \cdot n = M + N + 2S$ mit $S = \# Z_1$. Es folgt

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{M+N+2S} = (-1)^{mn}. \qquad \square$$

**Bemerkungen: 10.12** a) Wir haben die Äquivalenzen:

$$\begin{aligned}
p \equiv 1 (\mathrm{mod}\ 4) &\iff \frac{p-1}{2} \text{ gerade} &&\iff \left(\frac{-1}{p}\right) = 1, \\
p \equiv -1 (\mathrm{mod}\ 4) &\iff \frac{p-1}{2} \text{ ungerade} &&\iff \left(\frac{-1}{p}\right) = -1.
\end{aligned}$$

Lasst uns $p$ „brav“ nennen, wenn $p \equiv 1 \pmod 4$ ist, sonst „interessant“.
Das quadratische Reziprozitätsgesetz besagt:
Wenn mindestens eine der verschiedenen ungeraden Primzahlen $p$ und $q$ brav ist, gilt

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Wenn beide interessant sind, gilt hingegen

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

b) Mit Hilfe des quadratischen Reziprozitätsgesetzes und folgender Regeln kann man das Legendre–Symbol oft leicht berechnen:

(1) $\left(\frac{a}{p}\right)$ ist nach Definition nur von der Restklasse von $a$ modulo $p$ abhängig: $\left(\frac{a}{p}\right) = \left(\frac{a-kp}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ (10.3);

(3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (10.5)

(4) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{für } p \equiv \pm 1 \pmod 8 \\ -1 & \text{für } p \equiv \pm 3 \pmod 8 \end{cases}$ (10.10)

**Beispiel:** $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right)$
$= -\left(\frac{1}{7}\right) = -1.$

Die 1. und die 5. Gleichung gelten nach dem quadratischen Reziprozitätsgesetz, da 29 „brav“ ist, die 2. und die 6. nach (1), die 3. nach (2), die 4. nach (4).
Bei diesem Verfahren benötigt man die Primfaktorzerlegung. Wir werden ein Verfahren entwickeln, das ohne diese auskommt.
c) Die o.a. Regeln (3) und (4), d.h. 10.5 und 10.10 werden auch die

Ergänzungssätze zum Quadratischen Reziprozitätsgesetz genannt.

**Definition: 10.13** *Sei $b$ eine ungerade natürliche Zahl mit der Primfaktorzerlegung $b = p_1 \cdot \ldots \cdot p_m$. Für $a \in \mathbb{Z}$ definieren wir*

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_n}\right).$$

*Dieses für eine größere Definitionsmenge definierte Symbol heißt das Jacobi–Symbol.*

**Bemerkungen: 10.14** a) $\left(\frac{a}{1}\right) = 1.$

b) Falls $a$ und $b$ nicht teilerfremd sind, ist $\left(\frac{a}{b}\right) = 0.$

c) Das Jacobisymbol $\left(\frac{*}{b}\right)$ stimmt für prime $b$ mit dem Legendresymbol überein.

**Feststellung: 10.15** *a)* $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$*, falls $a \equiv a' \pmod b$ ist.*

*b)* $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right).$

*c)* $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right).$

**Beweis:** Sei $b = p_1 \cdot \ldots \cdot p_m$ mit $p_i \in \mathbb{P}$.

a) Mit $a \equiv a' \pmod b$ ist $a \equiv a' \pmod{p_i}$, also $\left(\frac{a}{p_i}\right) = \left(\frac{a'}{p_i}\right)$ für alle $i = 1, \ldots, m$.

b) Es ist ja $\left(\frac{a_1 a_2}{p_i}\right) = \left(\frac{a_1}{p_i}\right) \cdot \left(\frac{a_2}{p_i}\right).$

c) folgt direkt aus der Definition des Jacobisymbols. □

**Satz: 10.16** *Seien $a$ und $b$ zueinander teilerfremde ungerade natürliche Zahlen. Dann gilt:*

*a)* $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$*;*

*b)* $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$*;*

*c)* $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

Der Beweis wird mit Hilfe des nächsten Hilfssatzes geführt.

**Hilfssatz: 10.17** *Seien $r, s$ ungerade. Dann gilt:*

*a)* $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod 2$*;*

*b)* $\frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod 2$*.*

**Beweis:** a) Es ist $rs-1 = (r-1)\cdot(s-1) + (r-1) + (s-1)$. Da $4 \mid (r-1)(s-1)$, folgt: $(rs-1) \equiv (r-1) + (s-1) \pmod 4$.
Wende 4.11 d) an.
b) Da $4 \mid r^2-1$ und $4 \mid s^2-1$ gilt – es ist ja sogar $8 \mid r^2-1$ –, folgt

$$r^2s^2 - 1 \equiv (r^2-1) + (s^2-1) \pmod{16}$$

wie unter a). □

**Korollar: 10.18** *Seien $r_1, \ldots r_n \in 1 + 2\mathbb{Z}$. Dann gilt:*

*a)* $\sum_{i=1}^{m} \frac{r_i-1}{2} \equiv \frac{\left(\prod_{i=1}^m r_i\right)-1}{2} \pmod 2$*;*

*b)* $\sum_{i=1}^{m} \frac{r_i^2-1}{8} \equiv \frac{\left(\prod_{i=1}^m r_i^2\right)-1}{8} \pmod 2$*.*

**Beweis** des Satzes 10.16: Sei $b = p_1 \cdot \ldots \cdot p_m$ mit $p_i \in \mathbb{P}$.

a) $$\left(\frac{-1}{b}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right) = \prod_{i=1}^{m} \left((-1)^{\frac{p_i - 1}{2}}\right)$$
$$= (-1)^{\sum \frac{p_i - 1}{2}} = (-1)^{\frac{b-1}{2}} \text{ nach 10.18 a).}$$

b) beweist sich genauso mit Hilfe von 10.18 b).

c) Sei $a = q_1 \cdot \ldots \cdot q_n$ mit $q_i \in \mathbb{P}$. Mit Hilfe von 10.15 b) und c) erhält man dann

$$\begin{aligned} \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{m} \prod_{j=1}^{n} \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \\ &= (-1)^{\sum_i \left(\sum_j \frac{q_j - 1}{2} \cdot \frac{p_i - 1}{2}\right)} \\ &= (-1)^{\sum_i \frac{a-1}{2} \cdot \frac{p_i - 1}{2}} = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}. \end{aligned}$$ □

**Beispiel: 10.19** 5333 ist eine Primzahl $\equiv 1 \pmod 4$. (Hingegen ist 2001 keine Primzahl.)

$$\left(\frac{2001}{5333}\right) = \left(\frac{5333}{2001}\right) = \left(\frac{-670}{2001}\right)$$

$$= \underbrace{\left(\frac{-1}{2001}\right)}_{=1} \cdot \underbrace{\left(\frac{2}{2001}\right)}_{=1} \cdot \left(\frac{335}{2001}\right) = \left(\frac{2001}{335}\right) = \left(\frac{2001 - 6 \cdot 335}{335}\right)$$

$$= \left(\frac{-9}{335}\right) = \left(\frac{-1}{335}\right) \cdot \underbrace{\left(\frac{3}{335}\right)^2}_{=1} = -1,$$

da $335 \equiv -1 \pmod 4$.

Aus dem quadratischen Reziprozitätsgesetz (in der speziellen Form 10.11 oder in der allgemeinen Form 10.16 c)) und den beiden sogenannten Ergänzungssätzen (10.5 und 10.10, bzw. 10.16a) und b)) ergeben sich auch für die Theorie interessante Folgerungen:

**Satz: 10.20** *Seien $a \in \mathbb{N}_1$, $p$ und $q$ ungerade Primzahlen mit* $p \equiv \pm q \ (\mathrm{mod} 4a)$. *Dann gilt*

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

**Beweis:** *Behauptung:* Es genügt, den Satz im Falle, dass $a$ prim ist, zu zeigen. Sei nämlich $a = p_1 \cdot \ldots \cdot p_m$ mit $p_i \in \mathbb{P}$. Aus $p \equiv \pm q (\mathrm{mod} 4a)$ folgt $p \equiv \pm q$ (mod $4p_i$) für alle $i$. Wenn man hieraus $\left(\frac{p_i}{p}\right) = \left(\frac{p_i}{q}\right)$ folgern kann, ist auch $\left(\frac{a}{p}\right) = \prod_{i=1}^{m} \left(\frac{p_i}{p}\right) = \prod_{i=1}^{m} \left(\frac{p_i}{q}\right) = \left(\frac{a}{q}\right)$.
Wir nehmen also ab jetzt an, $a$ sei prim.
Wenn $a = 2$ ist und $p \equiv \pm q$ (mod 8), so ist mit $p \equiv \pm 1$ (mod 8) auch $q \equiv \pm 1$ (mod 8) und umgekehrt.
Sei nun $a$ eine ungerade Primzahl („ungerade Zahl" würde genügen) und zunächst $p \equiv q$ (mod $4a$), also insbesondere auch $p \equiv q$ (mod $a$).
Durch zweimalige Anwendung des Reziprozitätsgesetzes und mit 10.12 b)(1) erhalten wir

$$\begin{aligned}\left(\frac{a}{p}\right) &= (-1)^{\frac{p-1}{2} \cdot \frac{a-1}{2}} \left(\frac{p}{a}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{a-1}{2}} \left(\frac{q}{a}\right) \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{a-1}{2} + \frac{q-1}{2} \cdot \frac{a-1}{2}} \left(\frac{a}{q}\right) \\ &= (-1)^{\frac{a-1}{2} \cdot (\frac{p-1}{2} + \frac{q-1}{2}} \left(\frac{a}{q}\right).\end{aligned}$$

Da $p \equiv q \mathrm{mod}\ 4$ ist, sind $(p-1)/2$ und $(q-1)/2$ beide gerade oder ungerade, also ihre Summe gerade und deshalb $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Falls $p \equiv -q$ (mod $4a$), also genau eine der beiden Zahlen $(p-1)/2$, $(q-1)/2$

gerade ist, ergibt sich analog

$$\begin{aligned}
\left(\frac{a}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{p}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{-q}{a}\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{-1}{a}\right)\left(\frac{q}{a}\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\cdot(-1)^{\frac{a-1}{2}}\cdot(-1)^{\frac{q-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{p}\right) \\
&= (-1)^{\frac{a-1}{2}\cdot(\frac{p-1}{2}+1+\frac{q-1}{2})}\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right).
\end{aligned}$$

□

**Satz: 10.21** *Sei $a \in \mathbb{Z}$ kein Quadrat in $\mathbb{Z}$. Es gibt unendlich viele Primzahlen, modulo welchen $a$ kein Quadrat ist.*

**Beweis:** Wenn ein $b \in \mathbb{Z}$ modulo einer Primzahl $p$ kein Quadrat und $m$ zu $p$ teilerfremd ist, ist auch $bm^2$ kein Quadrat modulo $p$. Man darf deshalb annehmen, dass $a$ quadratfrei, d.h. nicht durch das Quadrat einer Primzahl teilbar ist.

Sei $a = (-1)^\delta 2^\varepsilon q_1 \cdot \ldots \cdot q_n$ mit ungeraden paarweise verschiedenen Primzahlen $q_1, \ldots, q_n$ und $\delta, \varepsilon \in \{0, 1\}$.

1. Fall: $n \geq 1$, d.h. $a$ hat mindestens einen ungeraden Primfaktor.
Seien $s$ ein quadratischer Nichtrest (10.2) modulo $q_n$ und $r_1, \ldots, r_k$ (mit beliebig großem $k \in \mathbb{N}$) endlich viele ungerade Primzahlen, die von allen $q_j$ verschieden sind.
Nach dem Chinesischen Restsatz gibt es ein $b \in \mathbb{N}$ mit $b \equiv 1 \pmod 8$, $b \equiv 1 \pmod{r_i}$ für $i = 1, \ldots, k$, $b \equiv 1 \pmod{q_i}$ für $i = 1, \ldots, n-1$ und $b \equiv s \pmod{q_n}$.
Sei $b = p_1 \cdot \ldots \cdot p_m$ mit $p_i \in \mathbb{P}$.
Wegen $b \equiv 1 \pmod 8$ ist $p_i \neq 2$ für alle $i$.
Wegen $b \equiv 1 \pmod{r_j}$ ist $p_i \neq r_j$ für alle $i, j$.

*Behauptung:* Es ist $\left(\frac{a}{p_i}\right) = -1$ für wenigstens ein $i \in \{1, \ldots, m\}$.

Da $p_i$ nicht zu der beliebig großen endlichen Menge $\{r_1, \ldots, r_k\}$ gehört, folgt aus der Behauptung der Satz im 1. Fall.

*Beweis der Behauptung:* Für das Jacobisymbol $\left(\frac{a}{b}\right)$ gilt:

$$\begin{aligned}
\left(\frac{a}{b}\right) &= \left(\frac{-1}{b}\right)^{\delta}\left(\frac{2}{b}\right)^{\varepsilon}\cdot\left(\frac{q_1}{b}\right)\cdot\ldots\cdot\left(\frac{q_n}{b}\right)\\
&= \left(\frac{b}{q_1}\right)\cdot\ldots\cdot\left(\frac{b}{q_n}\right), \quad \text{da} \quad b\equiv 1 \pmod 8,
\end{aligned}$$

also auch $b \equiv 1 \pmod 4$ ist. Deshalb gilt
$\left(\frac{a}{b}\right) = \left(\frac{1}{q_1}\right)\cdot\ldots\cdot\left(\frac{1}{q_{n-1}}\right)\cdot\left(\frac{s}{q_n}\right)$ nach Wahl von $b$. Da $\left(\frac{1}{q_i}\right) = 1$ und nach Voraussetzung $\left(\frac{s}{q_n}\right) = -1$ ist, folgt $\left(\frac{a}{b}\right) = -1$.

Andererseits ist $\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\cdot\ldots\cdot\left(\frac{a}{p_m}\right)$, also $\left(\frac{a}{p_i}\right) = -1$ für mindestens ein $i$.

Es bleiben die Fälle $a = -1$, $a = 2$, $a = -2$ übrig.

Zunächst ist $\left(\frac{-1}{p}\right) = -1$ genau dann, wenn $p \equiv -1 \pmod 4$ gilt. Nach 4.28 gibt es unendlich viele Primzahlen $p$ dieser Art.

Was $\pm 2$ betrifft, wissen wir die Äquivalenz

$$\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod 8,$$

und wir sehen mittels $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ leicht

$$\left(\frac{-2}{p}\right) = -1 \iff p \equiv -3 \pmod 8 \quad \text{oder} \quad p \equiv -1 \pmod 8.$$

Dies bedeutet: $\left(\frac{2}{p}\right) = -1 \iff \overline{p} \notin \{\overline{1}, -\overline{1}\}$ und
$\left(\frac{-2}{p}\right) = -1 \iff \overline{p} \notin \{\overline{1}, \overline{3}\}$, wobei $\overline{a} := (a \bmod 8)$ gesetzt wurde.

Da $\{\overline{1}, -\overline{1}\}$ und $\{\overline{1}, \overline{3}\}$ Untergruppen von $(\mathbb{Z}/8)^*$ sind, werden die letztgenannten Fälle also durch den folgenden Satz erledigt, der eine Verallgemeinerung von 4.27 ist:

**Satz: 10.22** *Sei $m \in \mathbb{N}_3$, $U \subset (\mathbb{Z}/m)^*$ eine echte Untergruppe ($U \neq (\mathbb{Z}/m)^*$). Dann gibt es unendlich viele Primzahlen $p$ mit $(p \bmod m) \notin U$.*

**Beweis:** Wähle ein $s \in \mathbb{N}$ mit $(s \bmod m) \in (\mathbb{Z}/m)^* - U$. Seien $p_1, \dots, p_r$ endlich viele Primzahlen der gesuchten Art, die zudem $s$ nicht teilen. Möglicherweise ist $r = 0$. Es genügt, eine Primzahl $p_0 \neq p_i$ für $i = 1, \dots, r$ mit $(p_0 \bmod m) \in (\mathbb{Z}/m)^* - U$ und $p_0 \nmid s$ zu finden.
Nun gibt es einen Primfaktor $p_0$ von $N := mp_1 \cdot \ldots \cdot p_r + s$, der obige Bedingung erfüllt. (Im Falle $r = 0$ ist $N = m + s$.) Denn für jeden Primfaktor $p$ von $N$ gilt $p \notin \{p_1, \dots, p_r\}$ und $(p \bmod m) \in (\mathbb{Z}/m)^*$, da $p$ sowohl zu den $p_i$, wie zu $m$ teilerfremd ist. Lägen nun die Restklassen aller Primfaktoren $p$ von $N$ in $U$, so auch die Restklasse von $N$ selber. Es ist aber $(N \bmod m) = (s \bmod m) \notin U$. Da $s$ teilerfremd zu $N$ ist, gilt auch $p_0 \nmid s$. □

**10.23 N.B.** Ein Spezialfall von 11. A2 b) besagt, dass jede ganze Zahl modulo unendlich vielen Primzahlen ein Quadrat ist.

**Satz: 10.24** *Sei $m$ eine ungerade natürliche Zahl $m = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ mit $\alpha_i \in \mathbb{N}_1$, $p_i \in \mathbb{P}$, ferner $a \in \mathbb{Z}$ zu $m$ teilerfremd.*
*Die Kongruenz $x^2 \equiv a \pmod m$ ist genau dann lösbar, wenn $\left(\frac{a}{p_i}\right) = 1$ für alle $i = 1, \dots, n$ ist.*

**Beweis:** Man kann ohne Einschränkung der Allgemeinheit voraussetzen, dass die $p_i$ verschieden sind. Nach dem Chinesischen Restsatz ist die Kongruenz $x^2 \equiv a \pmod m$ genau dann lösbar, wenn alle Kongruenzen $x^2 \equiv a \pmod{p_i^{\alpha_i}}$ lösbar sind. Es genügt also, folgendes zu zeigen:
*Behauptung:* Sei $p$ eine ungerade Primzahl, $\alpha \in \mathbb{N}_1$, $a \in \mathbb{Z}$ nicht durch $p$ teilbar. Die Kongruenz $x^2 \equiv a \pmod{p^\alpha}$ ist genau dann lösbar, wenn $x^2 \equiv a \pmod p$ lösbar ist.
*Beweis hierfür:* Sei $E \subset (\mathbb{Z}/p^\alpha)^*$ die Untergruppe der 1–Einheiten. (Vgl. 9.1).

Sie ist von der ungeraden Ordnung $p^{\alpha-1}$. Sei $p^{\alpha-1}+1=2m$. Für $e \in E$ gilt dann:
$$(e^m)^2 = e^{\sharp E+1} = e \quad \text{nach 6.5 b)}.$$

Also sind alle Elemente von $E$ Quadrate. Nun ist $E$ der Kern des kanonischen Gruppenhomomorfismus

$$g : (\mathbb{Z}/p^m)^* \longrightarrow (\mathbb{Z}/p)^*, \quad (a \bmod p^m) \longmapsto (a \bmod p).$$

Sei jetzt $(a \bmod p)$ ein Quadrat in $(\mathbb{Z}/p)^*$, etwa $a \equiv x^2 \pmod p$ mit einem $x \in \mathbb{Z}$. Für die Restklassen $\overline{a} = (a \bmod p^m)$und
$\overline{x} = (x \bmod p^m)$ gilt dann $g(\overline{a}) = g(\overline{x}^2)$, also $\overline{a}(\overline{x}^2)^{-1} = \varepsilon$ mit einem $\varepsilon \in E$.
Wie oben gesehen, ist $\varepsilon = \delta^2$ mit einem $\delta \in (\mathbb{Z}/p^m)^*$. Es folgt
$\overline{a} = (\overline{x} \cdot \delta)^2$, d.h. $\overline{a}$ ist ein Quadrat. Die Umkehrung ist trivial. □

**Satz: 10.25** *Sei $a$ ungerade, $m \in \mathbb{N}_1$. In $(\mathbb{Z}/2^m)^*$ ist $(a \bmod 2^m)$ genau dann ein Quadrat, wenn*

*$a$ beliebig im Falle $m=1$,*

*$a \equiv 1 \pmod 4$ im Falle $m=2$,*

*$a \equiv 1 \pmod 8$ im Falle $m \geq 3$ ist.*

**Beweis:** Der Fall $m=1$ ist trivial.
Die Fälle $m=2,3$ rechnet man wie folgt nach:
$x \equiv \pm 1 \pmod 8 \Longrightarrow x^2 \equiv 1 \pmod 8$;
$x \equiv \pm 3 \pmod 8 \Longrightarrow x^2 \equiv 1 \pmod 8$.
Für $m>3$ ist also $a \equiv 1 \pmod 8$ notwendig dafür, dass $(a \bmod 2^m)$ ein Quadrat ist.

Die Gruppe $G$ der Restklassen $\overline{a} \in (\mathbb{Z}/2^m)^*$ mit $a \equiv 1 \pmod 4$ ist zyklisch von der Ordnung $2^{m-2}$. (9.13)
Die Untergruppe $Q$ der Quadrate in dieser Gruppe $G$ hat die Ordnung $2^{m-3}$.
Die Gruppe $H$ der $\overline{a}$ mit $a \equiv 1 \pmod 8$ ist auch eine Untergruppe von $G$ und hat ebenfalls die Ordnung $2^{m-3}$. Da in einer zyklischen Gruppe zu jeder Ordnung höchstens eine Untergrupe existiert, ist
$H = Q$. D.h. in $G$, also erst recht in $(\mathbb{Z}/2^m)^*$ sind die $\overline{a}$ mit
$a \equiv 1 \pmod 8$ Quadrate. □

## AUFGABEN UND HINWEISE

**1)** a) Ein Designer will eine Verpackung für ein Vielfaches von 10 Kugeln entwerfen. Dabei sollen die Kugeln in einer „Ebene“ „quadratisch“ angeordnet sein, aber – dem interessanteren Design zuliebe – zwei gegenüberliegende Ecken freibleiben.
(Ein Beispiel dieser Anordnung mit 34 Kugeln befindet sich vorne auf dem Buch.)
Können Sie ihm helfen?
Untersuchen sie das Problem, wo 10 durch eine andere ganze Zahl $d$ ersetzt ist. (Etwa für alle $d$ mit $3 \leq d \leq 15$).
b) Variieren Sie das Problem weiter: Alle vier Ecken und ein weiterer Platz sollen freibleiben.

**2)** Seien $p$ eine ungerade Primzahl und $r$ eine Primitivwurzel modulo $p$. Dann ist bekanntlich: $\left(\dfrac{r}{p}\right) = -1.$ (10.1 d)) Insbesondere ist 2 keine Primitivwurzel modulo $p$, wenn $p \equiv \pm 1$ (8) ist. Außerdem ist das Produkt zweier Primitivwurzeln modulo einer ungeraden Primzahl nie eine Primitivwurzel. (Allgemein ist das Produkt zweier Erzeuger einer zyklischen Gruppe gerader Ordnung kein Erzeuger dieser Gruppe. Es liegt nämlich in der Untergruppe vom Index 2.)

**3)** Seien $p$ und $q$ ungerade Primzahlen, $m \in \mathbb{N}_1$ mit $p = 2^m q + 1$.
a) Zeigen Sie: $r$ ist genau dann eine Primitivwurzel modulo $p$, wenn

$$\left(\frac{r}{p}\right) = -1 \quad \text{und} \quad r^{2^{m-1}} \not\equiv \pm 1 \pmod{p}$$

gilt.
b) Der Fall $m = 1$ (d.h. $p = 2q + 1$) ist bereits in 8. A1 untersucht worden. Mit Hilfe von 10.10 kann man durch eine Kongruenzbedingung (an $p$ oder) an $q$ beschreiben, wann 2 oder -2 eine Primitivwurzel modulo $p$ ist.
c) Zeigen Sie, dass für $m \geq 2$ mit $r$ auch $-r$ eine Primitivwurzel modulo $p$ ist.
d) Zeigen Sie, für $m = 2$ (d.h. $p = 4q + 1$) ist 2 (und wegen c) natürlich auch $-2$) eine Primitivwurzel modulo $p$. Falls zusätzlich $q > 3$ d.h. $p \geq 29$ gilt, sind auch 3 und $-3$ Primitivwurzeln.
(Hinweis: Für „2“ reicht 10.10. Für „3“ benutze man das quadratische

Reziprozitätsgesetz und die Voraussetzung, dass $p, q$ beide Primzahlen sind.)
e) Für $m > 2$ ist 2 sicher keine Primitivwurzel modulo $p$ (also auch -2 keine solche). Finden Sie eine hinreichende Bedingung – in Form einer Ungleichung für $q$ – dafür, dass 3 eine Primitivwurzel ist.
f) Es ist unbekannt, ob es unendlich viele Primzahlpaare $p, q$ mit
$p = 2q + 1$ gibt. (Ich glaube, es ist sogar unbekannt, ob es unendlich viele Tripel $(p, q, m)$ mit $p, q \in \mathbb{P}$ und $p = 2^m q + 1$ gibt.)

**4)** (Fermatsche und Mersennesche Primzahlen)
a) Die Summenformel für endliche geometrische Reihen ergibt sich aus einer Darstellung von $1-q^n$ als Produkt $(1-q)\cdot\sum_{i=0}^{n-1} q^i$. Diese Darstellung benutzend, kann man für $a \in \mathbb{N}_2$ zeigen:

i) Wenn $a^n + 1$ prim ist, so ist $a$ gerade und $n = 2^m$ mit einem $m \in \mathbb{N}$.

ii) Wenn $a^n - 1$ prim ist, so ist $a = 2$ und $n$ prim.

(Übrigens sind $6^2 + 1 = 37$ und $6^4 + 1 = 1297$ prim.)
Die Zahlen $F_m := 2^{2^m} + 1$ heißen Fermatsche Zahlen bzw. Fermatsche Primzahlen, soweit sie prim sind. (*Fermat* hatte irrtümlich angenommen, alle $F_m$ wären Primzahlen. Dies ist zwar so für $m = 0, 1, \ldots, 4$. Aber *Euler* hat erkannt, dass $F_5$ nicht prim ist. S.u.)
Die Zahlen $M_p := 2^p - 1$ mit Primzahlen $p$ heißen Mersennesche Primzahlen, soweit sie prim sind. ($M_{11}$ ist keine Primzahl.)

b) Sei $p$ ein Primfaktor von $F_n$ und $n \geq 2$. Nach 6. A3 gilt
$p \equiv 1 \pmod{2^{n+1}}$, da die Ordnung von $(2 \bmod p)$ in $(\mathbb{Z}/p)^*$ gerade $2^{n+1}$ ist. Da aber $(2 \bmod p)$ ein Quadrat in $(\mathbb{Z}/p)^*$ ist (warum?), gibt es in $(\mathbb{Z}/p)^*$ ein Element der Ordnung $2^{n+2}$. Folglich ist $p \equiv 1$ (mod $2^{n+2}$.) Nachdem nun die Menge der möglichen Primteiler von $F_n$ stark eingeschränkt ist, können Sie mit relativ geringem Aufwand nachprüfen, dass $F_4$ prim ist, nicht aber $F_5$. (Verwenden Sie dabei noch A3 a), c) und A5 b).)

c) Für welche $n$ ist $\varphi(n)$ eine Potenz von 2 ?
Für solche $n$ lässt sich das regelmäßige $n$–Eck mit Zirkel und Lineal konstruieren. S. [*Lorenz*] §§1 und 11.

d) Eine Zahl $n \in \mathbb{N}$ heißt vollkommen, wenn sie gleich der Summe aller ihrer positiven echten Teiler ist. (Z.B. $6 = 1 + 2 + 3$ ist vollkommen.)

Zeigen Sie: Eine gerade Zahl $n$ ist genau dann vollkommen, wenn sie von der Form

$$2^{p-1}M_p$$

mit einer Mersenneschen Primzahl $M_p$ ist.

e) Seien $F_n$ prim und $r \in \mathbb{Z}$. Zeigen Sie:
Genau dann ist $r$ eine Primitivwurzel modulo $F_n$. wenn $\left(\dfrac{r}{F_n}\right) = -1$ ist.
Folgern Sie: Für $n \geq 1$ ist 3 eine Primitivwurzel modulo $F_n$.
Für $n \geq 2$ ist 5 eine Primitivwurzel modulo $F_n$, aber 2 nicht.

f) Zeigen Sie: Für jede Primzahl $p$ ist jeder Primfaktor von $M_p$ größer als $p$. (Hieraus folgt die Unendlichkeit der Primzahlmenge.)

g) Es gilt $M_p \equiv 1 \pmod{p}$.

h) Bestimmen Sie $\mathrm{ggT}(M_q, M_p)$.
(Hinweis: 1. A8.)

i) Zeigen Sie $\displaystyle\prod_{k=0}^{n} F_k = F_{n+1} - 2$ .

j) Folgern Sie, dass je 2 verschiedene Fermat-Zahlen zueinander teilerfremd sind. (Auch hieraus folgt die Unendlichkeit der Primzahlmenge)

k) Es ist unbekannt, ob es unendlich viele Fermatsche oder Mersennesche Primzahlen gibt.
Zu Primzahltests für Fermatsche und Mersennesche Zahlen siehe [*Scheid*] III. 10 und IV.4.
Das Gebiet der Fermatschen und Mersenneschen Zahlen hat manche Rechner (lebende und Maschinen) zu allerlei langweiligen sportlichen Höchstleistungen veranlasst.

**5)** a) Seien $a \in \mathbb{Z}$, $r \in \mathbb{N}$.
Zeigen Sie: $a + 1 \mid a^{2r} - 1$.

b) Seien $a \in \mathbb{Z}$, $n, m \in \mathbb{N}$, $n \neq m$. $d = \mathrm{g\,gT}(a^{2^n} + 1, a^{2^m} + 1)$.
Zeigen Sie: Wenn $a$ ungerade ist, ist $d = 2$, wenn $a$ gerade ist, ist $d = 1$.
(Wenn $n < m$ ist, gilt $a^{2^n} + 1 \mid a^{2^m} - 1$). )

**6)** Sei $p$ eine Primzahl.

a) Sei $p \equiv -1 \pmod 4$. Geben Sie eine Lösung der Kongruenz $x^2 \equiv a \pmod p$ in der Form $x = a^r$ an (falls eine Lösung existiert).

b) Sei $p \equiv 5 \pmod 8$. Geben Sie eine Lösung der Kongruenz $x^2 \equiv a \pmod p$ in der Form $x = a^r 2^s$ an (falls eine Lösung existiert).

**7)** Seien $p, q$ ungerade Primzahlen.

a) Bestimmen Sie $\left(\frac{-2}{p}\right)$, $\left(\frac{3}{p}\right)$, $\left(\frac{5}{p}\right)$.

b) Zeigen Sie: $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$.

c) Zeigen Sie:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{für} \quad q \equiv 1 \pmod 4 \\ \left(\frac{-q}{p}\right) & \text{für} \quad q \equiv -1 \pmod 4. \end{cases}$$

**8)** Was gilt, wenn man in 10.20 die Voraussetzung $a \in \mathbb{N}_1$ durch $-a \in \mathbb{N}_1$ ersetzt?

**9)** Seien $p$ eine ungerade Primzahl, $a, b, c \in \mathbb{Z}$ mit $p \nmid a$. Zeigen Sie: Die Kongruenz

$$ax^2 + bx + c \equiv 0 \pmod p$$

hat genau dann eine Lösung, wenn $\left(\frac{b^2 - 4ac}{p}\right) \in \{0, 1\}$ ist.

bf 10) Zeigen Sie, dass für jedes $a \in \mathbb{Z}$ und jede Primzahl $p$ die Kongruenz

$$(x^2+1)(x^4-a^2) \equiv 0 \pmod p$$

lösbar ist.

# § 11

# Etwas mehr Ringtheorie

Auch wenn man nur an Aussagen über den Ring $\mathbb{Z}$ interessiert ist, erweist sich die Betrachtung weiterer Ringe als nützlich. Wir werden deshalb hier die Ringtheorie ein klein wenig ausbauen.

**Bemerkungen: 11.1** a) Für ein Ideal $I$ eines Ringes $A$ gilt:

$$I = A \iff u \in I \quad \text{für ein} \quad u \in A^*.$$

Denn wegen der Idealeigenschaft gilt mit $u \in I$ und $a \in A$ auch
$a = au^{-1}u \in I$.

b) $\{0\}$ ist ein Ideal.

c) Wenn $x \in A$ gilt, ist $Ax = \{ax \mid a \in A\}$ ein Ideal. Denn es ist $0 = 0x \in Ax$ und $ax - a'x = (a - a')x \in A$ für alle $a, a' \in A$ und $b(ax) = (ba)x \in Ax$ für alle $a, b \in A$.

d) Ein Ring $A$ ist genau dann ein Körper, wenn folgendes gilt:
(i) $A \neq \{0\}$, (ii) $\{0\}$ und $A$ sind die einzigen Ideale von $A$.
Denn sei $A$ ein Körper und $I \neq \{0\}$ ein Ideal von $A$, etwa $x \in I - \{0\}$. Da $x$ in dem Körper $A$ eine Einheit ist, folgt $I = A$ mit a).
Ist umgekehrt $x \in A - \{0\}$, so ist $Ax \neq \{0\}$. Wenn jedes Ideal $\neq \{0\}$ schon mit $A$ übereinstimmt, hat man $Ax = A$. Folglich existiert ein $x' \in A$ mit $x'x = 1$.

**Definitionen: 11.2** *a) Ein Hauptideal eines Ringes $A$ ist ein Ideal der Form $Ax$ mit einem $x \in A$.*
*b) Für $a, b \in A$ bedeute $a \mid b$, dass ein $c \in A$ mit $ac = b$ existiert.*

**Bemerkungen: 11.3** a) Jedes Ideal von $\mathbb{Z}$ ist von der Form $m\mathbb{Z}$, also ein Hauptideal.
b) Seien $a, b \in A$, $A$ ein Ring, so hat man:

$$a \mid b \iff Aa \supset Ab.$$

**Definition: 11.4** *Ein Ring $A$ heißt ein Hauptidealring, wenn*
*(i) $A$ nullteilerfrei und*
*(ii) jedes Ideal von $A$ ein Hauptideal ist.*

**Definition: 11.5** *Ein Ring $A$ heißt euklidisch, wenn gilt:*
*(i) $A$ ist nullteilerfrei;*
*(ii) es gibt eine Abbildung*

$$\varepsilon : A \longrightarrow \mathbb{N},$$

*so dass für alle $a, b \in A$ mit $b \neq 0$ Elemente $q, r \in A$ mit*

$$a = bq + r \quad \text{und} \quad \varepsilon(r) < \varepsilon(b)$$

*existieren.*

**Satz: 11.6** *Jeder euklidische Ring ist ein Hauptidealring.*

**Beweis:** Sei $I$ ein Ideal von $A$.
Wenn $I = \{0\}$ ist, so ist $I = A \cdot 0$, also ein Hauptideal.

Sei nun $I \neq \{0\}$ und $x \in I - \{0\}$ so gewählt, dass $\varepsilon(x)$ minimal ist unter allen $\varepsilon(y)$ mit $y \in I - \{0\}$. (Die Menge $\varepsilon(I - \{0\})$ ist eine nichtleere Teilmenge von $\mathbb{N}$, besitzt also ein kleinstes Element.)

*Behauptung:* $I = Ax$.

*Beweis hierfür:* Da $x \in I$ ist, gilt $ax \in I$ für alle $a \in A$, also $Ax \subset I$.

Sei umgekehrt $y \in I$ beliebig.
Nach Voraussetzung gibt es $q, r \in A$ mit $y = qx + r$ und $\varepsilon(r) < \varepsilon(x)$. Mit $y$ und $x$ gehört $r = y - qx$ zu $I$. Da $\varepsilon(r) < \varepsilon(x)$ und $\varepsilon(z) \geq \varepsilon(x)$ für alle $z \in I - \{0\}$ gilt, kann nur $r = 0$ sein. Dann ist aber $y = qx \in Ax$.

$\square$

Wir werden zeigen, dass in Hauptidealringen ein Satz von der eindeutigen Primfaktorzerlegung gilt. Um diesen adäquat formulieren und beweisen zu können, brauchen wir ein paar Vorbereitungen.

**Definitionen: 11.7** *Sei $A$ ein Ring, $x \in A$.*

*a) $x$ heißt (in $A$) irreduzibel, wenn $x \neq 0$ und keine Einheit in $A$, aber bei jeder Zerlegung $x = ab$ einer der beiden Faktoren $a, b$ eine Einheit ist.*
*b) $x$ heißt prim, wenn $x$ weder Einheit noch Null ist und für alle $a, b \in A$ gilt:*

$$x \mid ab \implies x \mid a \quad \textit{oder} \quad x \mid b.$$

**Feststellung: 11.8** *$A$ sei ein Integritätsring und $x \in A$ prim. Dann ist $x$ irreduzibel.*

**Beweis:** Aus $x = ab$ folgt $x \mid ab$ und daraus $x \mid a$ oder $x \mid b$.
Es gelte etwa $x \mid a$, d.h. $xy = a$ für ein $y \in A$. Mit $x = ab$ folgt $aby = a$.
Da $x$ als Primelement von 0 verschieden und $x = ab$ ist, ist auch $a \neq 0$. Aus $aby = a$ folgt deshalb $by = 1$, d.h. $b \in A^*$. □

**Feststellung: 11.9** *Für einen Integritätsring $A$ und $x, y \in A$ sind folgende Aussagen äquivalent:*

*(i) $x \mid y$ und $y \mid x$;*

*(ii) $Ax = Ay$;*

*(iii) es gibt ein $u \in A^*$ mit $ux = y$.*

**Beweis:** Die Äquivalenz von (i) und (ii) folgt mit 11.3b).
(iii) $\Rightarrow$ (i): $ux = y \Rightarrow x \mid y$; $u^{-1}y = x \Rightarrow y|x$.
(i) $\Rightarrow$ (iii): Aus $ax = y$ und $by = x$ folgt $bax = x$. Wenn $x = 0$ ist, so auch $y = ax$, also $1 \cdot x = y$. Wenn $x \neq 0$ ist, folgt aus $bax = x$ die Gleichung $ba = 1$, also $a \in A^*$, und für diese Einheit $a$ gilt $ax = y$. □

**Definition: 11.10** *Elemente $a, b$ eines Integritätsringes heißen (zueinander) assoziiert, wenn sie die äquivalenten Aussagen (i) – (iii) von 11.9 erfüllen.*

**Bemerkungen: 11.11** Seien $a$ zu $a'$ und $b$ zu $b'$ assoziiert, alle zu einem Integritätsring gehörig. So gilt:
a) $a \mid b \iff a' \mid b'$.
b) $a$ ist irreduzibel $\iff$ $a'$ ist irreduzibel.
c) $a$ ist prim $\iff$ $a'$ ist prim.

**11.12 Lemma** (*Euklid*, vgl. 2.4):*In einem Hauptidealring $A$ ist jedes irreduzible Element $x$ auch prim.*

**Beweis** (*Gauß*): Es gelte $x \mid ab$.
Betrachte $I := \{c \in A \;\big|\; x \mid ac\}$. Offenbar ist $I$ ein Ideal mit $b,\ x \in I$. Da $A$ ein Hauptidealring ist, gibt es ein $d \in A$ mit $I = Ad$. Wegen $x \in Ad$ und der Irreduzibilität von $x$ ist $d \in A^*$ oder $d$ zu $x$ assoziiert.

Im ersten Fall folgt aus $x \mid ad$ schon $x \mid a$. Im zweiten Fall folgt aus $d \mid b$, dass $x \mid b$ gilt. □

Das folgende, etwas abstrakte Lemma wird nur benötigt, wenn man die Existenz von Primfaktorzerlegungen für allgemeine Hauptidealringe zeigen will. Für die Ringe,welche in diesem Buch betrachtet werden, wird hierfür ein gesonderter Beweis gegeben werden.

**Lemma: 11.13** *In einem Hauptidealring $A$ werden aufsteigende Folgen von Idealen stationär. D.h. wenn für Ideale $I_j$ gilt*

$$I_0 \subset I_1 \subset I_2 \subset \ldots,$$

*so gibt es ein $n \in \mathbb{N}$ mit $I_{n+i} = I_n$ für alle $i \in \mathbb{N}$.*

**Beweis:** Sei $I := \bigcup\limits_{i \in \mathbb{N}} I_i$. Obwohl im allgemeinen eine Vereinigung von Idealen kein solches ist, gilt in diesem Fall doch die

*Behauptung:* $I$ ist ein Ideal.

*Beweis hierfür:* Zunächst ist $0 \in I_0 \subset I$. Wenn ferner $x \in I$ ist, gilt $x \in I_n$ für ein $n$ und deshalb $ax \in I_n \subset I$ für jedes $a \in A$.
Seien schließlich $x, y \in I$, etwa $x \in I_n$, $y \in I_m$. Es ist $n \leq m$ oder $m \leq n$, etwa $n \leq m$. Dann ist auch $I_n \subset I_m$, also $x, y \in I_m$ und deshalb $x - y \in I_m \subset I$.

Da $A$ ein Hauptidealring ist, gilt $I = Ax$ für ein $x \in I$. Nun gibt es ein $n$ mit $x \in I_n$. Für dieses gilt $I = Ax \subset I_n \subset I$. Somit ist auch $I \subset I_{n+i} \subset I$ für alle $i \in \mathbb{N}$. $\square$

**Satz: 11.14** *In einem Hauptidealring $A$ gilt die eindeutige Primfaktorzerlegung. D.h.:*
*Sei $a \in A - \{0\}$. Dann gibt es ein $u \in A^*$ und Primelemente $p_1, \ldots, p_n$ mit*

$$a = u \cdot p_1 \cdot \ldots \cdot p_n. \quad (n \geq 0.)$$

*Diese Zerlegung ist im wesentlichen eindeutig; d.h. wenn auch $a = vq_1 \cdot \ldots \cdot q_m$ mit $v \in A^*$ und Primelementen $q_1, \ldots, q_m$ gilt, folgt:*
*Es ist $n = m$, und es gibt eine Permutation $\sigma \in S_n$, derart dass $p_i$ zu $q_{\sigma(i)}$ für jedes $i = 1, \ldots, n$ assoziiert ist.*

**Beweis:** Zur Existenz der Zerlegung:

Zunächst geben wir einen Beweis, der für diejenigen Ringe ausreicht, die in diesem Buch behandelt werden. Diese Ringe sind nämlich sämtlich euklidisch mit einem euklidischen Maß $\varepsilon$, für welches gilt:

*Ist $a = bc$ und $c$ keine Einheit, so ist $\varepsilon(b) < \varepsilon(a)$.*

Angenommen in dem euklidischen Ring $A$ mit der angegebenen Eigenschaft gebe es Elemente $\neq 0$ ohne eine Zerlegung in eine Einheit und irreduzible Faktoren. Sei $a$ eine solches mit minimalem $\varepsilon(a)$. Dann ist $a$ weder eine Einheit noch irreduzibel. Also gibt es Nichteinheiten $b, c$ mit $a = bc$. Nach Voraussetzung ist dann $\varepsilon(b) < \varepsilon(a)$ und $\varepsilon(c) < \varepsilon(a)$. Wegen der Minimalität von $\varepsilon(a)$ sind dann $b$ und $c$ wie angegeben zerlegbar, deshalb aber auch $a$. Widerspruch!

Nun zum Beweis des allgemeinen Falles:

Wir nehmen an, die Menge $M$ derjenigen Ideale $Aa$ mit einem nicht wie angegeben in irreduzible Faktoren zerlegbaren $a$ sei nicht leer.
Es gibt in $M$ ein maximales Element $Aa_0$; d.h. $Aa_0 \subsetneqq Ab$ impliziert $Ab \notin M$. Sonst könnte man, ausgehend von einem beliebigen $Aa_1 \in M$, eine unendliche

echt aufsteigende Folge

$$Aa_1 \subsetneqq Aa_2 \subsetneqq Aa_3 \subsetneqq \ldots$$

bilden – im Widerspruch zu 11.13.
Sei also $Aa_0$ maximal in $M$.
Das Element $a_0$ ist weder eine Einheit noch irreduzibel; sonst wäre es wie angegeben zerlegbar, mit $n = 0$ oder $n = 1$. Somit ist $a_0$ echt zerlegbar:

$$a_0 = bc \quad \text{mit} \quad b, c \notin A^*.$$

Dann ist aber $Aa_0 \subsetneqq Ab$ und $Aa_0 \subsetneqq Ac$. Wegen der Maximalität von $Aa_0$ sind dann $b$ und $c$ in irreduzible Faktoren zerlegbar; also ist es auch $a_0$ – ein Widerspruch.

Somit ist $M$ leer und die Existenz von Zerlegungen gezeigt.

Die Eindeutigkeit wird so bewiesen wie in 2.6.
Aus $up_1 \cdot \ldots \cdot p_n = vq_1 \cdot \ldots \cdot q_m$ folgt $p_1 \mid vq_1 \cdot \ldots \cdot q_m$.
Da $p_1$ prim ist, teilt $p_1$ einen der Faktoren $v, q_1, \ldots, q_m$, aber nicht $v$, da $p_1$ sonst eine Einheit wäre. Es gelte etwa $p_1 \mid q_1$, d.h. $p_1 w_1 = q_1$ für ein $w_1 \in A$. Da $q_1$ irreduzibel, ist $w_1 \in A^*$, also $p_1$ zu $q_1$ assoziiert. Durch Kürzen erhält man:

$$up_2 \cdot \ldots \cdot p_n = v \cdot w_1 \cdot q_2 \cdot \ldots \cdot q_m,$$

wo $vw_1$ eine Einheit ist.
Durch Induktion nach $n$ erhält man die Eindeutigkeitsaussage des Satzes. □

**Bemerkungen: 11.15** a) Wir haben oben zweierlei gezeigt: Jeder euklidische Ring ist ein Hauptidealring, und in jedem Hauptidealring gilt der Satz von der eindeutigen Primfaktorzerlegung. Die Umkehrungen dieser Aussagen gelten nicht. Hierauf wollen wir nicht weiter eingehen.

b) Als Beispiele für euklidische Ringe kennen wir bereits:

1) $\mathbb{Z}$ mit $\varepsilon(n) = |n|$,

2) $k[x]$, wo $k$ ein Körper ist mit

$$\varepsilon(f) = \begin{cases} 0, & \text{falls } f = 0 \\ 1 + \text{grad}(f), & \text{falls } f \neq 0 \text{ ist.} \end{cases}$$

Diese Polynomringe über Körpern werden im vorliegenden Buch nicht mehr betrachtet, sind aber für die Algebra äußerst wichtig. Für uns werden folgende Beispiele euklidischer Ringe noch eine Rolle spielen:

3) Der Gaußsche Zahlenring

$$\mathbb{G} := \mathbb{Z} + \mathbb{Z}i = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

und

4) $\mathbb{Z} + \mathbb{Z} \cdot \zeta = \{a + b\zeta \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$;
wo $\zeta \left(= \frac{1}{2}(-1 + i\sqrt{3})\right)$ eine nichttriviale dritte Einheitswurzel ist, d.h. $\zeta \neq 1$, aber $\zeta^3 = 1$ gilt.

Dass diese Ringe euklidisch sind, wird in den nächsten Paragrafen gezeigt – und ausgenutzt.

AUFGABEN UND HINWEISE

**1)** Sei $K$ ein Körper. Bestimmen Sie die Einheiten von $K[X]$.
Wann sind zwei Polynome über $K$ assoziiert?

**2)** a) Zeigen sie: Es gibt unendlich viele paarweise nichtassoziierte irreduzible Polynome in $K[X]$. (Vgl. 3.1.)
b) Eine weitere Anwendung der euklidischen Idee führt zum Beweis des folgenden Satzes:
*Sei $f \in \mathbb{Z}[X] - \mathbb{Z}$, d.h. ein nicht konstantes Polynom mit ganzen Koeffizienten. Modulo unendlich vielen Primzahlen hat $f$ eine Nullstelle. D.h. es gibt unendlich viele Primzahlen $p$, für die ein $n \in \mathbb{Z}$ mit $p|f(n)$ existiert.*
Beweisen Sie dies zunächst unter der Voraussetzung $f(0) = 1$ – nach Euklid. Durch eine Modifikation von $f$ können Sie (außer im trivialen Fall $f(0) = 0$) den allgemeinen Fall auf den Spezialfall zurückzuführen.

**3)** Eine Teilmenge $M$ der Ebene, oder allgemeiner des $\mathbb{R}^n$, heißt konvex, wenn mit je zwei Punkten auch deren Verbindungsstrecke zu $M$ gehört. (Die Verbindungsstrecke von 2 Punkten $x, y \in \mathbb{R}^n$ ist die Menge $\{\lambda x+\mu y \mid \lambda, \mu \geq 0, \ \lambda + \mu = 1\}$.) Sei

$$M_0 \subset M_1 \subset \dots$$

eine aufsteigende Folge konvexer Teilmengen. Zeigen Sie:
$\bigcup\limits_{i\in\mathbb{N}} M_i$ ist ebenfalls konvex. (Vgl. Beweis von 11.13.)

**4)** Die Behauptung des Lemmas 11.13 gilt unter der allgemeineren Voraussetzung, dass die Ideale von $A$ endlich erzeugt sind; sie ist sogar dazu äquivalent. (Vgl. z.B. [*Brüske–Ischebeck–Vogel*] 3.2.)

**5)** a) Sei $A$ ein Ring mit eindeutiger Primfaktorzerlegung. Zeigen Sie:
Für $n \in \mathbb{N}_1, \ \ a, b \in A$ gilt:

$$a^n \mid b^n \Longrightarrow a \mid b.$$

b) Folgern Sie: Sei $m \in \mathbb{N}_2$. Im Ring

$$\{a + mbi \quad | \quad a, b \in \mathbb{Z}\}$$

gilt die eindeutige Primfaktorzerlegung nicht! (Überzeugen Sie sich davon, dass wirklich ein Ring vorliegt.)

# § 12

# Der Gaußsche Zahlenring und Summen zweier Quadrate

Wir betrachten hier den schon zweimal erwähnten Gaußschen Zahlenring

$$\mathbb{G} := \{a + bi \quad | \quad a, b \in \mathbb{Z}\},$$

wo $i$ die imaginäre Einheit bezeichnet, also $i^2 = -1$ gilt.

In der Gaußschen Zahlenebene, deren Punkte beliebige komplexe Zahlen bedeuten, bilden die Elemente von $\mathbb{G}$ ein sogenanntes Gitter:

Abb. 12

**Definition: 12.1** *Sei $\alpha := a + bi$, $a, b \in \mathbb{Z}$ (bzw. $\mathbb{R}$).*
*a) Definiere $\overline{\alpha} := a - bi$. Die Zahl $\overline{\alpha}$ heißt das Konjugierte von $\alpha$, die Abbildung*

$$\mathbb{G} \longrightarrow \mathbb{G} \quad (bzw. \quad \mathbb{C} \longrightarrow \mathbb{C}), \quad \alpha \longmapsto \overline{\alpha}$$

*heißt Konjugation. (Anschaulich gesprochen, ist sie die Spiegelung des Gitters $\mathbb{G}$ (bzw. der Gaußschen Zahlenebene) an der reellen Achse.*

*b) Definiere $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{N}$ (bzw. $\mathbb{R}_+$). Man nennt $N(\alpha)$ die Norm von $\alpha$ und $N : \mathbb{G} \longrightarrow \mathbb{N}$ (bzw. $\mathbb{C} \longrightarrow \mathbb{R}_+$) die Norm (-abbildung).*

**Bemerkung: 12.2** Mit der üblichen Betragsfunktion $| \quad |$ (die anschaulich den Abstand eines Punktes von 0 beschreibt) gilt: $N(\alpha) = |\alpha|^2$. Beachte, dass $|1 + i| = \sqrt{2}$ ist und somit die Betragsfunktion den Ring $\mathbb{G}$ nicht in $\mathbb{Z}$ abbildet.

**Feststellung: 12.3** *Konjugation und Norm haben folgende Eigenschaften:*
*a) $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$;*
*b) $\overline{\alpha} \cdot \overline{\beta} = \overline{\alpha\beta}$;*
*c) $\overline{1} = 1$ .*
*d) Die Konjugation ist ein Isomorfismus des Ringes $\mathbb{G}$ (bzw. Körpers $\mathbb{C}$) zu sich selbst, ein sogenannter Automorfismus.*
*e) $N(\alpha) = 0 \iff \alpha = 0$;*
*f) $N(\alpha\beta) = N(\alpha)N(\beta)$;*
*g) für $\alpha \in \mathbb{G}$ gilt: $\alpha \in \mathbb{G}^* \iff N(\alpha) = 1$.*

**Beweis:** a) und c) sind trivial, und b) ist leicht nachzurechnen.
d) folgt aus a), b) und c) und daraus, dass die Konjugation offensichtlich bijektiv ist.
e) $N(a+bi) = a^2+b^2$ für $a, b \in \mathbb{R}$. Eine Summe von Quadraten reeller Zahlen ist genau dann Null, wenn diese selbst es sind.
f) ergibt sich sofort aus b) und der Kommutativität und Assoziativität der Multiplikation.
g) Wenn $N(\alpha) = 1$ ist, ist $\alpha\overline{\alpha} = 1$, also $\alpha$ eine Einheit, da mit $\alpha$ auch $\overline{\alpha}$ zu

$\mathbb{G}$ gehört.
Umgekehrt, wenn $\alpha \in \mathbb{G}^*$ ist, gibt es ein $\beta \in \mathbb{G}$ mit $\alpha\beta = 1$, also $N(\alpha) \cdot N(\beta) = N(\alpha\beta) = 1$. Das Produkt der natürlichen Zahlen $N(\alpha)$ und $N(\beta)$ kann aber nur dann 1 sein, wenn beide Zahlen selbst es sind. □

**Korollar: 12.4** $\mathbb{G}^* = \{1, -1, i, -i\}$.

Denn nur die angegebenen 4 Elemente aus $\mathbb{G}$ haben die Norm 1. □

**Bemerkungen: 12.5** a) Ein Element von $\mathbb{Z}$ ist offenbar genau dann in $\mathbb{Z}$ eine Summe zweier Quadrate, wenn es von der Form $N(\alpha)$ mit einem $\alpha \in \mathbb{G}$ ist. (Dabei ist der Summand $0^2$ nicht ausgeschlossen: $1 = 0^2+1^2$, $4 = 0^2+2^2$.)

b) Aus a) und der Identität $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ folgt, dass $ab$ in $\mathbb{N}$ eine Summe von 2 Quadraten ist, wenn $a$ und $b$ es sind.

c) Nicht jede natürliche Zahl ist in $\mathbb{Z}$ eine Summe zweier Quadrate. Denn in $\mathbb{Z}/4$ sind $\overline{0}$ und $\overline{1}$ die einzigen Quadrate. Wenn also
$n \equiv -1 \pmod 4$ ist, ist $n$ nicht Summe zweier Quadrate.

d) Jedes Element $\alpha \in \mathbb{G} - \{0\}$ ist zu genau 4 Elementen assoziiert: $\alpha, -\alpha, i\alpha, -i\alpha$. Von diesen 4 Elementen liegt genau eines in dem Quadranten $\{x + yi \mid x > 0,\ y \geq 0\}$.
Dies ist anschaulich klar, weil die Multiplikation mit $i$ (bzw. $-1$, bzw. $-i$) die Drehung der Gaußschen Zahlenebene um den Nullpunkt mit dem Winkel $\pi/2$ (bzw. $\pi$, bzw. $3\pi/2$) bedeutet.
Man kann sich jedoch auch ohne Anschauung leicht von obiger Behauptung überzeugen.

**Satz: 12.6** *Der Ring $\mathbb{G}$ ist euklidisch. Genauer gilt: Zu $a, b \in \mathbb{G}$, $b \neq 0$ gibt es $q, r \in \mathbb{G}$ mit*

*1)* $a = bq + r$ *und* *2)* $N(r) \leq \frac{1}{2}N(b)$.

**Beweis:** In $\mathbb{C}$ können wir $a$ durch $b$ (ohne Rest) dividieren:

$$\frac{a}{b} = x + iy =: z \quad \text{mit} \quad x, y \in \mathbb{R}.$$

(Es ist sogar $x, y \in \mathbb{Q}$, wie der Leser sich überlegen möge.)
Es gibt $m, n \in \mathbb{Z}$ mit $|x - m| \leq \frac{1}{2}$ und $|y - n| \leq \frac{1}{2}$. (Z.B. sei $m = [x]$, wenn

$x \leq [x] + \frac{1}{2}$ und $m = [x] + 1$, wenn $x > [x] + \frac{1}{2}$.)
Setze $q := m + in$.
Mit $z = x + iy$ gilt dann:

$$\begin{array}{rcl} a - bz & = & 0 \quad \text{und} \\ N(z-q) & = & (x-m)^2 + (y-n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}. \end{array}$$

Mit $r := a - bq$ folgt

$$\begin{array}{rcl} N(r) & = & N(a - bq) = N(a - bz + bz - bq) \\ & = & N(bz - bq) = N(b) \cdot N(z - q) \leq \frac{1}{2} N(b). \end{array}$$ □

**12.7** Der Ring $\mathbb{G}$ ist also ein Hauptidealring. Somit ist jedes irreduzible Element in $\mathbb{G}$ auch prim, und es gilt der Satz von der eindeutigen Primfaktorzerlegung. Wir wollen die Primelemente in $\mathbb{G}$ bestimmen.

**Definition: 12.8** *Die Primelemente von $\mathbb{G}$ heißen Gaußsche Primzahlen. Der Deutlichkeit halber werden die Primzahlen aus $\mathbb{N}$, d.h. diejenigen im bisherigen Sinne, auch rationale Primzahlen genannt.*

(In $\mathbb{Z}$ hatten wir nur die positiven Primelemente Primzahlen genannt. Jedes negative Primelement ist ja zu einer (positiven) Primzahl assoziiert. In $\mathbb{G}$ tun wir dies nicht. Denn so kanonisch die Auszeichnung der positiven ganzen Zahlen in $\mathbb{Z}$ ist, so wenig kanonisch wäre etwa die Auszeichnung des Quadranten $\{x + iy \mid x > 0, \; y \geq 0\}$ in $\mathbb{G}$.)

**Feststellung: 12.9** *Wenn $\alpha \in \mathbb{G}$ und $N(\alpha)$ eine rationale Primzahl ist, dann ist $\alpha$ eine Gaußsche Primzahl.*

**Beweis:** Sei $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{G}$. Dann ist $N(\alpha) = N(\beta) \cdot N(\gamma)$ gemäß 12.3 f), also $N(\beta) = 1$ oder $N(\gamma) = 1$, da $N(\alpha)$ prim in $\mathbb{N}$ ist. Es folgt, dass $\beta$ oder $\gamma$ eine Einheit in $\mathbb{G}$, also $\alpha$ irreduzibel in $\mathbb{G}$, d.h. eine Gaußsche Primzahl ist. □

**Beispiel: 12.10** $1 + i$ ist eine Gaußsche Primzahl, da $N(1 + i) = 2$ ist. Wegen $1 - i = -i(1 + i)$ ist $1 - i$ zu $1 + i$ assoziiert. Eine Primfaktorzerlegung von 2 in $\mathbb{G}$ ist also $2 = (-i)(1 + i)^2$. Die weiteren zu $1 + i$ assoziierten Zahlen sind $-1 \pm i$.

**Satz: 12.11** *Sei $p$ eine ungerade rationale Primzahl. Dann ist $p$ entweder auch eine Gaußsche Primzahl oder die Norm einer Gaußschen Primzahl, $p = q \cdot \overline{q}$. In diesem Falle sind $q$ und $\overline{q}$ zueinander nicht assoziierte Gaußsche Primzahlen, und $p = q \cdot \overline{q}$ ist eine Primfaktorzerlegung in $\mathbb{G}$.*

**Beweis:** Wir betrachten eine Primfaktorzerlegung von $p$ in $\mathbb{G}$, etwa $p = uq_1 \cdot \ldots \cdot q_r$ mit $u \in \mathbb{G}^*$ und Gaußschen Primzahlen $q_1, \ldots, q_r$.
Wegen $N(u) = 1$ nach 12.3 g) ist also $p^2 = N(p) = N(q_1) \cdot \ldots \cdot N(q_r)$.
Hieraus folgt $1 \leq r \leq 2$, da genau die Einheiten in $\mathbb{G}$ die Norm 1 haben.

1. Fall: $r = 1$, d.h. $p = uq_1$.
In diesem Fall ist $p$ zu einer Gaußschen Primzahl, nämlich $q_1$, assoziiert, also selbst eine Gaußsche Primzahl.

2. Fall: $r = 2$, d.h. $p = uq_1 \cdot q_2$.
Aus $p^2 = N(q_1) \cdot N(q_2)$ folgt dann $N(q_1) = N(q_2) = p$, da $N(q_i) > 1$ ist. Für $q = q_1$ gilt also $p = q \cdot \overline{q}$. Da die Konjugation ein Isomorfismus von $\mathbb{G}$ auf sich selbst ist, ist mit $q$ auch $\overline{q}$ eine Gaußsche Primzahl.
Wir haben noch auszuschließen, dass $q$ zu $\overline{q}$ assoziiert ist, und setzen $q = x + iy$ mit $x, y \in \mathbb{Z}$, also $\overline{q} = x - iy$. Angenommen, es wäre $uq = \overline{q}$ mit einem $u \in \mathbb{G}^*$.
Im Falle $u = \pm 1$ wäre $y = 0$ oder $x = 0$, also $p = q\overline{q} = x^2$ oder $y^2$, also ein Quadrat in $\mathbb{Z}$ und deshalb $p$ keine rationale Primzahl.
Im Falle $u = \pm i$ wäre $x = \mp y$, also $p = q\overline{q} = 2x^2$ und deshalb $p$ keine ungerade rationale Primzahl. $\square$

**12.12** Welche rationalen Primzahlen sind nun Gaußsche Primzahlen, und welche sind Normen Gaußscher Primzahlen?

**Satz:** *Sei $p$ eine ungerade rationale Primzahl. Dann gilt:*
*Ist $p \equiv -1 \pmod 4$, so ist $p$ eine Gaußsche Primzahl.*
*Ist $p \equiv 1 \pmod 4$, so ist $p$ die Norm einer Gaußschen Primzahl.*

**Beweis:** Ist $p \equiv -1 \pmod 4$, so ist $p$ in $\mathbb{Z}$ nicht Summe zweier Quadrate nach 12.5 c), d.h. $p$ ist nicht die Norm irgendeiner Zahl aus $\mathbb{G}$. Gemäß 12.11 muss $p$ eine Gaußsche Primzahl sein.
Ist $p \equiv 1 \pmod 4$, so müssen wir zeigen, dass $p$ keine Gaußsche Primzahl ist.
Aus $p \equiv 1 \pmod 4$ folgt nun $\left(\frac{-1}{p}\right) = 1$ nach 10.5. D.h. es gibt ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod p$, also $p \mid x^2 + 1 = (x + i)(x - i)$. Wäre $p$ eine Gaußsche

Primzahl, so folgte $p \mid x+i$ oder $p \mid x-i$. Das geht aber nicht. Denn für beliebige $a, b \in \mathbb{Z}$ ist $p \cdot (a+bi) = pa + pbi$ mit $pb \neq \pm 1$, da $p$ eine rationale Primzahl ist. □

**Korollar: 12.13** *Sei $q$ eine Gaußsche Primzahl. Dann gilt genau eine der drei folgenden Aussagen:*

*(i)* *$q$ ist assoziiert zu $1+i$ (d.h. $q = \pm 1 \pm i$);*

*(ii)* *$N(q)$ ist eine rationale Primzahl $p$ und $p \equiv 1 \pmod 4$;*

*(iii)* *$q$ ist assoziiert zu einer rationalen Primzahl $p$ mit $p \equiv -1 \pmod 4$.*

**Beweis:** Da $q$ eine Gaußsche Primzahl ist, teilt $q$ einen der rationalen Primfaktoren der natürlichen Zahl $q\overline{q}$. Dieser heiße $p$. Dann ist entweder $q$ zu $p$ assoziiert oder $p = q'\overline{q'}$ mit einer zu $q$ assoziierten Zahl $q'$. Im letzteren Fall ist $p = N(q') = N(q)$, also entweder $p = 2$ oder
$p \equiv 1 \pmod 4$. □

**Korollar: 12.14** *Eine rationale Primzahl $p$ ist in $\mathbb{N}$ eine Summe zweier Quadrate genau dann, wenn $p = 2$ oder $p \equiv 1 \pmod 4$ ist. Eine solche Darstellung ist bis auf die Reihenfolge eindeutig.*

**Beweis:** Wenn $p$ von der Form $a^2+b^2$ mit $a, b \in \mathbb{N}$ ist, gilt $p = (a+bi)(a-bi)$. Also ist $p$ in $\mathbb{G}$ nicht irreduzibel und deshalb $p = 2$ oder $p \equiv 1 \pmod 4$. Umgekehrt ist in diesen Fällen $p$ die Norm einer Gaußschen (Prim–) Zahl, also Summe von Quadraten.
Zur Eindeutigkeit: Man hat in obigen Fällen in $\mathbb{G}$ eine Primfaktorzerlegung $p = q \cdot \overline{q}$ mit einer Gaußschen Primzahl $q$. Ist nun $p = a^2+b^2 = (a+bi)(a-bi)$, so muss $a+bi$ wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{G}$ eine zu $q$ oder $\overline{q}$ assoziierte Gaußsche Primzahl sein. Man überlegt sich nun leicht, dass die Darstellung $p = a^2+b^2$ nicht wesentlich von der durch $p = q\overline{q}$ bestimmten Darstellung von $p$ als Summe zweier Quadrate verschieden ist. □

**Korollar: 12.15** *Sei $n \in \mathbb{N}_1$. Genau dann ist $n$ in $\mathbb{N}$ eine Summe zweier Quadrate, wenn für jede rationale Primzahl $p \equiv 3 \pmod 4$ die Vielfachheit $v_p(n)$ gerade ist.*

**Beweis:** „$\Leftarrow$“: Nach Voraussetzung ist $n$ von der Form $n = m^2 p_1 \cdot \ldots \cdot p_r$ mit rationalen Primzahlen $p_i \equiv 1 \pmod 4$. Letztere sind Summen je zweier Quadrate und $m^2 = m^2 + 0^2$ auch. Nach 12.5 b) ist deshalb auch $n$ eine solche.
„$\Rightarrow$“: Nach Voraussetzung ist $n = N(\alpha)$ mit einem $\alpha \in \mathbb{G}$. Sei $\alpha = uq_1 \cdot \ldots \cdot q_s$ eine Primfaktorzerlegung in $\mathbb{G}$. Dann ist

$$n = N(u)N(q_1) \cdot \ldots \cdot N(q_s) = N(q_1) \cdot \ldots \cdot N(q_s).$$

Für $i \in \{1, \ldots, s\}$ ist entweder $N(q_i) = 2$ oder $N(q_i)$ eine rationale Primzahl $p_i \equiv 1 \pmod 4$, oder es ist $q_i$ zu einer rationalen Primzahl
$p_i \equiv -1 \pmod 4$ assoziiert, also $N(q_i) = p_i^2$. Die modulo 4 zu 3 kongruenten rationalen Primfaktoren von $n$ treten also in gerader Potenz auf. $\square$

**Korollar: 12.16** *Seien $m, n \in \mathbb{N}_1$ und $m^2 n$ in $\mathbb{N}$ eine Summe zweier Quadrate, so ist auch $n$ eine solche.*

**Korollar: 12.17** *Sei $n \in \mathbb{N}$, $n = r_1^2 + r_2^2$ mit $r_1, r_2 \in \mathbb{Q}$. Dann gibt es auch $a_1, a_2 \in \mathbb{N}$ mit $n = a_1^2 + a_2^2$.*

**Beweis:** Aus $n = \dfrac{m_1^2}{c_1^2} + \dfrac{m_2^2}{c_2^2}$ folgt $n(c_1c_2)^2 = (m_1c_2)^2 + (m_2c_1)^2$. Mit Hilfe von 12.16 ergibt sich die Behauptung. $\square$

**Bemerkung: 12.18** Mit 12.14 kann man schnell feststellen, ob eine Primzahl Summe zweier Quadrate ist oder nicht. Man hat allerdings mit dieser Entscheidung eine solche Darstellung noch nicht gefunden. Bei Zahlen, deren Primfaktorzerlegung unbekannt ist, braucht man nicht viel mehr Zeit, über die Darstellbarkeit als Summe zweier Quadrate durch Probieren zu entscheiden und dabei gegebenenfalls eine solche Darstellung zu finden, als einen einzigen Primfaktor durch Probieren zu finden. Das Korollar 12.15 ist also von „nur“ theoretischem Gewicht.
Andererseits, wer will schon von einer einzelnen konkreten Zahl wirklich wissen, ob und auf welche Weise sie als Summe von zwei Quadraten darstellbar ist?

AUFGABEN UND HINWEISE

**1)** Angenommen, jemand besitzt $n$ quadratische Steinplatten. Er kann mit ihnen zwar 2 quadratische Flächen (gleichzeitig) vollständig bedecken, ohne dass Platten übrigbleiben, aber dasselbe gelingt ihm mit keiner rechteckigen Fläche, die mindestens 2 Plattenbreiten breit ist.
Von welcher Art ist die Zahl $n$ ?

**2)** a) Sei $G$ eine endliche Untergruppe der Einheitengruppe eines nullteilerfreien Ringes. Bestimmen Sie $\sum\limits_{u \in G} u$.
Dabei ist zwischen $\#G = 1$ und $\#G > 1$ zu unterscheiden.
(Betrachten sie $v \cdot \sum\limits_{u \in G} u$ für ein $v \in G - \{1\}$. Was ist $\{vu \mid u \in G\}$ ?)

b) Wie kann man den Mittelpunkt eines regelmäßigen $n$–Ecks in $\mathbb{C}$ aus seinen Eckpunkten berechnen?

**3)** a) Sei $K$ ein Teilkörper von $\mathbb{C}$, aufgefasst als Punktmenge in der Gaußschen Zahlenebene. Zeigen Sie: Genau dann gibt es ein regelmäßiges (nicht zu einem Punkt entartetes) $n$–Eck, dessen Eckpunkte in $K$ liegen, wenn $\zeta_n := \exp(2\pi i/n) \in K$ gilt. (Man kann 2)b) benutzen, braucht es aber nicht zu tun.)

b) Man kann daraus folgern, dass $n$ (verschiedene) Punkte von $\mathbb{G}$ für $n \geq 3$, $n \neq 4$ nie die Eckpunkte eines regelmäßigen $n$–Ecks sein können. Dies gilt auch, wenn man $\mathbb{G}$ durch seinen „Quotientenkörper“ $K = \mathbb{Q} + \mathbb{Q}i$ ersetzt.
Für $n = 3$ sehen Sie, dass $\zeta_3 = \exp\frac{2\pi i}{3} \notin K$ ist, indem Sie $\zeta$ in der Form $a + bi$ mit reell–algebraischen $a, b$ bestimmen. (Vgl. §15.)
Daraus ergibt sich die Behauptung auch für $n = 6$.
Für die anderen $n$ kommt man mit ein wenig Algebra zum Ziel. Vergleichen Sie die Grade von $K$ über $\mathbb{Q}$ und von $\zeta_n$ über $\mathbb{Q}$. Siehe [*Lorenz*] §9.

**4)** Geben Sie konkret an, wie man aus Darstellungen zweier (natürlicher) Zahlen als Summe von je zwei Quadraten eine entsprechende Darstellung ihres Produktes bekommt.

**5)** In $\mathbb{Z}$ sei $m = a^2 + b^2$ mit $\mathrm{ggT}(a, b) = 1$. Zeigen Sie:
Jeder positive Teiler von $m$ besitzt ebenfalls eine Darstellung als Summe zweier teilerfremder Quadrate in $\mathbb{Z}$.

**6)** Zeigen Sie: Zu jedem $n \in \mathbb{N}_1$ gibt es $a, b, c \in \mathbb{N}_1$ mit $a^2 + b^2 = c^n$.
(Wenn $c$ Summe zweier Quadrate ist, dann auch $c^n$. Aber einer der Summanden könnte 0 sein! Bei den Beweisen, die mir vorschweben, verwendet man die Ungleichung $\arctan x < x$ für $x > 0$, bzw. A3 b).)

**7)**

Abb. 13

Konstruieren Sie ein „Denkmal" von der oben angedeuteten schlichten Art: ein Würfel auf 2 Platten mit quadratischer Grundfläche. Dabei sollen die Höhe jeder Platte 1 Fuß, alle Kantenlängen in Fuß gemessen ganzzahlig und das Volumen des Würfels gleich dem Gesamtvolumen beider Platten zusammen sein.

**8)** Sei $\alpha \in \mathbb{G}$. Bestimmen sie alle Paare $(x, y) \in \mathbb{G}^2$ mit

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

(Man kann sich auf den Fall beschränken, dass $x, y$ keinen gemeinsamen Primteiler haben. Dann ist aber auch $xy$ teilerfremd zu $x^2 + y^2$.)

**9)** Wir haben hier mit Hilfe des Studiums des Gaußschen Zahlenringes gezeigt, dass jede Primzahl $p \equiv 1 \pmod 4$ Summe zweier Quadrate ist.

Es gibt verschiedene elementarere Beweise hierfür: [*Scholz–Schoeneberg*] §19, Satz 50, [*Scharlau–Opolka*] p. 11ff., [*Scheid*] IV.5 Satz 12. Wir deuten hier einen Beweis von *D. Zagier* an, den Sie ausführen mögen: Wir betrachten die Menge:

$$S := \left\{ (x, y, z) \in \mathbb{N}_1^3 \quad \middle| \quad x^2 + 4yz = p \right\}.$$

Offenbar ist $S$ endlich. Auf $S$ betrachten wir die Involution

$$i : S \longrightarrow S$$

mit

$$i(x, y, z) := \begin{cases} (x + 2z, z, y - x - z) & \text{für} \quad x < y - z \\ (2y - x, y, x - y + z) & \text{für} \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{für} \quad x > 2y. \end{cases}$$

(Eine Involution auf einer Menge $M$ ist eine Abbildung $i : M \longrightarrow M$ mit $i^2 := i \circ i = id_M$. Sie ist immer bijektiv.) Da $i$ genau einen Fixpunkt hat, ist $\#S$ ungerade. Also hat die Involution $j : S \longrightarrow S$,
$(x, y, z) \longmapsto (x, z, y)$ mindestens einen Fixpunkt. (Vgl. 6. A2.)

# § 13

# Der Satz von Lagrange

In diesem Paragrafen wird bewiesen, dass jede natürliche Zahl eine Summe von 4 Quadraten ist. Vorher jedoch wollen wir einen Blick auf die Frage werfen, welche natürlichen Zahlen Summen dreier Quadrate sind.

**Satz: 13.1** *Sei $m \in \mathbb{N}$ Summe dreier Quadrate. Dann ist*
$m \neq 4^k(8n+7)$ *für alle* $k, n \in \mathbb{N}$.

**Beweis:** Die Quadrate in $\mathbb{Z}/8$ sind $\overline{0}, \overline{1}$ und $\overline{4}$. Die Summen von je drei solchen sind somit $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$, aber nicht $\overline{7}$. Also ist keine natürliche Zahl der Form $8n+7$ eine Summe von 3 Quadraten. Der Rest ergibt sich durch Induktion nach $k$ aus der

*Behauptung:* Ist $4r = x^2 + y^2 + z^2$ mit $x, y, z \in \mathbb{N}$, so sind $x, y$ und $z$ alle gerade. Somit ist $r = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$ ebenfalls eine Summe dreier Quadrate in $\mathbb{N}$.

*Beweis hierfür:* Wenn nicht alle drei Zahlen $x, y, z$ gerade wären, müssten genau 2 von ihnen ungerade sein, da $x^2+y^2+z^2$ gerade ist. Für eine ungerade Zahl $x$ gilt aber $x^2 \equiv 1 \pmod 4$. Man hätte demnach
$x^2 + y^2 + z^2 \equiv 2 \pmod 4$, im Widerspruch zur Voraussetzung
$4 \mid x^2 + y^2 + z^2$. □

**Bemerkungen: 13.2** Die Umkehrung von Satz 13.1 hat *Gauß* bewiesen. Sie ist weniger einfach zu zeigen. Vgl. [*Serre*] IV, Appendice, sowie [*Scheid*] IV.9 Satz 31.

**Lemma: 13.3** *Sei $p$ eine Primzahl. In $\mathbb{Z}/p$ ist jedes Element Summe zweier Quadrate.*

**Beweis:** Für $p = 2$ ist dies trivial.
Sei jetzt $p > 2$ und $a \in \mathbb{Z}/p$. In $\mathbb{Z}/p$ gibt es einschließlich $\overline{0}$ genau $\frac{p-1}{2}+1 = \frac{p+1}{2}$ Quadrate. D.h. die Abbildung

$$\mathbb{Z}/p \longrightarrow \mathbb{Z}/p, \quad x \longmapsto x^2$$

nimmt genau $\frac{p+1}{2}$ Werte an. Da die Abbildung $y \longmapsto a - y$ bijektiv ist (das gilt in jeder Gruppe), nimmt die zusammengesetzte Abbildung

$$\mathbb{Z}/p \longrightarrow \mathbb{Z}/p, \quad x \longmapsto a - x^2$$

auch genau $\frac{p+1}{2}$ Werte an. Mindestens einer dieser Werte muss wieder ein Quadrat sein, da es in $\mathbb{Z}/p$ nur $(p-1)/2$ Nichtquadrate gibt.
D.h. es gibt $x$ und $z$ mit $z^2 = a - x^2$, also $a = x^2 + z^2$. □

**Korollar: 13.4** *Zu jeder Primzahl $p$ gibt es $x, y, m \in \mathbb{N}$ mit*

$$x^2 + y^2 + 1 = mp \textit{ und } 0 < m \leq \frac{p}{2}.$$

**Beweis:** Dies ist wieder trivial für $p = 2$.
Sei jetzt $p \neq 2$. Nach 13.3 gibt es $x', y' \in \mathbb{N}$ mit
$x'^2+y'^2+1 \equiv 0 \pmod{p}$. Dabei kann man $x', y'$ aus dem Intervall $]-p/2, \ \ p/2]$, also aus $\left[\frac{-p+1}{2}, \ \ \frac{p-1}{2}\right]$ wählen. Setze $x = |x'|, \ \ y = |y'|$, so dass $x^2 = x'^2$ und $y^2 = y'^2$ ist. Es ist also $x^2 + y^2 + 1 = mp$ mit einem $m \in \mathbb{N}$. Ferner gilt (u.a. wegen $p \geq 3$):

$$0 < x^2 + y^2 + 1 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 = \frac{p^2 - 2p + 3}{2} \leq \frac{p^2 - 6 + 3}{2} < \frac{p^2}{2}.$$

Es ist also $mp < \frac{p^2}{2}$ und somit $m < \frac{p}{2}$. □

**Lemma: 13.5** *Ist $2n$ mit $n \in \mathbb{N}$ eine Summe von 4 Quadraten in $\mathbb{Z}$, so auch $n$.*

**Beweis:** Sei $2n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Offenbar sind $0, 2$ oder $4$ der Zahlen $x_1, x_2, x_3, x_4$ gerade. Deshalb kann man – nach eventueller Umordnung – annehmen, $x_1$ und $x_2$ seien beide gerade oder beide ungerade, und dasselbe für $x_3$ und $x_4$. Dann sind aber

$$\frac{x_1 + x_2}{2}, \ \frac{x_1 - x_2}{2}, \ \frac{x_3 + x_4}{2}, \ \frac{x_3 - x_4}{2}$$

allesamt ganze Zahlen, und es gilt:

$$n = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

□

Bei der Behandlung der Summen von 2 Quadraten war es nützlich, den Körper $\mathbb{C}$ und in ihm den Ring der Gaußschen Zahlen zu betrachten. Hier benutzen wir den sogenannten Schiefkörper $\mathbb{H}$ der Quaternionen. (Ein Schiefkörper erfüllt alle Axiome eines Körpers bis auf die Kommutativität der Multiplikation.)

Manchen Lesern dürfte bekannt sein, dass sich der Körper $\mathbb{C}$ als Ring der reellen $2 \times 2$–Matrizen der Form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

einführen lässt. Diese Einführung hat den Vorteil, dass die Assoziativität der Multiplikation und die Distributivität sich aus den entsprechenden Regeln für die Multiplikation und Addition von Matrizen ergibt. Hier gehen wir entsprechend vor.

### 13.6 Definition der Quaternionen:

*In dem nichtkommutativen Ring $M_2(\mathbb{C})$ der komplexen $2 \times 2$–Matrizen bilden die Matrizen der Form*

$$\begin{pmatrix} c & -\overline{d} \\ d & \overline{c} \end{pmatrix}$$

*einen nichtkommutativen Unterring, wie man leicht nachrechnen kann. („*$\bar{\cdot}$*“ bedeutet hier die komplexe Konjugation.) Er wird (nach* HAMILTON*) mit* $\mathbb{H}$ *bezeichnet. Seine Elemente heißen Quaternionen. Die Abbildung*

$$\mathbb{R} \to \mathbb{H} \qquad a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

*ist ein injektiver Homomorfismus. Wir identifizieren* $\mathbb{R}$ *mit seinem Bild unter dieser Abbildung, d.h. die reelle Zahl* $a$ *mit der Matrix* $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$*. Da die skalaren Vielfachen der Einheitsmatrix mit allen Matrizen vertauschbar sind, liegt* $\mathbb{R}$ *im Zentrum von* $\mathbb{H}$*. (*$\mathbb{R}$ *ist sogar das genaue Zentrum von* $\mathbb{H}$*, d.h. für ein Element* $a$ *von* $\mathbb{H}$ *gilt genau dann* $ax = xa$ *für alle* $x \in \mathbb{H}$*, wenn* $a \in \mathbb{R}$ *ist. Das werden wir nicht benötigen.)*

*Als* $\mathbb{R}$*-Vektorraum hat* $\mathbb{H}$ *eine Basis aus folgenden 4 Elementen:*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

*Hiermit haben wir für einen Quaternio die beiden Schreibweisen.*

$$\begin{pmatrix} a_1 + a_2 i & -a_4 + a_3 i \\ a_4 + a_3 i & a_1 - a_2 i \end{pmatrix} = a_1 + a_2\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}. \qquad (*)$$

*Die Multiplikation in* $\mathbb{H}$ *ist durch die Ringgesetze und die folgende Multiplikationstafel vollständig beschrieben:*

| | **i** | **j** | **k** |
|---|---|---|---|
| **i** | -1 | **k** | -**j** |
| **j** | -**k** | -1 | **i** |
| **k** | **j** | -**i** | -1 |

Wir definieren eine Abbildung $\mathbb{H} \longrightarrow \mathbb{H}$, die sogenannte Konjugation, durch

$$a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k} \mapsto \overline{(a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}} := a_1 - a_2\mathbf{i} - a_3\mathbf{j} - a_4\mathbf{k}.$$

Dies entspricht bei der Matrizenschreibweise der transponierten (komplex) konjugierten Matrix. Für die Konjugation in $\mathbb{H}$ gilt deshalb:

$$\overline{x + y} = \overline{x} + \overline{y}, \quad \overline{xy} = \overline{y}\,\overline{x}.$$

Sie ist also kein Ringautomorfismus, aber ein sogenannter Antiautomorfismus.

Wir definieren ferner eine Norm $N : \mathbb{H} \longrightarrow \mathbb{R}$ wie folgt: Sei $x$ der in $(*)$ bezeichnete Quaternio. Dann sei definiert

$$N(x) := \det(x) = x\overline{x} = \overline{x}x = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Natürlich gilt

$$N(x) \geq 0 \quad \text{und} \quad N(x) = 0 \iff x = 0.$$

(In $\mathbb{R}$ ist eine Summe von Quadraten nur dann 0, wenn jeder Summand es ist.)
Für $x \in \mathbb{H} - \{0\}$ gibt es deshalb ein (beidseitiges) Inverses:

$$\left(N(x)^{-1}\overline{x}\right) \cdot x = (\overline{x}x)^{-1}\overline{x}x = 1 = x\left(\overline{x} \cdot N(x)^{-1}\right).$$

In $\mathbb{H}$ gelten alle Körperaxiome bis auf das Kommutativgesetz für die Multiplikation. $\mathbb{H}$ ist ein sogenannter Schiefkörper.
Die Elemente von $\mathbb{H}$ heißen Quaternionen.

Wir betrachten nun – analog zum Gaußschen Zahlenring in $\mathbb{C}$ – folgenden Unterring von $\mathbb{H}$:

$$\Gamma := \{(a_1, a_2, a_3, a_4) \mid a_i \in \mathbb{Z}\}.$$

Offenbar besteht $N(\Gamma)$ aus allen Summen von 4 Quadraten in $\mathbb{N}$.

**Bemerkung: 13.7** Für $x, y \in \mathbb{H}$ gilt wegen des Determinantenmultiplikationssatzes $N(xy) = N(x) \cdot N(y)$.
Wenn $m$ und $n$ in $\mathbb{N}$ Summen von je 4 Quadraten sind, so gilt dies folglich auch für $mn$.

**Bemerkung: 13.8** Geometrisch gesehen ist $\Gamma$ ein vierdimensionales „Würfelgitter" im $\mathbb{R}^4$. Der Ring $\Gamma$ ist nicht euklidisch. Das ist erst der Ring $\overline{\Gamma}$, der aus $\Gamma$ entsteht, indem man noch die Mittelpunkte der Einheitswürfel des Würfelgitters hinzunimmt: Sei $h := 1/2 + \mathbf{i}/2 + \mathbf{j}/2 + \mathbf{k}/2 \in \mathbb{H}$; dann ist $\overline{\Gamma} = \Gamma \cup (h + \Gamma)$. (Dabei sei $h + \Gamma := \{h + \gamma | \gamma \in \Gamma\}$ wie in 6.1.) Indem man mit $\overline{\Gamma}$ arbeitet, kann man den Satz von Lagrange ganz analog zum Vorgehen im §12 beweisen. Mehr dazu können Sie in den Aufgaben und Hinweisen lesen. Hier machen wir es etwas kürzer, allerdings nicht unbedingt eleganter. Das folgende Lemma zeigt für $\Gamma$ eine eingeschränkte Euklidizität.

**Lemma: 13.9** *Seien $a, b \in \Gamma$, $b \neq 0$. Ferner sei $b^{-1}a \notin h + \Gamma$. Dann gibt es $q, r \in \Gamma$ mit*

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

*Die Voraussetzung $b^{-1}a \notin h + \Gamma$ ist insbesondere dann erfüllt, wenn $b \in \mathbb{Z}$ ungerade ist.*

**Beweis:** Sei $q$ ein dem Punkt $b^{-1}a \in \mathbb{H}$ „nächstgelegener" Punkt aus $\Gamma$. (Kommentar: Der Abstand zweier Punkte $x, y \in \mathbb{H}$ sei der euklidische, also $|x-y| = N(x-y)^{1/2}$. Man sieht leicht, dass in einer beschränkten Teilmenge von $\mathbb{H}$ nur endlich viele Punkte von $\Gamma$ liegen. Deshalb gibt es Punkte aus $\Gamma$ mit minimalem Abstand zu $b^{-1}a$ – möglicherweise mehrere. Einer von ihnen sei $q$. Ist zufällig $b^{-1}a \in \Gamma$, so ist natürlich $q = b^{-1}a$.)
Sei $b^{-1}a = (x_1, x_2, x_3, x_4)$ und $q = (q_1, q_2, q_3, q_4)$. Dann ist $|x_i - q_i| \leq 1/2$ für alle $i$ und wegen $b^{-1}a \notin h + \Gamma$ sogar $|x_i - q_i| < 1/2$ für mindestens ein $i \in \{1, 2, 3, 4\}$. Für $r := a - bq$ ergibt sich

$$N(r) = N(a - bq) = N(b) \cdot N(b^{-1}a - q) < N(b) \cdot 4 \cdot (1/4) = N(b).$$

□

**Satz: 13.10** *(EULER, LAGRANGE): Jede natürliche Zahl ist Summe von 4 Quadraten natürlicher Zahlen.*

**Beweis:** Für die natürlichen Zahlen 0, 1 ist dies trivialerweise richtig. Wegen 13.6 genügt es, den Satz für Primzahlen zu zeigen, wobei er für $p = 2$ trivial ist.
Sei also $p$ eine ungerade Primzahl.
Nach 13.4 gibt es eine natürliche Zahl $m$ mit $0 < m < p/2$, derart dass $mp$ sogar eine Summe dreier Quadrate ist.
Sei nun $m_0 \in \mathbb{N}_1$ minimal mit der Eigenschaft, dass $m_0 p = N(x)$ für ein $x \in \Gamma$ gilt.

Im Falle $m_0 = 1$ sind wir fertig. Wir nehmen also an, es sei $m_0 > 1$, und führen dies zu einem Widerspruch.
Wegen 13.5 ist $m_0$ ungerade. Nach 13.9 gibt es deshalb $w, y \in \Gamma$ mit
(*) $\qquad x = m_0 w + y$ und $N(y) < N(m_0) = m_0^2$.
Wir rechnen

$$N(y) = N(x - m_0 w) = (x - m_0 w)(\overline{x} - m_0 \overline{w}) = x\overline{x} - m_0 x\overline{w} - m_0 w\overline{x} - m_0^2 w\overline{w}$$

$$= m_0 p - m_0(x\overline{w} + w\overline{x} + m_0 w\overline{w}) = m_0 m_1$$

für ein $m_1 \in \mathbb{Z}$, da der Ausdruck in der letzten Klammer sich bei Konjugation nicht ändert.
Nun ist zunächst $m_1 \neq 0$. Sonst wäre $N(y) = 0$, also $y = 0$, also $x = m_0 w$ und deshalb $m_0 p = N(x) = m_0^2 N(w)$. Es folgte $p = m_0 N(w)$ im Widerspruch dazu, dass $1 < m_0 < p$ und $p$ prim war.
Ferner gilt $0 < m_1 < m_0$, da $m_1 m_0 = N(y)$ und $0 \leq N(y) < N(m_0) = m_0^2$ ist.
Aus (*) folgt weiter

$$\overline{x}y = \overline{x}x - m_0\overline{x}w = m_0(p - \overline{x}w).$$

Somit ist $m_0^{-1}\overline{x}y = p - \overline{x}w \in \Gamma$.
Es ergibt sich:

$$N(m_0^{-1}\overline{x}y) = m_0^{-2}N(x)N(y) = m_0^{-2}m_0 p m_0 m_1 = m_1 p$$

im Widerspruch zur Minimalität von $m_0$. □

## AUFGABEN UND HINWEISE

**1)** Seien $a, b \in \mathbb{N}$ jeweils als Summe von 4 Quadraten gegeben. Geben sie konkret an, wie sich $ab$ als Summe von 4 Quadraten schreibt. Mit der sich ergebenden Formel und einigen weiteren Anpassungen kann man auch ohne Benutzung der Quaternionen den im Prinzip gleichen Beweis für den Satz von Lagrange führen. Vgl.[*Chandrasekharan*] IV. 4.)

**2)** Geben Sie ein Beispiel für natürliche Zahlen $a, b$, derart dass zwar $a$ eine Summe von 2 und $b$ eine Summe von 3, aber $ab$ keine Summe von 3 Quadraten ist. (Vgl. 12.5 b) und 13.6.)

**3)** Die Quaternionen der Norm 1 aus $\Gamma$ bilden bezüglich der Multiplikation eine nichtabelsche Gruppe, die sogenannte Quaternionengruppe $G_H$. Sie besteht aus folgenden acht Elementen:

$$\pm 1, \pm(0, 1, 0, 0, 0), \pm(0, 0, 1, 0), \pm(0, 0, 0, 1).$$

Wir verwenden die Bezeichnungen

$$i := (0,1,0,0), \quad j = (0,0,1,0), \quad k = (0,0,0,1).$$

Außer den Untergruppen $\{1\}$ und $G_H$ hat $G_H$ noch folgende vier Untergruppen:

$$\langle -1 \rangle, \quad \langle i \rangle, \quad \langle j \rangle, \quad \langle k \rangle.$$

($\langle x \rangle$ ist die von $x$ erzeugte zyklische Gruppe $\{x^n \mid n \in \mathbb{Z}\}$.)
Zwischen den Untergruppen gibt es folgende Inklusionen:

$$\begin{array}{ccc} & G_H & \\ & \cup & \\ \langle i \rangle & \langle j \rangle & \langle k \rangle \\ & \cup & \\ & \langle -1 \rangle & \\ & \cup & \\ & \{1\} & \end{array}$$

Prüfen Sie alle aufgestellten Behauptungen.
Zeigen Sie: Alle Untergruppen von $G_H$ sind Normalteiler (6.18).
Zeigen Sie, dass $G_H/\langle -1 \rangle$ abelsch ist, und geben sie ein zu $G_H/\langle -1 \rangle$ isomorfes direktes Produkt zyklischer Gruppen an.

**4)** Sei $K$ ein endlicher Körper ungerader Ordnung (=Elementezahl).
a) Wieviele Quadrate besitzt $K$?
b) Seien $a, b, c \in K$, $a \neq 0 \neq b$. Zeigen Sie: Es gibt $x, y \in K$ mit $ax^2 + by^2 = c$. (Vgl. 13.3.)

**5)** Sei $n \in \mathbb{N}$ eine Summe von 3 Quadraten rationaler Zahlen. Zeigen Sie gemäß folgender Skizze, dass $n$ dann auch eine Summe von 3 Quadraten ganzer Zahlen ist.
Betrachten Sie die Bilinearform

$$\beta : \mathbb{Q}^4 \times \mathbb{Q}^4 \longrightarrow \mathbb{Q},$$

$$\Big((x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3)\Big) \mapsto -nx_0y_0 + x_1y_1 + x_2y_2 + x_3y_3.$$

Nach Voraussetzung gibt es $x = (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$, so dass $x_0 \neq 0$ und $\beta(x, x) = 0$ ist. Sei $|x_0|$ minimal, aber $|x_0| \neq 1$. Es gibt $q_i, r_i \in \mathbb{Z}$

mit $x_i = x_0 q_i + r_i$ und $|r_i| \leq |x_0/2|$. (Es ist $q_0 = 1, r_0 = 0$.) Sei $q := (q_0, q_1, q_2, q_3)$, $r := (r_0, r_1, r_2, r_3)$ und $y := \beta(q,q)x - 2\beta(x,q)q \in \mathbb{Z}^4$. Zeigen Sie $\beta(y,y) = 0$.
(Durch die Gleichung $\beta(X,X) = 0$ wird eine Fläche 2. Grades im 3-dimensionalen projektiven Raum über $\mathbb{Q}$ definiert, und $y$ ist der von $x$ verschiedene Schnittpunkt der Geraden durch $x$ und $q$ mit dieser Fläche.)
U.a. wegen $q_0 = 1, r_0 = 0, \beta(x,x) = 0$ errechnet man

$$y_0 = \beta(q,q)x_0 - 2\beta(x,q) = \frac{\beta(x_0 q, x_0 q)}{x_0} - \frac{2\beta(x, x_0 q)}{x_0}$$

$$= \frac{\beta(x-r, x-r) - \beta(2x, x-r)}{x_0} = \frac{\beta(-x-r, x-r)}{x_0} = \frac{\beta(r,r)}{x_0} = \frac{r_1^2 + r_2^2 + r_3^2}{x_0}.$$

Aus $|r_i| \leq |x_i/2|$ folgt $|y_0| \leq 3|x_0|/4$ im Widerspruch zur Minimalität von $|x_0|$.

**6)** Wir betrachten jetzt die in 13.8 definierte Teilmenge $\overline{\Gamma}$ von $\mathbb{H}$.

Sie ist ein Unterring von $\mathbb{H}$ (und ein Oberring von $\Gamma$): Man kann etwa zeigen, dass $h^2, hi, hj, hk, ih, jh, kh$ zu $\overline{\Gamma}$ gehören, wo $i, j, k$ wie in A3 definiert sind.

Man sieht leicht, dass die Norm eines jeden Elementes von $\overline{\Gamma}$ in $\mathbb{Z}$ liegt. Mit Hilfe von Lemma 13.5 erkennt man, dass $N(\overline{\Gamma}) = N(\Gamma)$ ist.

Ferner zeigt der Beweis von Lemma 13.9, dass $\overline{\Gamma}$ euklidisch ist. Hier wird „euklidisch“ formal wie in §11 definiert – mag auch $\overline{\Gamma}$ nicht kommutativ sein. Hieraus folgt das euklidische Lemma.

Sei $p$ eine Primzahl. Nach 13.3 gibt es $x, y \in \mathbb{Z}$ mit $p | 1 + x^2 + y^2$. In $\overline{\Gamma}$ ist aber $1 + x^2 + y^2 = (1 + xi + yj)(1 - xi - yj)$. Wäre $p$ in $\overline{\Gamma}$ irreduzibel, so müsste es $1 + xi + yj$ oder $1 - xi - yj$ teilen – was nicht geht. Es folgt $p = ab$ mit Nichteinheiten $a, b \in \overline{\Gamma}$. In $\mathbb{N}$ gilt dann aber $p^2 = N(a)N(b)$, folglich $p = N(a) = N(b)$.

# § 14

# Pythagorastripel und die Fermatvermutung für den Exponenten 4

Wenn Sie das Buch bis hierher durchgearbeitet haben, werden Sie diesen Paragrafen als willkommene Entspannung genießen. Man kann ihn schon im Anschluss an den §2 ohne weiteres verstehen.

**14.1** Ein Pythagorastripel ist ein Tripel natürlicher Zahlen $(a, b, c)$ mit $a^2 + b^2 = c^2$. Ein primitives Pythagorastripel (PPT) ist ein Pythagorastripel $(a, b, c)$, wo $a, b, c$ keinen gemeinsamen Teiler $> 1$ haben. Das kleinste und bekannteste nichttriviale Pythagorastripel ist $(3, 4, 5)$.

**Bemerkungen: 14.2** a) Seien $a, b, c, d \in \mathbb{N}$, $d \neq 0$. Genau dann ist $(a, b, c)$ ein Pythagorastripel, wenn $(ad, bd, cd)$ ein solches ist. (Denn $a^2 + b^2 = c^2 \iff a^2d^2 + b^2d^2 = c^2d^2$.)
Man kennt also sämtliche Pythagorastripel, wenn man die primitiven unter ihnen kennt.

b) Wenn $(a, b, c)$ ein PPT ist, so sind je zwei der Zahlen $a, b, c$ schon teilerfremd. Denn wegen $a^2 + b^2 = c^2$ ist z.B. jeder Primfaktor von $a$ und $b$ auch ein solcher von $c^2$, also von $c$.

c) In einem Pythagorastripel $(a, b, c)$ ist eine der beiden Zahlen $a, b$ gerade. Denn, wenn $a, b$ beide ungerade sind, ist $a^2 + b^2 \equiv 1 + 1 \pmod 4$, also kein

Quadrat.
(Für Leser, welche diesen Paragrafen im Anschluss an §2 lesen:
Jede ungerade Zahl ist von der Form $2m + 1$. Und es ist
$(2m+1)^2 = 4m^2 + 4m + 1 = 4m' + 1$. Wenn $a$ und $b$ ungerade sind, ist also $a^2 + b^2$ von der Form $4m'' + 2$, d.h. durch 2, aber nicht durch 4 teilbar, kann also kein Quadrat sein.)
In einem PPT $(a, b, c)$ – wo ja $\mathrm{ggT}(a, b) = 1$ ist – ist somit eine der Zahlen $a, b$ gerade, die andere ungerade und deshalb $c$ ungerade.

**Lemma: 14.3** *a) Seien $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ und $mn = k^2$ mit einem $k \in \mathbb{N}$. Dann sind auch $m$ und $n$ Quadrate in $\mathbb{N}$.*

*b) Allgemeiner, sind $m_1, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen, deren Produkt ein Quadrat natürlicher Zahlen ist, so sind sie selber Quadrate in $\mathbb{N}$*

**Beweis:** a) Ist $k = 0$, so ist $m = 0$ oder $n = 0$. Wegen der Teilerfremdheit muss dann $n = 1$ bzw. $m = 1$ sein. Ansonsten gilt für jeden Primfaktor $p$ von $m$, dass $v_p(n) = 0$, also $v_p(m) = v_p(mn) = v_p(k^2) \in 2\mathbb{Z}$ ist. Ebenso folgt $v_q(n) \in 2\mathbb{Z}$ für jeden Primfaktor $q$ von $n$.

b) wird analog bewiesen. □

**Satz: 14.4** *a) Seien $m, n$ teilerfremde natürliche Zahlen, $m > n$, eine von ihnen gerade, die andere ungerade. Dann ist*

$$(m^2 - n^2,\ \ 2mn,\ \ m^2 + n^2)$$

*ein PPT.*

*b) Jedes PPT $(a, b, c)$ mit ungeradem $a$ ist von obiger Gestalt, und zwar auf genau eine Weise.*

**Beweis:** a) Offenbar ist

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2.$$

Die Primitivität überlegt man sich so: Wenn $p$ ein Primfaktor von $2mn$ ist, gilt $p = 2$ oder $p|m$ oder $p|n$. Da genau eine der beiden Zahlen $m^2, n^2$ gerade

ist, haben wir $2 \nmid m^2 - n^2$ und $2 \nmid m^2 + n^2$.
Im Falle $p|m$ gilt $p \nmid n$, da $m$ und $n$ teilerfremd zueinander sind. Also ergibt sich dann $p \nmid m^2 - n^2$, $p \nmid m^2 + n^2$.

b) Sei $(a, b, c)$ ein PPT und $a$ ungerade. Dann ist $b$ gerade, $b = 2b'$ und $c$ ungerade (14.2 c)).
Mit $b^2 = c^2 - a^2 = (c + a)(c - a)$ ergibt sich $b'^2 = \dfrac{c+a}{2} \cdot \dfrac{c-a}{2}$, wobei $(c + a)/2$, $(c - a)/2 \in \mathbb{N}$ gilt, da $a$ und $c$ ungerade sind und $c \geq a$ ist.
Nun ist $\mathrm{ggT}((c + a)/2,\ (c - a)/2) = 1$. Denn jeder gemeinsame Teiler von $(c + a)/2$ und $(c - a)/2$ wäre auch ein solcher von $a = \dfrac{c+a}{2} - \dfrac{c-a}{2}$ und $c = \dfrac{c+a}{2} + \dfrac{c-a}{2}$. Aus $\dfrac{c+a}{2} \cdot \dfrac{c-a}{2} = b'^2$ ergibt sich deshalb, dass $(c+a)/2$ und $(c - a)/2$ Quadrate sind (14.3).
Mit $(c + a)/2 = m^2$, $(c - a)/2 = n^2$ und $m, n \in \mathbb{N}$ erhält man $a = m^2 - n^2$, $c = m^2 + n^2$ und $b = 2b' = 2\sqrt{m^2n^2} = 2mn$. Da $c = m^2 + n^2$ ungerade ist, ist genau eine der Zahlen $m, n$ gerade. Ferner sind $m$ und $n$ teilerfremd, da $m^2 = (c + a)/2$ und $n^2 = (c - a)/2$ es sind.
Durch $m^2 - n^2 = a$ und $m^2 + n^2 = c$ sind $m^2$ und $n^2$ eindeutig bestimmt, somit auch $m$ und $n$, da $m, n \in \mathbb{N}$ vorausgesetzt war. Es ergibt sich die behauptete Eindeutigkeit der Darstellung. $\square$

**Beispiele: 14.5** Es gibt unendlich viele PPT's. Z.B. hat man folgende beiden Serien:

a) $n = 1,\ m = 2k,\ k \in \mathbb{N}_1$, d.h. $a = 4k^2 - 1, b = 4k, c = 4k^2 + 1:$
$(3, 4, 5), (15, 8, 17), (35, 12, 37), \ldots$

b) $n \in \mathbb{N},\ m = n + 1$, d.h. $a = 2n + 1, b = 2n^2 + 2n, c = 2n^2 + 2n + 1$
$(1, 0, 1), (3, 4, 5), (5, 12, 13), (7, 24, 25), \ldots.$

**Korollar: 14.6** *Auf dem Einheitskreis $\{(x, y) \in \mathbb{R}^2 \quad | \quad x^2 + y^2 = 1\}$ liegen unendlich viele Punkte mit rationalen Koordinaten, sogenannte rationale Punkte.*

**Beweis:** Ist $(a, b, c)$ ein Pythagorastripel, so liegt der Punkt $\left(\dfrac{a}{c}, \dfrac{b}{c}\right)$ auf dem Einheitskreis. Sind $(a, b, c)$ und $(a', b', c')$ verschiedene PPT's, so ist $\dfrac{a}{c} \neq \dfrac{a'}{c'}$, also auch $\left(\frac{a}{c}, \frac{b}{c}\right) \neq \left(\frac{a'}{c'}, \frac{b'}{c'}\right)$. Denn wegen der Primitivität ist $\mathrm{ggT}(a,c) = 1 = \mathrm{ggT}(a',c')$. Gekürzte Brüche $\frac{a}{c}$ und $\frac{a'}{c'}$ natürlicher Zahlen können aber nur dann gleich sein, wenn Zähler und Nenner gleich sind. Aus $\frac{a}{c} = \frac{a'}{c'}$ folgt also $a = a'$, $c = c'$ und somit $b = b'$. □

**Bemerkung: 14.7** Man kann auch sagen: Ein PPT ist von der Form

$$(|m^2 - n^2|, \;\; 2mn, \;\; m^2 + n^2)$$

mit teilerfremden $m, n$, wo $m$ ungerade und $n$ gerade ist.

**14.8 Satz** (*Fermat, Euler*): *Für $a, b, c \in \mathbb{N}$ gelte*

$$a^4 + b^2 = c^4.$$

*Dann ist $a = 0$ oder $b = 0$.*

**Beweis:** Wir nehmen an, der Satz sei falsch. Dann gibt es ein Gegenbeispiel $(a, b, c) \in \mathbb{N}_1^3$ mit minimalem $c$. Hätten zwei der drei Zahlen $a, b, c$ einen gemeinsamen Primfaktor $p$, so offenbar auch die dritte. Ferner wäre dann $p^2$ ein Teiler von $b$. Das Tripel $\left(\frac{a}{p}, \;\frac{b}{p^2}, \;\frac{c}{p}\right)$ wäre dann auch ein Gegenbeispiel im Widerspruch zur Minimalität von $c$. Also sind $a, b, c$ paarweise teilerfremd und deshalb

$$(a^2, b, c^2) \quad \text{ein PPT.}$$

Wir unterscheiden 2 Fälle:

1. Fall: $a$ sei ungerade.
Dann gibt es $m, n \in \mathbb{N}$ mit

$$a^2 = m^2 - n^2, \quad b = 2mn, \quad c^2 = m^2 + n^2.$$

Da $b \neq 0$ ist, sind auch $m, n \neq 0$.
Wir erhalten

$$(ac)^2 = (m^2 - n^2)(m^2 + n^2) = m^4 - n^4,$$

also

$$n^4 + (ac)^2 = m^4$$

mit

$$m, n, ac \neq 0 \quad \text{und} \quad m < c,$$

da $m^2 + n^2 = c^2$ ist.
Dies steht im Widerspruch zur Minimalität von $c$.

2. FALL: $a$ sei gerade.
Dann gibt es teilerfremde $m, n \in \mathbb{N}$, $m$ ungerade, mit

(1) $a^2 = 2mn$, (2) $b = |m^2 - n^2|$, (3) $c^2 = m^2 + n^2$.

Aus (1) und $a \neq 0$ folgt $m \neq 0 \neq n$. Mit (3) ergibt sich also:

$$(m, n, c) \quad \text{ist ein PPT.}$$

Da zudem $m$ ungerade ist, gibt es teilerfremde $r, s \in \mathbb{N}$ mit

(4) $m = r^2 - s^2$, (5) $n = 2rs$, (6) $c = r^2 + s^2$.

Wegen (5) und $n \in \mathbb{N}_1$ ist $r \neq 0 \neq s$. Aus (1) und (5) erhalten wir

(7) $a^2 = 2mn = 4mrs$.

Da jeweils $r$ zu $s$ und $m$ zu $n = 2rs$ teilerfremd ist, sind $r, s$ und $m$ paarweise teilerfremd. Da ferner 4 ein Quadrat ist, folgt aus (7), dass $r$, $s$ und $m$ Quadrate sind (vgl. 14.3):

(8) $r = \rho^2$, (9) $s = \sigma^2$, (10) $m = \mu^2$.

Mit (8), (9) und (10) schreibt sich (4) folgendermaßen:

(11) $\sigma^4 + \mu^2 = \rho^4$.

Wegen $s \neq 0 \neq m$ ist $\sigma \neq 0 \neq \mu$. Ferner ist $\rho \leq \rho^4 = r^2 < r^2 + s^2 = c$. Mit (11) ist also $(\sigma, \mu, \rho)$ ein Gegenbeispiel mit $\rho < c$. Dies widerspricht der Minimalität von $c$. $\square$

**Korollar: 14.9** *a) Wenn für $a, b, c \in \mathbb{N}$ die Gleichung $a^4 + b^4 = c^4$ gilt, ist $a = 0$ oder $b = 0$.*
*b) $a^{4k} + b^{2m} = c^{4n}$ mit $a, b, c, k, m, n \in \mathbb{N}_1$ ist unmöglich.*
*c) Auf der Kurve $\{(x, y) \in \mathbb{R}^2 \mid x^{4m} + y^{4m} = 1\}$ liegen nur endlich viele rationale Punkte, nämlich $(\pm 1, 0), (0, \pm 1)$.*

AUFGABEN UND HINWEISE

**1)** Anstelle von 14.8 wird in der Regel der entsprechende Satz für die Gleichung

$$a^4 + b^4 = c^2$$

gezeigt. (Verzeihen Sie dem Autor, dass er es mal anders machen wollte. In [*Euler*] §§202 ff. finden sich beide Sätze.)
Sie können den üblichen Satz analog zum Fall 2 im Beweis von 14.8 beweisen.

**2)** Seien $a, b, \in \mathbb{Z}$, so dass $a^2 + b^2$ und $a^2 - b^2$ Quadrate in $\mathbb{Z}$ sind. Zeigen Sie: $b = 0$.

**3)** Ist folgende Figur in der (euklidischen) Ebene

derart möglich, dass $a \neq 0$ ist und $a, b, c, d$ kommensurabel , d.h. alle Streckenverhältnisse $a : b$, $b : c$, $c : d$ rational sind? ( bedeutet: rechter Winkel).

**4)** Machen Sie sich klar, dass jede der beiden Gleichungen

$$x^2 + y^2 = z^4 \quad \text{und} \quad x^4 + y^2 = z^2$$

sehr viele nichttriviale „primitive" Lösungen hat. (12. A6 und 1. A7 b).)

**5)** Für Tischtennisspieler, Intellektuelle, Nachtschwärmer, Individualisten und andere sympathische Menschen wie Schachspieler und Mathematiker wird ein Park entworfen. Zur Erinnerung an Pythagoras soll in einem Teil des Parkes ein Beet in der Form eines rechtwinkligen Dreiecks entstehen. Die drei angrenzenden „Pythagorasquadrate" sollen nun durch gleichgroße dunkle und weiße quadratische Steinplatten schachbrettartig so gepflastert werden, dass auf einem der Quadrate genau 64 Steinplatten liegen, dieses also als Freilichtschachbrett benutzt werden kann. Überlegen Sie sich, dass es im wesentlichen genau zwei Möglichkeiten gibt, den Plan zu realisieren.

# § 15

# Der Ring der dritten Einheitswurzeln und die Fermatvermutung für den Exponenten 3

Abb. 15

Ist so etwas möglich? Gibt es natürliche Zahlen $x, y, z \neq 0$ mit $x^3 + y^3 = z^3$?
Die Antwort ist: **Nein.**

Mit anderen Worten $(-z^3 = (-z)^3)$: Es gibt keine $x, y, z \in \mathbb{Z} - \{0\}$ mit

$$x^3 + y^3 + z^3 = 0.$$

Dies wird in 15.7 gezeigt werden.

Wir betrachten zum Beweis einen weiteren Ring:

$$R := \{a + b\zeta \quad | \quad a, b \in \mathbb{Z}\},$$

wobei $\zeta := \frac{1}{2}(-1+\sqrt{-3})$ $=\exp(2\pi i/3) \in \mathbb{C}$ ist. (Es sei $\sqrt{-3} := i\sqrt{3}$.)

**Bemerkungen: 15.1** a) Für $\zeta$ errechnet man:

$$\begin{aligned} &\zeta^2 = \tfrac{1}{2}\left(-1-\sqrt{-3}\right) = -(1+\zeta), \\ &\zeta^3 = 1, \quad \text{also} \quad \zeta^2 = \zeta^{-1}. \end{aligned}$$

Somit ist $\zeta$ eine sogenannte dritte Einheitswurzel, und zwar eine primitive dritte Einheitswurzel. Denn die 3 Nullstellen des Polynoms $x^3 - 1$ sind $\zeta^0, \zeta^1, \zeta^2$, also Potenzen von $\zeta$.

b) $R$ ist in der Tat ein Ring, genauer ein Unterring von $\mathbb{C}$.
Denn zunächst ist $R$ offenbar bezüglich der Addition eine Untergruppe der additiven Gruppe von $\mathbb{C}$. Da aber $\zeta^2 = -1-\zeta$ zu $R$ gehört, sieht man sofort, dass $R$ in $\mathbb{C}$ multiplikativ abgeschlossen, also (da auch
$1 \in R$) ein Unterring von $\mathbb{C}$ ist.

c) Da 1 und $\zeta$ über $\mathbb{R}$ linear unabhängig sind, besitzt jedes Element von $R$ eine eindeutige Darstellung als $a + b\zeta$ mit $a, b \in \mathbb{Z}$.

**15.2** Die Elemente von $R$, aufgefasst als Punkte der Gaußschen Zahlenebene, ergeben folgendes Bild:

Abb. 16

(Die eingekreisten Punkte sind Elemente des Unterringes $S$, der in 15.4 h) eingeführt wird. Mit * sind die Einheiten gekennzeichnet.)

**15.3** Man kann $R$ auch anders beschreiben: Sei nämlich

$$R' := \left\{ \frac{c}{2} + \frac{d}{2}\sqrt{-3} \;\middle|\; c, d \in \mathbb{Z},\;\; c \equiv d\,(2) \right\}.$$

Die Kongruenz $c \equiv d\,(2)$ bedeutet, dass $c$ und $d$ beide gerade oder beide ungerade sind. Es gilt die

**Feststellung:** $R = R'$.

**Beweis:** Es ist $a+b\zeta = a+b\cdot\frac{1}{2}(-1+\sqrt{-3}) = a-\frac{b}{2}+\frac{b}{2}\sqrt{-3} = \frac{2a-b}{2}+\frac{b}{2}\sqrt{-3}$.
Da aber $2a-b \equiv b \pmod 2$ gilt, erhalten wir $R \subset R'$.
Umgekehrt ist $\frac{c}{2}+\frac{d}{2}\sqrt{-3} = \frac{c+d}{2} + d\cdot\frac{1}{2}(-1+\sqrt{-3}) \in R$, da $\frac{c+d}{2} \in \mathbb{Z}$ wegen $c \equiv d(2)$ gilt. Also ist $R' \subset R$. $\square$

**Bemerkungen: 15.4** a) Die Einschränkung der Konjugation von $\mathbb{C}$ auf $R$ sieht folgendermaßen aus:

$$\overline{\frac{c}{2}+\frac{d}{2}\sqrt{-3}} = \frac{c}{2}-\frac{d}{2}\sqrt{-3}$$

bzw.

$$\overline{a+b\zeta} = a-b(1+\zeta) = a+b\zeta^2 = a+b\overline{\zeta} = a+b\zeta^{-1};$$

denn $\overline{\zeta} = \zeta^2 = \zeta^{-1} = -(1+\zeta)$.

b) Die Konjugation ist natürlich ein Automorfismus von $R$.

c) Für $\alpha = \frac{c}{2}+\frac{d}{2}\sqrt{-3} \in R$ ist

$$N(\alpha) := \alpha\overline{\alpha} = |\alpha|^2 = \tfrac{1}{4}(c^2+3d^2) \in \mathbb{N},$$

da aus $c \equiv d(2)$ folgt, dass $4 \mid c^2+3d^2$ gilt. Letzterer Schluss lässt sich vermeiden, wenn man für $\alpha = a+b\zeta$ errechnet:

$$N(\alpha) = (a+b\zeta)(a+b\overline{\zeta}) = a^2+ab(\zeta-(1+\zeta))+b^2\zeta\zeta^{-1} = a^2-ab+b^2.$$

Denn, offenbar ist $a^2-ab+b^2 \in \mathbb{Z}$ und $\frac{1}{4}(c^2+3d^2) \geq 0$, woraus sich $N(\alpha) \in \mathbb{N}$ ergibt.
Natürlich gilt die Äquivalenz:

$$N(\alpha) = 0 \iff \alpha = 0.$$

Ferner haben wir $N(\alpha\beta) = N(\alpha)N(\beta)$.

d) Wie in 12.3 g) zeigt man die Äquivalenz:

$$\alpha \in R^* \iff N(\alpha) = 1.$$

e) Offenbar sind folgende Elemente Einheiten:

$$1, \ \ \zeta, \ \ \zeta^2, \ \ -1, \ \ -\zeta, \ \ -\zeta^2.$$

Dies sind die sechs 6–ten Einheitswurzeln. Denn, wenn man $\omega = -\zeta^2$ setzt, gilt:

$$\omega^0 = 1, \quad \omega^1 = -\zeta^2, \quad \omega^2 = \zeta, \quad \omega^3 = -1, \quad \omega^4 = \zeta^2, \quad \omega^5 = -\zeta, \quad \omega^6 = 1.$$

f) Umgekehrt, wenn $\alpha = \frac{1}{2}(c + d\sqrt{-3}) \in R^*$ ist, muss

$$N(\alpha) = 1, \quad \text{d.h.} \quad \tfrac{1}{4}(c^2 + 3d^2) = 1$$

sein.
Dies ist jedoch offenbar nur in den 6 Fällen

$$\begin{array}{ll} c = \pm 2, \quad d = 0, & \quad \text{bzw.} \\ c = \pm 1, \quad d = \pm 1 & \end{array}$$

möglich. D.h. die oben angegebenen 6–ten Einheitswurzeln sind bereits sämtliche Einheiten von $R$.

Übrigens kann man auch in Abb. 16 erkennen, dass die 6–ten Einheitswurzeln die einzigen Zahlen aus $R$ sind, deren Betrag 1 ist. (Beachte $|\alpha|^2 = N(\alpha)$.)

g) Die imaginären (d.h. nicht reellen) Einheiten von $R$ sind die vier Zahlen $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$.

h) Die Menge

$$S := \{a + 2b\zeta \ \ | \ \ a, b \in \mathbb{Z}\} = \left\{c + d\sqrt{-3} \ \ | \ \ c, d \in \mathbb{Z}\right\}$$

ist ein echter Unterring von $R$, wie man sich leicht überzeugt.
In Abb. 16 gehört zu $S$ nur jede zweite Zeile von Punkten.

In $S$ gilt der Satz von der eindeutigen Primfaktorzerlegung nicht. Denn in diesem Ring ist zwar $2 \nmid 2\zeta$, aber $2^3 = (2\zeta)^3$. (Vgl. 11. A5.)

**Satz: 15.5** *$R$ ist ein euklidischer Ring. Genauer gilt:*
*Sind $\alpha, \beta \in R, \beta \neq 0$, so gibt es $q, \rho \in R$ mit*

$$\alpha = \beta q + \rho \quad \textit{und} \quad N(\rho) \leq \tfrac{3}{4} N(\beta).$$

*Insbesondere gilt in $R$ der Satz von der eindeutigen Primfaktorzerlegung.*

**Beweis** (vgl. 12.6): Beachte, dass $\mathbb{C} = \{x + y\zeta \mid x, y \in \mathbb{R}\}$ ist, da 1 und $\zeta$ über $\mathbb{R}$ linear unabhängig sind und somit eine Basis des $\mathbb{R}$–Vektorraumes $\mathbb{C}$ bilden.
Wir dividieren $\alpha$ durch $\beta$ in $\mathbb{C}$ (ohne Rest). $\dfrac{\alpha}{\beta} = x + y\zeta =: z$ mit $x, y \in \mathbb{R}$.
Wähle $m, n \in \mathbb{Z}$ mit

$$|x - m| \leq \frac{1}{2}, \quad |y - n| \leq \frac{1}{2}$$

und setze $q := m + n\zeta$ und $\rho := \alpha - q\beta$.
Dann gilt: mit 15.4 c):

$$\begin{aligned} N(\rho) &= N(\alpha - q\beta) = \\ N(z - q)N(\beta) &= ((x-m)^2 + (y-n)^2 - (x-m)(y-n))N(\beta) \\ &\leq ((x-m)^2 + (y-n)^2 + |x-m| \cdot |y-n|)\, N(\beta) \\ &\leq \frac{3}{4}\, N(\beta). \end{aligned}$$

□

**Bemerkungen: 15.6** a) Das Konjugierte von $1 - \zeta$ ist
$1 - \overline{\zeta} = 1 - \zeta^2 = -\zeta^2(1 - \zeta)$, also insbesondere zu $1 - \zeta$ assoziiert. Für seine Norm gilt:
$3 = 1^2 - 1 \cdot (-1) + (-1)^2 = N(1 - \zeta) = -\zeta^2(1 - \zeta)^2$; also ist 3 assoziiert zu $(1 - \zeta)^2$. Ferner folgt aus $N(1 - \zeta) = 3$, dass $1 - \zeta$ irreduzibel, also prim ist (vgl. 12.9).

b) Der Restklassenring $R/3R$ besteht aus 9 Elementen.
Denn die Abbildung

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow R, \quad (a, b) \longmapsto a + b\zeta$$

ist offenbar ein Isomorfismus für die additiven Gruppen. (Sie ist kein Ringisomorfismus!) Man hat deshalb die folgenden Isomorfismen für die additiven Gruppen

$$R/3R \cong (\mathbb{Z} \times \mathbb{Z})/3 \cdot (\mathbb{Z} \times \mathbb{Z}) \cong (\mathbb{Z}/3) \times (\mathbb{Z}/3).$$

Hieraus folgt die Behauptung.

c) Jedes Element von $R$ ist modulo $3R$ zu genau einem der folgenden 9 Elemente kongruent:

$$\pm 1, \pm\zeta, \pm\zeta^2 \ \text{ (die Einheiten von } R), \ \ 1-\zeta, \ 1-\overline{\zeta}(= -\zeta^2(1-\zeta)), \ 0.$$

(Man drückt das auch so aus: Obige Elemente bilden ein vollständiges Repräsentantensystem modulo $3R$.)
Da die Anzahl der obigen Elemente mit der Zahl der Restklassen modulo $3R$ übereinstimmt, genügt es zu zeigen, dass je zwei verschiedene dieser Elemente $\alpha$ und $\beta$ in verschiedenen Restklassen liegen, d.h. modulo $3R$ nicht kongruent sind. Aus $\alpha \equiv \beta \pmod{3R}$ würde aber $N(3)|N(\alpha-\beta)$, d.h. $9 \mid |\alpha-\beta|^2$ in $\mathbb{Z}$ folgen. Nun sieht man leicht (etwa geometrisch in Abb. 16), dass $|\alpha-\beta| < 3$ für alle $\alpha, \beta$ unter obigen Elementen ist.

d) Jeder Kubus (i.e. dritte Potenz) in $R$ ist modulo $3R$ kongruent zu einer der drei Zahlen $-1, 0, 1$, wie man mit c) sofort nachrechnet.
Umgekehrt folgt hieraus: Sind $x \in R$, $u \in R^*$ und gilt

$$ux^3 \equiv \pm 1 \pmod{3R},$$

dann ist $u = \pm 1$, also $ux^3$ ein Kubus in $R$.

**15.7 Satz** *(Fermat, Euler, Gauß): Es gibt keine* $a, b, c \in R - \{0\}$ *mit*

$$(1) \qquad a^3 + b^3 + c^3 = 0.$$

**Beweis:** *(Gauß)* Wir nehmen an, (1) gelte für gewisse $a, b, c \in R$ mit $abc \neq 0$, und führen dies zu einem Widerspruch.
Ohne Einschränkung der Allgemeinheit können wir annehmen, dass $a$, $b$ und $c$ in $R$ keinen gemeinsamen Primfaktor besitzen; denn man könnte durch einen solchen teilen. (Vgl. Beweis von 14.8.)

Dann sind aber die Zahlen $a$, $b$, $c$ sogar paarweise teilerfremd, da jeder Teiler von zweien wegen (1) auch die dritte teilt. M.a.W.: Wir dürfen und werden annehmen, dass $(a, b, c)$ ein primitives Tripel sei.
*Behauptung 1*: Eine der drei Zahlen $a$, $b$, $c$ wird durch $1 - \zeta$ geteilt.
*Beweis hierfür:* Wir setzen

$$\alpha := b + c, \quad \beta := c + a, \quad \gamma := a + b.$$

Dann sind auch $\alpha, \beta, \gamma$ paarweise teilerfremd. Denn jeder Primfaktor von z.B. $\gamma = a + b$ teilt auch $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$, also $c^3$ (wegen (1)) und somit $c$. Gemeinsame Primfaktoren von $\beta$ und $\gamma$ teilen deshalb auch $b$ und $c$.

Aus $2a = \beta + \gamma - \alpha$ usw. und (1) folgt

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = 0. \tag{2}$$

Andererseits hat man die Identität

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = (\alpha + \beta + \gamma)^3 - 24\alpha\beta\gamma. \tag{3}$$

Aus (2) und (3) ergibt sich

$$(\alpha + \beta + \gamma)^3 = 24\alpha\beta\gamma,$$

also

$$(1 - \zeta)^2 \mid (\alpha + \beta + \gamma)^3, \text{ da } 3 = -\zeta^2(1 - \zeta)^2 \text{ ist.}$$

Weil $1 - \zeta$ prim ist, erhalten wir hieraus:

$$(1 - \zeta)^3 \mid (\alpha + \beta + \gamma)^3$$

und deshalb

$$(1 - \zeta)^3 \ \mid \ 2^3 \cdot 3\alpha\beta\gamma. \tag{4}$$

Wegen $-\zeta^2(1 - \zeta)^2 - 2 = 3 - 2 = 1$ ist $1 - \zeta$ zu 2 in $R$ teilerfremd. Deshalb ergibt sich aus (4):

$$1 - \zeta \mid \alpha\beta\gamma.$$

Da $1-\zeta$ prim ist, teilt es eine der Zahlen $\alpha, \beta, \gamma$, etwa $\gamma$. Dann ist auch $1-\zeta | c$, wie oben gesehen. –

Für ein primitives Tripel $(a, b, c) \in (R - \{0\})^3$, welches (1) erfüllt, können wir also $1-\zeta \mid c$ annehmen. Unter allen solchen sei eines mit minimalem $v_{1-\zeta}(c)$ gewählt. (Dabei bezeichnet $v_{1-\zeta}(c)$ analog zu 2.11 den größten Exponenten $r$ mit $(1-\zeta)^r \mid c$.)

Der gewünschte Widerspruch ergibt sich nun aus der folgenden

*Behauptung 2*: Es gibt ein primitives Tripel $(a_*, b_*, c_*)$ mit $a_*^3 + b_*^3 + c_*^3 = 0$, $1-\zeta \nmid a_* b_*$ und $v_{1-\zeta}(c_*) < v_{1-\zeta}(c)$.

*Beweis hierfür:* Da $a$ und $b$ wegen der vorausgesetzten Primitivität nicht durch $1-\zeta$ teilbar sind, sind sie nach 15.6 c) modulo $3R$ je zu einer der Zahlen $\pm 1, \pm\zeta, \pm\zeta^2$ kongruent. Da $a^3 = (a\zeta^2)^3 = (a\zeta)^3$ ist, wir also $a$ und $b$ in (1) entsprechend ersetzen können, dürfen wir auch annehmen, dass $a, b$ je zu einer der Zahlen $1, -1$ kongruent sind.
Nun ist weder $a \equiv 1 \equiv b \pmod{3R}$, noch $a \equiv -1 \equiv b \pmod{3R}$ möglich. Denn dann wäre

$$a^3 + b^3 + c^3 \equiv \pm 2 \pmod{3R}.$$

(Aus $1-\zeta \mid c$ folgt $3 = -\zeta^2(1-\zeta)^2 \mid c^3$). Demzufolge dürfen wir

$$a \equiv 1 \pmod{3R} \quad \text{und} \quad b \equiv -1 \pmod{3R}$$

annehmen, also

(5) $$a = 1 + 3\alpha \text{ und } b = -1 + 3\beta$$

mit gewissen $\alpha, \beta \in R$ (die nicht mit den $\alpha, \beta$ aus dem Beweis der 1. Behauptung zu verwechseln sind).

Wir setzen jetzt

$$(6)\qquad \begin{cases} A' := \dfrac{a+b\zeta}{1-\zeta} = \dfrac{1+3\alpha-\zeta+3\beta\zeta}{1-\zeta} = 1-\zeta^2(1-\zeta)(\alpha+\beta\zeta), \\[2ex] B' := \dfrac{a\zeta+b}{1-\zeta} = \dfrac{\zeta+3\alpha\zeta-1+3\beta}{1-\zeta} = -1-\zeta^2(1-\zeta)(\alpha\zeta+\beta), \\[2ex] C' := \dfrac{\zeta^2(a+b)}{1-\zeta} = \dfrac{3\zeta^2(\alpha+\beta)}{1-\zeta} = -\zeta(1-\zeta)(\alpha+\beta). \end{cases}$$

Es sind also $A', B', C' \in R$. Ferner folgt aus $1+\zeta+\zeta^2=0$ sofort

$$(7)\qquad A'+B'+C'=0.$$

Und es gilt

$$(8)\qquad \begin{aligned} A'B'C' &= (1-\zeta)^{-3}(a+b\zeta)(a+b\zeta^2)(a+b) \\ &= (1-\zeta)^{-3}(a^3+b^3) \\ &= \left(\frac{-c}{1-\zeta}\right)^3. \end{aligned}$$

Da man

$$-\zeta A' + \zeta^2 B' = a \quad \text{und} \quad \zeta^2 A' - \zeta B' = b$$

errechnet, sieht man, dass mit $a$ und $b$ auch $A'$ und $B'$ zueinander teilerfremd sind. Zusammen mit (7) ergibt sich, dass $A', B', C'$ paarweise teilerfremd sind.

Hieraus folgt mit (8), dass $A', B', C'$ bis auf Einheiten Kuben sind. Denn für jedes Primelement $p$ von $R$ gilt $3 \mid v_p(A'B'C')$, da $A'B'C'$ nach (8) ein Kubus ist. Da aber jedes Primelement wegen der Teilerfremdheit nur eine der drei Zahlen $A', B', C'$ teilen kann, gilt

$$(9)\qquad 3 \mid v_p(A'), \quad 3 \mid v_p(B') \text{ und } 3 \mid v_p(C')$$

für jedes Primelement $p$. D.h. jede der Zahlen $A', B', C'$ ist von der Form $ux^3$ mit $u \in R^*$, $x \in R$. (Vgl. 14.3.)

Nach (6) ist $C'$ durch $1-\zeta$ teilbar und damit wegen (9) sogar durch $(1-\zeta)^3$, also auch durch $3 = -\zeta^2(1-\zeta)^2$.

Aus (7) ergibt sich deshalb

$$A' + B' \equiv 0 \pmod{3R}.$$

Da $A' \equiv 1$ (mod $(1-\zeta)R$) und $B' \equiv -1$ (mod $(1-\zeta)R$) ist, bleibt nach 15.6. c) nur die Möglichkeit

$$A' \equiv u \pmod{3R}, \quad B' \equiv -u \pmod{3R}$$

mit einem geeigneten $u \in R^*$. Wir setzen jetzt

$$A := u^{-1}A', \quad B := u^{-1}B', \quad C := u^{-1}C'.$$

Dann gilt

$$A + B + C = u^{-1}(A' + B' + C') = 0; \tag{10}$$

$$ABC = u^{-3}A'B'C' = \left(\frac{\pm c}{1-\zeta}\right)^3; \tag{11}$$

ferner

$$A \equiv 1 \ (\mathrm{mod}\ 3R), \quad B \equiv -1 \ (\mathrm{mod}\ 3R). \tag{12}$$

Nach 15.6 d) sind $A$ und $B$ also Kuben, da sie bis auf Einheiten Kuben sind.
Mit (11) ist auch $C$ ein Kubus.
Es gibt also $a_*, b_*, c_* \in R$ mit

$$a_*^3 = A, \quad b_*^3 = B, \quad c_*^3 = C.$$

Für diese gilt nach (10)

$$a_*^3 + b_*^3 + c_*^3 = 0.$$

Da nach (11)

$$a_*^3 b_*^3 c_*^3 = \left(\frac{\pm c}{1-\zeta}\right)^3$$

gilt und $a_*^3, b_*^3$ nach (12) zu $1-\zeta$ teilerfremd sind, ist

$$v_{1-\zeta}(c_*) = v_{1-\zeta}(c) - 1$$

und damit die Behauptung 2 gezeigt. $\square$

AUFGABEN UND HINWEISE

**1)** Ein Würfel sei aus zueinander kongruenten Quadern lückenlos zusammengesetzt. Ist es möglich, aus denselben Quadern zwei kleinere Würfel lückenlos zusammenzusetzen, ohne dass auch nur ein Quader übrigbleibt? (Hinweis: 2.A 18 b) und 15.7. Kongruenz ist hier natürlich in geometrischem Sinne gemeint.)

**2)** Jede rationale Zahl ist Summe von 3 Kuben rationaler Zahlen:

$$a = \left(\frac{a^3 - 3^6}{3^2a^2 + 3^4a + 3^6}\right)^3 + \left(\frac{-a^3 + 3^5a + 3^6}{3^2a^2 + 3^4a + 3^6}\right)^3 + \left(\frac{3^3a^2 + 3^5a}{3^2a^2 + 3^4a + 3^6}\right)^3.$$

**3)** Sei $S$ der in 15.4 h) definierte Unterring von $R$. Zeigen Sie:
Zu jedem $\alpha \in R$ gibt es ein $\eta \in \{1, \zeta, \zeta^2\}$ mit $\alpha\eta \in S$.
(Wenn $a, b \in \mathbb{Z}$ und $a + b\zeta \notin S$ ist, ist $b$ ungerade. Unterscheiden Sie, ob $a$ gerade oder ungerade ist.)

**4)** Zeigen Sie:
a) Für $x \in \mathbb{N}$ sind folgende Aussagen äquivalent:

(i) Es gibt $a, b \in \mathbb{Z}$ mit $x = a^2 - ab + b^2$;

(ii) es gibt $n, m \in \mathbb{N}$ mit $x = n^2 + 3m^2$;

(iii) es gibt $c, d \in \mathbb{Z}$ mit $c \equiv d \pmod 2$ und $x = \frac{1}{4}(c^2 + 3d^2)$.

(Hinweis: 15.4 c) und A3.)
b) Falls $x$ und $y$ die Aussagen (i) – (iii) von a) erfüllen, so auch $xy$.

**5)** Zeigen Sie: Für Primzahlen $p > 3$ gilt:

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3.$$

**6)** Zeigen Sie – analog zum Vorgehen in §12:
Eine Primzahl $p$ ist genau dann von der Form $p = n^2 + 3m^2$ mit $n, m \in \mathbb{N}$,

wenn $p = 3$ oder $p \equiv 1 \pmod 3$ ist.

**7)** Historische Anmerkung (zur Fermatschen Vermutung):
*Fermat* hat vielleicht zeitweilig geglaubt, folgendes beweisen zu können:

$$(*)\ \text{Sind } a, b, c, n \in \mathbb{N},\quad n \geq 3 \text{ und gilt } a^n + b^n = c^n, \text{ so ist } a = 0 \text{ oder } b = 0.$$

Eine entsprechende *private* Notiz ist durch seinen Sohn überliefert. Da er diesen allgemeinen Satz, im Gegensatz zu den Spezialfällen $n = 3$ oder 4, nie gegenüber anderen (schriftlich) behauptet hat, ist anzunehmen, dass er keinen vollständigen Beweis von $(*)$ besaß. Siehe [*Scharlau–Opolka*] p. 15.
Bis heute ist $(*)$ nicht bewiesen. Es ist die berühmte „Fermatsche Vermutung".
Es ist klar, dass es genügt, diese Vermutung zu beweisen, wenn $n = 4$ oder eine Primzahl ist. (Eine 6–te Potenz z.B. ist auch eine dritte Potenz.) Von Fermat ist der Beweis im Falle $n = 3$ nicht überliefert, wohl aber seine Idee der „descente infinie", die wir in den Beweisen von 14.8 und 15.7 verwendet haben. In [*Euler*] finden sich Beweise für die Exponenten 4 und 3. Letzterer ist dort unvollständig. Man hat den Eindruck, *Euler* halte für den Ring $S$ (!) den Satz von der eindeutigen Primfaktorzerlegung für richtig und selbstverständlich. In [*Bergmann*] wird gezeigt wie man den Beweis aus *Eulers* Werken vervollständigen kann. Somit ist anzunehmen, dass *Euler* wahrscheinlich im Besitze eines vollständigen Beweises war und der angegebene Mangel einer unzureichenden Redaktion des Buches durch den fast erblindeten *Euler* und seinen mathematisch unbedarften Gehilfen zuzuschreiben ist. Wahrscheinlich war *Fermats* Beweis dem *Eulers* sehr ähnlich.
Unseren Beweis, der „Fermat–3" nicht nur für $\mathbb{Z}$, sondern für $R$ zeigt, entnahm ich *Gauß'* Nachlass, [*Gauß*] Bd. II, S. 387 ff. Dort findet sich auch eine Beweisandeutung für den Fall $n = 5$.
Den größten Fortschritt im 19. Jahrhundert erzielte *Kummer*, der die Fermatsche Vermutung für eine große – möglicherweise unendlich große – Klasse von Primzahlexponenten bewies. (Siehe [*Hilbert*] Bd. I S. 349 ff.)
Die Fermatsche Vermutung war einer der Anstöße zum Aufbau der Algebraischen Zahlentheorie. (Wichtiger hierfür war allerdings das Interesse an der Entwicklung höherer Reziprozitätsgesetze.)
Die Mordell–Vermutung, die 1983 durch *Faltings* bewiesen wurde, liefert

bezüglich der Fermat–Vermutung zwar nur die Aussage, dass die Anzahl der primitiven Lösungen der Gleichung $x^n + y^n = z^n$ (für $n > 3$) endlich ist, geht andererseits an Allgemeinheit ganz wesentlich über die Fermat–Vermutung hinaus ([*Faltings, Wüstholz* et.al.]) [*Bombieri*]. Durch *Adleman* und *Heath–Brown* wurde 1985 der sogenannte erste Fall der Fermat–Vermutung für unendlich viele Primzahlexponenten bewiesen. D.h. für unendlich viele Primzahlen $p$ gibt es keine $a, b, c \in \mathbb{N}$ mit $a^p + b^p = c^p$ und $p \nmid abc$ ([*Heath–Brown*]).

Nachtrag (1999):
Inzwischen ist die Fermat-Vermutung duech Andrew Wiles endgültig und vollständig bewiesen worden.

# § 16

# Konstruktion der natürlichen, ganzen und rationalen Zahlen

Uns kommt es darauf an, die natürlichen Zahlen konstruktiv einzuführen und gleichzeitig ihre Bedeutung als Kardinalzahlen endlicher Mengen zu erklären. Hat man dies erst einmal geschafft und definiert dann Summe und Produkt mittels Vereinigung und kartesischem Produkt, so erhält man einfache und natürliche Beweise für die aritmetischen Grundgesetze (Kommutativität etc.). Der Zusammenhang zwischen den Verknüpfungen natürlicher Zahlen und denjenigen endlicher Mengen wird vielerorts in der Matematik benutzt, in diesem Buch etwa beim Beweis des „kleinen“ Satzes von Fermat (6.7).

Ein solches Programm ist in [*Lorenzen* 1] §§12-14 sehr präzise und filosofisch befriedigend durchgeführt.
Die folgenden Ausführungen lehnen sich an dieses Vorbild an, sind aber nicht so streng.
(Das genannte Buch wird in dem ganzen Paragrafen mit „l.c.“ zitiert.)

**16.1** Die positiven natürlichen Zahlen, d.h. die Elemente von $\mathbb{N}_1$, sollen hier als Symbole eingeführt werden, die wir kurz „Ziffern“ nennen wollen (nicht zu verwechseln mit den bekannten Ziffern, etwa des Dezimalsystems). Ziffern seien

$$|,\ ||,\ |||\quad \text{usw.}$$

Um klarzumachen, was dies – insbesondere das „usw." – bedeutet, geben wir einen Konstruktionsmechanismus, einen sogenannten Kalkül, an, mit dem man diese Ziffern allesamt erhält.

(1) $\longrightarrow |$,

d.h. $|$ ist eine Ziffer;

(2) $n \longrightarrow n|$,

d.h. wenn ich schon eine Ziffer $n$ konstruiert habe, so entsteht wieder eine Ziffer, indem ich rechts einen Strich anfüge. (In der Regel (2) ist $n$ eine Variable für Ziffern.)
In der Verwendung des Striches $|$ liegt natürlich eine Willkür. Ebensogut könnte man Punkte, Kreise, Kreuze, Kerben im Kerbholz (die auch ein Blinder ertasten kann), o.ä. nehmen.

**16.2** Das Wesentliche an Symbolen ist nicht ihre völlig exakte Ausführung – die ohnehin in aller Absolutheit nicht möglich wäre –, sondern dass man erkennen kann, ob zwei Ausführungen das gleiche Symbol darstellen oder nicht; d.h. dass man ein Symbol wiedererkennen und abschreiben kann.
Z.B. gilt $| \neq n|$ für jede Ziffer $n$.
Bei „längeren" Ziffern ist das Erkennen der Gleichheit nicht auf den ersten Blick möglich. Der Leser mag sich Verfahren ausdenken, die dieses kontrollieren.
(Man kann z.B. bei zwei zu vergleichenden Ziffern damit beginnen, bei beiden Ziffern gleichzeitig unter dem jeweils „ersten" (d.i. am weitesten linksstehenden) Strich einen weiteren Strich machen, so fährt man fort mit dem jeweils nächsten Strich usw. Man hat Gleichheit, wenn man gleichzeitig beim letzten Strich landet. Ebenso kann man die Gleichheit durch sukzessives „Wegnehmen" des jeweils letzten Striches kontrollieren.)
Wie man dies auch macht, man sollte die Richtigkeit der folgenden Aussage erkennen:

$$n = m \Longleftrightarrow n| = m|.$$

**16.3** *Es gilt das folgende Prinzip der vollständigen Induktion:*

*Sei $A(n)$ eine Aussage, wo $n$ eine Variable für Ziffern ist. Es gelte:*

*(1)* $A(|)$.

*(2)* $A(n) \Longrightarrow A(n|)$ *– und das für jede Ziffer* $n$.

*Dann gilt* $A(m)$ *für jede Ziffer* $m$.

Man kann sich nämlich davon überzeugen, dass es für jedes einzelne $m$ einen Beweis von $A(m)$ gibt.
Man erinnere sich, wie $m$ zu konstruieren ist:

$$|, \quad ||, \quad |||, \ldots, m.$$

Wegen (2) weiß man, dass aus $A(|)$ auch $A(||)$ folgt. Hieraus folgt $A(|||)$ wiederum wegen (2). Usw.
Parallel zur Konstruktion der Ziffer $m$ entwickelt man so einen Beweis für $A(m)$. $\square$

Man kann das Induktionsprinzip als eine matematische Erkenntnis, auffassen, die einer formal–logischen Ableitung weder bedarf, noch fähig ist.

**16.4 Endliche Mengen:** Eine endliche Menge konstituiert sich z.B. dadurch, dass gewisse Gegenstände einzeln angegeben werden. Diese werden als die Elemente der Menge bezeichnet.
Also: Jemand deutet auf „diesen Apfel, jene Birne,...“, und er hört irgendwann auf. (Damit kein Streit entsteht, ist eine schriftliche Fixierung vorzuziehen.) Dabei kommt es nur darauf an, ob ein gewisser Gegenstand als Element der Menge bezeichnet wird, aber nicht, wann, und nicht, wie oft.
Was dieser Satz bedeutet, wird in 16.6ff erklärt. (Wir sehen natürlich von praktischen Schwierigkeiten ab, etwa von der, dass die Lebensspanne eines Menschen zur Beschreibung gewisser endlicher Mengen auf die oben angegebene Weise nicht ausreicht, etc.)
Gelegentlich werden endliche Mengen als Mengen definiert, die zu keiner echten Teilmenge gleichmächtig sind. Nur definiert man auf diese Weise den relativ harmlosen Begriff einer „endlichen Menge“ durch den viel unbestimmteren Begriff einer allgemeinen Menge.
*Im folgenden – bis einschließlich 16.15 – soll unter einer endlichen Menge stets eine solche verstanden werden, die durch Einzelangabe ihrer Elemente gegeben ist.* Ferner werden wir uns hier auf Mengen von Symbolen

beschränken. Diese Beschränkung ist nicht sehr wesentlich, da man andere Objekte durch Namen angeben kann und Namen Symbole sind.
Endliche Mengen sind zum Beispiel

$$\{||,\ ||,\ |||,\ ||||, |\},\ \{||,\ |||\}.$$

(Zunächst verwenden wir Ziffern als Symbole, später auch Paare von solchen etc.) In den geschweiften Klammern steht eine Symbolsequenz (= System in l.c.), welche die Menge beschreibt. Verschiedene Symbolsequenzen können die gleiche Menge beschreiben, z.B.

$$\{||,\ ||,\ |||,\ |||||,\ |||\} = \{|||||,\ ||,\ |||\}.$$

Dazu Genaueres im nächsten Abschnitt.

**16.5** Sei $M$ eine endliche Menge, gegeben durch die (Symbol–) Sequenz $S$, also $M = \{S\}$. Für ein Symbol $x$ schreiben wir $x \in M$, wenn $x$ unter den Symbolen der Sequenz $S$ vorkommt. (Hier ist $x$ eine Variable für Symbole, $S$ eine solche für Sequenzen.) Es ist klar, dass man jemandem (ob Mensch, ob Computer) beibringen kann, wie er im konkreten Fall zu entscheiden hat, ob $x \in M$ gilt.

**Beispiele:** $|| \in \{||,\ ||||\},\quad | \notin \{||,\ |||\}.$

**16.6** Die Inklusionsbeziehung zwischen zwei endlichen Mengen

$$M \subset N \quad (\text{bzw.} N \supset M)$$

wird dadurch definiert, dass jedes Element von $M$ ein solches von $N$ ist, d.h.

$$M \subset N \ :\Longleftrightarrow [x \in M \Longrightarrow x \in N].$$

Auch hier ist klar, wie man (in endlicher Zeit) nachprüfen kann, ob $M \subset N$ gilt.

Die Gleichheit wird dann wie folgt definiert:

$$M = N :\Longleftrightarrow M \subset N \quad \text{und} \quad N \subset M.$$

**16.7** Man sieht hier, dass der Begriff „Symbolsequenz" im Grunde zuerst zu definieren ist. Dies geschieht analog zur Definition der Ziffern als „Strichsequenzen" (l.c. 12.1). Anschließend definiert man (induktiv), was

$$\text{„}x \text{ kommt in der Sequenz } S \text{ vor"}$$

zu bedeuten hat (l.c. 12.33). Dann definiert man für Symbolsequenzen eine Äquivalenzrelation „$\sim$" durch:

$$S \sim T :\Longleftrightarrow [x \text{ kommt in } S \text{ vor} \Longleftrightarrow x \text{ kommt in } T \text{ vor}].$$

(Zum Begriff „Äquivalenzrelation" siehe 6. A6) Schließlich macht man aus Symbolsequenzen durch den logischen Prozess der „Abstraktion" bezüglich „$\sim$" endliche Mengen.
D.h. man bildet zu jeder Symbolsequenz $S$ ein abstraktes Objekt, die endliche Menge $\{S\}$, und definiert

$$\{S\} = \{T\} :\Longleftrightarrow S \sim T.$$

Was sind aber nun die abstrakten Objekte $\{S\}$?
Anstelle dieser Frage wird die folgende (pragmatischere) Frage beantwortet: Wie geht man mit ihnen um?

Aussagen über endliche Mengen sind Aussagen über Sequenzen $\mathcal{A}(S)$ (mit einer freien Variablen $S$ oder auch mehreren solchen), für die

$$S \sim T \Longrightarrow [\mathcal{A}(S) \Longleftrightarrow \mathcal{A}(T)]$$

gilt.

Z.B. ist die Aussage

$$\mathcal{A}(S) := \text{„}| \text{ kommt als erstes Element in } S \text{ vor"}$$

keine Aussage über Mengen $\{S\}$. Denn es gilt zwar

$$|,\ || \sim ||,\ |,$$

aber $\mathcal{A}(|,\ ||)$ ist richtig und $\mathcal{A}(||,\ |)$ ist falsch. Hingegen ist

$$\{S\} \subset \{T\}$$

eine Aussage über Mengen. Denn aus $S \sim S'$, $T \sim T'$ folgt

$$\{S\} \subset \{T\} \Longleftrightarrow \{S'\} \subset \{T'\}.$$

(„$\Longrightarrow$" z.B. wird wie folgt bewiesen: $x$ komme in $S'$ vor. Wegen $S \sim S'$ kommt $x$ auch in $S$ vor, also wegen $\{S\} \subset \{T\}$ auch in $T$. Aus $T \sim T'$ erhält man schließlich: $x$ kommt in $T'$ vor.)
Der Abstraktionsprozess wird auch in l.c. §10 und [*Lorenzen* 2] §2 beschrieben.

Gemeinhin werden in der Matematik die abstrakten Objekte bezüglich einer Äquivalenzrelation „$\sim$" als sogenannte Äquivalenzklassen, d.h. als gewisse Mengen, definiert. (Die Äquivalenzklassen z.B. bezüglich der Kongruenz modulo $m$ sind die Restklassen modulo $m$.) Dementsprechend wäre die endliche Menge $\{S\}$ definiert als die unendliche Klasse aller Sequenzen $T$ mit $T \sim S$. Wenn hierin kein Zirkel liegen soll, muss man Klassen (oder Mengen) als undefinierten Grundbegriff in der Matematik verwenden.

**16.8** Jeder endlichen Menge $M$ wollen wir eine Ziffer als ihre Mächtigkeit oder Kardinalzahl $\#M$ zuordnen.
Folgendes Verfahren ist naheliegend:

Sei $M = \{S\}$. Gehe die Sequenz $S$ von links an durch und mache jedesmal einen Strich, wenn ein neues, vorher noch nicht dagewesenes Symbol erscheint. Nachdem man erst einmal $S$ gewählt hat, ist dieses Verfahren offenbar determiniert.

Ich will jetzt, l.c. §14 folgend, beweisen, dass $\#M$ auch von der Wahl der Sequenz $S$ (mit $M = \{S\}$) nicht abhängt. Wem dies als unnötige Pedanterie erscheint, der mag mit 16.11 fortfahren.
Zunächst definieren wir die Länge $L(S)$ einer Sequenz $S$:
$L(S)$ sei diejenige Ziffer, die entsteht, wenn man beim Durchlaufen der Sequenz $S$ beim ersten Symbol und dann nach jedem Komma (d.h. für jedes Symbol sooft es in $S$ auftaucht) einen Strich macht.
(Man kann $L$ induktiv, wie folgt, definieren:

(1) $L(x) := |$, wenn $x$ ein Symbol ist,

(2) $L(S, x) := L(S)|$, wenn $S$ eine Sequenz ist und $x$ ein Symbol, also auch $S, x$ eine Sequenz ist.

Zur Berechtigung solcher induktiver Definitionen siehe l.c. S. 122 ff.

Wir nennen eine Sequenz einfach, wenn in ihr kein Symbol mehrfach auftritt. (Dies lässt sich mechanisch nachprüfen.)

**Lemma:** *Sind $x, y$ Symbole, $S$ eine einfache Sequenz mit $y \in \{S, x\}$, so gibt es eine einfache Sequenz $T$ mit*

$$\{S, x\} = \{T, y\} \quad \textit{und} \quad L(S) = L(T).$$

**Beweis:** Induktion nach $L(S)$.
Ist $L(S) = |$, also $S = z$ mit einem Symbol $z$, so ist die Behauptung trivial: $T := z$, wenn $y = x$, bzw. $T := x$, wenn $y = z$ ist.
Sei nun die Behauptung für ein $S$ vorausgesetzt. Es genügt dann, sie für $S, z$ mit einem Symbol $z$ zu zeigen.
Sei also $y \in \{S, z, x\}$. Dann ist $y \in \{S, z\}$ oder $y = x$.
Wenn $y = x$ ist, setze $T := S, z$.
Wenn $y \in \{S, z\}$ ist, gibt es nach Induktionsvoraussetzung ein $T'$ mit $\{S, z\} = \{T', y\}$ und $L(S) = L(T')$. Setze dann $T := T', x$. □

**16.9** Wenn man eine Sequenz $S$ von links nach rechts durchgeht und jedes Symbol streicht, das bereits vorher aufgetaucht war, erhält man eine einfache Sequenz $S'$ mit $\{S\} = \{S'\}$.
Jede endliche Menge $M$ ist also von der Form $M = \{S\}$ mit einer einfachen Sequenz $S$. Aus dem Lemma folgt

**Satz:** *Seien $S, T$ einfache Sequenzen mit $\{S\} = \{T\}$, so ist $L(S) = L(T)$.*

**Beweis:** *Induktion nach $L(S)$. Sei zunächst $L(S) = |$. Dann ist $S = x$ mit einem Symbol $x$ und deshalb auch $T = x$ und die Aussage trivial.*

*Wir setzen jetzt also die Aussage für den Fall $L(S) = n$ voraus. Und betrachten ein $S$ mit $L(S) = n|$. Wir können $S = U, x$ mit einer Sequenz $U$ und einem Symbol $x$ schreiben. Auch $T$ is von der Form $T = V, y$. Wäre nämlich $T = y$ so würde wie oben $S = y$ folgen. Nach dem Lemma gibt es eine Sequenz $U'$ mit $S = U', y$ und $L(U') = L(U)$. Nun ist es ein Leichtes, zu* *überlegen, dass $U' = V$ ist, also nach Induktionsvoraussetzung $LU') = L(V)$ gilt. Es folgt $L(S) = L(U')| = L(V)| = L(T)$.* □

**Definition:** *Sei $M = \{S\}$ eine endliche Menge mit einer einfachen Sequenz $S$. Dann definieren wir $\#M := L(S)$ und nennen $\#M$ die Kardinalzahl von $M$.*

**16.10** Es wird sich als nützlich erweisen, unseren Symbolvorrat zu erweitern. Wir führen sogenannte Paare ein, wieder durch einen Kalkül

$$m, n \longrightarrow (m, n).$$

D.h. wenn wir schon Symbole $n, m$ haben (etwa Ziffern), dann ergibt sich als neues Symbol das „Paar" $(m, n)$. Die Gleichheit von Paaren ist die Gleichheit im Sinne von Symbolen, also:

$$(m, n) = (m', n') \Longleftrightarrow m = m' \quad \text{und} \quad n = n'.$$

Paare sind im Grunde Sequenzen der Länge 2 $(= ||)$. Durch die Einklammerung wollen wir angeben, dass sie in einer Sequenz als Einzelsymbol zu lesen (und zu zählen) sind:

$$L\left((|, |), |\right) = ||, \ L\left((|, |)\right) = |, \ L\left((|, ||), ((|, ||), |)\right) = ||.$$

Sind $M$ und $N$ endliche Mengen, so wird mit $M \times N$ die Menge aller Paare $(m, n)$ mit $m \in M$, $n \in N$ bezeichnet. Seien $S, T$ Sequenzen mit $M = \{S\}$, $N = \{T\}$, so ist klar, wie man eine Sequenz $S \times T$ konstruieren kann, in der alle Paare $(m, n)$ vorkommen, derart dass $m$ in $S$ und $n$ in $T$ vorkommt. Wenn $S = x_1, \ldots, x_m$, $T = y_1, \ldots, y_n$ ist, so definieren wir (etwa)

$$S \times T := (x_1, y_1), (x_1, y_2), \ldots, (x_1, y_n), (x_2, y_1), \ldots, (x_m, y_n).$$

**16.11** Eine Abbildung

$$f : M \longrightarrow N$$

wird dadurch gegeben, dass man jedem Element $m \in M$ genau ein Element $f(m) \in N$ „zuordnet". (Man beachte, dass hier der Pfeil $\longrightarrow$ in einer anderen Bedeutung benutzt wird als in Kalkülen.)
Das heißt, $f$ ist (oder wird gegeben durch) eine Menge von Paaren $(m, n)$ mit $m \in M$, $n \in N$, also $(m, n) \in M \times N$, für die folgendes gilt:

(i) $m \in M \Longrightarrow$ es gibt ein $n \in N$ mit $(m,n) \in f$.

(ii) $(m,n) \in f$ und $(m,n') \in f \Longrightarrow n = n'$.

Es ist klar, dass man eine (durch eine Sequenz gegebene) Teilmenge von $M \times N$ daraufhin überprüfen kann, ob sie eine Abbildung ist.
(In der Regel unterscheidet man eine Abbildung $f$ – im Sinne einer Zuordnungsvorschrift – von der durch sie bestimmten Teilmenge von $M \times N$. Letztere wird dann ihr Graf genannt und mit $\Gamma_f$ bezeichnet.) Das Element $f(m)$ wird durch $(m, f(m)) \in f$ definiert.

Die identische Abbildung einer Menge $M$:

$$id_M : M \longrightarrow M$$

wird durch die Menge aller Paare $(m,m)$ mit $m \in M$ gegeben:

$$M = \{x_1, \ldots, x_m\} \Longrightarrow id_M = \{(x_1,x_1),(x_2,x_2), \ldots (x_m,x_m)\}.$$

**16.12** Die Begriffe „injektiv", „surjektiv" und „bijektiv" werden wie üblich definiert. Und wieder ist klar, wie man nachprüfen kann, ob eine durch eine Sequenz konkret gegebene Abbildung eine dieser Eigenschaften hat.

Z.B. ist die folgende Abbildung bijektiv:

$$f : M \times N \longrightarrow N \times M, \quad f(m,n) := (n,m).$$

Wenn $f : M \longrightarrow N$ bijektiv ist, dann ist die Teilmenge $g$ von $N \times M$, welche durch

$$(n,m) \in g \Longleftrightarrow (m,n) \in f$$

gegeben ist – und zwar auf naheliegende Weise durch eine Sequenz –, offenbar wieder eine Abbildung. (Für $g$ gilt (i), weil $f$ surjektiv, (ii), weil $f$ injektiv ist.) Sie wird die zu $f$ inverse Abbildung genannt und mit $f^{-1}$ bezeichnet. Man sieht auch sofort, dass $f^{-1}$ bijektiv und $(f^{-1})^{-1} = f$ ist.

**16.13** Zwei endliche Mengen $M$ und $N$ heißen gleichmächtig, wenn es eine bijektive Abbildung

$$f : M \longrightarrow N$$

gibt. Wir schreiben dann $M \sim N$.
Offenbar gilt für jede (endliche) Menge $M$ die Beziehung $M \sim M$.
Ferner folgt $N \sim M$ aus $M \sim N$ (wegen der Möglichkeit, $f^{-1}$ zu einer bijektiven Abbildung $f$ zu bilden.) Schließlich gilt:

$$M \sim N, \quad N \sim P \Rightarrow M \sim P.$$

Denn wenn Abbildungen

$$f : M \longrightarrow N \quad \text{und} \quad g : N \longrightarrow P$$

beide bijektiv sind, ist es auch ihre Verkettung

$$g \circ f : M \longrightarrow P, \quad g \circ f(m) = g(f(m)).$$

**Satz: 16.14** *Seien $M$, $N$ endliche Mengen. $M$ und $N$ sind genau dann gleichmächtig, wenn $\#M = \#N$ ist.*

**Beweis:** Seien $S$, $T$ einfache Sequenzen mit $M = \{S\}$, $N = \{T\}$. Etwa

$$S = x_1, \ldots, x_m, \quad T = y_1, \ldots, y_n.$$

Sei jetzt $\#M = \#N$, d.h. $L(S) = L(T)$. Man kann dann versuchen, folgende Sequenz von Paaren zu bilden:

$$F := (x_1, y_1), (x_2, y_2), \ldots.$$

$L(S) = L(T)$ bedeutet offensichtlich, dass dies „aufgeht“, d.h. mit $(x_m, y_n)$ endet. (Ein präziser Beweis arbeitet mit Induktion nach $L(S)$. Der Leser möge einen solchen durchführen.) Die Menge $\{F\}$ ist dann eine bijektive Abbildung von $M$ nach $N$.

Umgekehrt, sei $S$ wie oben. Ferner sei $f : M \longrightarrow N$ eine bijektive Abbildung. Dann ist die Sequenz

$$f(S) := f(x_1), \ldots, f(x_m)$$

ebenfalls einfach, da $f$ injektiv ist. Ferner gilt $N = \{f(S)\}$, da $f$ surjektiv ist. Nun sieht man $L(S) = L(f(S))$. (Genau genommen muss man $f(S)$ induktiv definieren und kann dann induktiv die Gleichheit der Längen zeigen.) $\square$

Jede Ziffer ist eine Kardinalzahl: Sei $n$ wie in 16.1 konstruiert:

$$|,\ ||,\ |||, \ldots, n.$$

Man erhält eine einfache Sequenz der Länge $n$.

Man hat nun die Wahl, was man als positive ganze Zahlen betrachten will: Ziffern, oder abstrakte Objekte, die durch Abstraktion bezüglich der Gleichmächtigkeit aus endlichen (nichtleeren) Mengen hervorgehen. Für das Umgehen mit Zahlen spielt das keine Rolle.

Da das Hinschreiben eines leeren Symbols eine missliche Sache ist, haben wir bis jetzt weder die leere Menge noch die 0 definiert. Das wird im nächsten Abschnitt nachgeholt.
*Ab jetzt verwenden wir die üblichen Bezeichnungen* $1 = |,\ 2 = ||, \ldots$

**16.15** Allgemein werden Mengen durch Aussagenformen (d.h. Aussagen mit einer freien Variablen) definiert:
$M$ ist die Menge derjenigen $x$, für die $\mathcal{A}(x)$ gilt:

$$M = \{x \mid \mathcal{A}(x)\}.$$

Dann kann man definieren: $y \in M \ :\Longleftrightarrow\ \mathcal{A}(y)$.
Verschiedene Aussagen können dieselbe Menge beschreiben, z.B.

$$\begin{aligned} &\{x \mid x = 1 \text{ oder } x = 2\} \\ &= \{x \mid x \text{ ist eine positive ganze Zahl und } x \leq 2\}. \end{aligned}$$

Mengen entstehen also aus Aussagenformen durch Abstraktion bezüglich der folgenden Äquivalenzrelationen zwischen Aussagenformen.

Für alle $x$ gilt: $[\mathcal{A}(x) \iff \mathcal{B}(x)]$.

Wenn man nun die durch eine Sequenz gegebene endliche Menge
$M = \{x_1, \ldots, x_n\}$ mit der durch eine Aussageform gegebenen Menge $M' := \{x \mid x = x_1 \text{ oder } \ldots \text{ oder } x = x_n\}$ vergleicht, so sieht man, dass sie

dieselben Elemente haben, d.h.

$$x \in M \iff x \in M'.$$

Wir werden deshalb keinen Unterschied zwischen beiden machen.
Wir definieren die leere Menge:

$$\emptyset := \{x \mid x \neq x\}.$$

Wir betrachten sie als endliche Menge und kreieren eine neue Zahl 0 mit

$$0 = \#\emptyset.$$

Für diese sei $0 < n$ für alle positiven ganzen Zahlen festgelegt, ferner $0 \leq 0$. Die natürlichen Zahlen sind $0, 1, \ldots$. Mit $\mathbb{N}$ wird die Menge $\{x \mid x \text{ ist eine natürliche Zahl}\}$ bezeichnet.

**16.16** Für Mengen $M, N$ sind definiert

$$\begin{aligned} M \cup N &:= \{x \mid x \in M \ \text{ oder } \ x \in N\}, \\ M \cap N &:= \{x \mid x \in M \ \text{ und } \ x \in N\}, \\ M - N &:= \{x \mid x \in M \ \text{ und } \ x \notin N\}. \end{aligned}$$

Wenn $M, N$ endlich sind, so auch $M \cup N$, $M \cap N$, $M - N$. Man kann jeweils ein Verfahren angeben, wie aus Sequenzen, die $M$ und $N$ beschreiben, eine solche wird, die $M \cup N$ bzw. $M \cap N$ bzw. $M - N$ beschreibt. (Dies geht übrigens nicht unbedingt für $M \cap N$ und $M - N$, wenn zwar $M$, aber nicht $N$ endlich ist.) Es ist $M \cup \emptyset = M - \emptyset = M$ und $M \cap \emptyset = \emptyset$.

$M$ und $N$ heißen (zueinander) disjunkt, wenn $M \cap N = \emptyset$ gilt.

Zu Mengen $M$ und $N$ gibt es zueinander disjunkte Mengen $M'$ und $N'$, derart dass $M$ zu $M'$ und $N$ zu $N'$ gleichmächtig ist. Definiere etwa:

$$M' := \{(x, 0) \ \mid \ x \in M\} \ \text{ und } \ N' := \{(x, 1) \ \mid \ x \in N\}\ .$$

**16.17** Seien $M$ zu $N$ disjunkt und $M'$ zu $N'$ disjunkt. Wenn $M$ gleichmächtig zu $M'$ und $N$ gleichmächtig zu $N'$ ist, so sind auch $M \cup N$ und

$M' \cup N'$ gleichmächtig.

Aus bijektiven Abbildungen $M \longrightarrow M'$, $N \longrightarrow N'$ kann man nämlich leicht eine solche von $M \cup N$ nach $M' \cup N'$ zusammenbasteln.

*Seien nun $m, n \in \mathbb{N}$. Dann gibt es nach Obigem disjunkte endliche Mengen $M$ und $N$ mit $\#M = m$, $\#N = n$.*
*Wir definieren:*

$$m + n := \#(M \cup N).$$

*Dies ist, wie gerade gesehen, wohldefiniert.*

**16.18** Die „Rechengesetze“ Kommutativität, Assoziativität und Existenz eines neutralen Elementes – nämlich $0 = \#\emptyset$ – für die Addition folgen jetzt aus den elementaren Gesetzen der Mengenlehre:

$$m + n = n + m \text{ folgt aus } M \cup N = N \cup M.$$

Für die Assoziativität braucht man außer

$$K \cup (M \cup N) = (K \cup M) \cup N$$

noch:

$$K \cap (M \cup N) = \emptyset, \ \ M \cap N = \emptyset \Longrightarrow K \cap M = \emptyset \ \text{ und } \ (K \cup M) \cap N = \emptyset.$$

Offenbar ist $0 = \#\emptyset$ ein neutrales Element.

Ferner ist $n + 1 = n|$ für positive ganze Zahlen $n$.
Sei nämlich $S$ eine einfache Sequenz der Länge $n$ und $x \notin \{S\}$. Dann ist

$$n + 1 = \#(\{S\} \cup \{x\}) = \#\{S, x\} = L(S, x) = n|.$$

Vor der Einführung der Relation '$\leq$' beweisen wir folgenden

**Satz: 16.19** *Seien $M$, $N$ gleichmächtige Mengen unf $f : M \to N$ injektiv. Dann ist $f$ auch surjektiv.*

**Beweis:** Induktion nach der gemeinsamen Mächtigkeit $n$ der beiden Mengen. Im Falle $n = 0$ ist dei Aussage leer. Sei jetzt die Richtigkeit für $n$ vorausgesetzt und $\#M = \#N = n| = n + 1$. Wäre $f : M \to N$ injektiv aber nicht surjektiv, so gäbe es ein $y \in N$, welches nicht im Bild von $f$ läge. Die Abbildung $f$ wäre – als Teilmenge von $M \times (N - \{y\})$ – auch eine injektive Abbildung $M \to N - \{y\}$. Sei jetzt $x \in M$ beliebig. Die Einschränkung $f' : M - \{x\} \to N - \{y\}$ wäre auch injektiv, also nach Induktionsvoraussetzung surjektiv. Also gäbe es ein $x' \in M - \{x\}$ mit $f(x') = f(x)$ im Widerspruch zur Injektivität von $f$. □

**Satz: 16.20** *Seien $M, N$ endliche Mengen mit $\#M = m$ und $\#N = n$. Folgende Aussagen sind äquivalent:*

*(i) Es gibt ein $k \in \mathbb{N}$ mit $m + k = n$;*

*(ii) es gibt eine injektive Abbildung $f : M \longrightarrow N$.*

**Beweis:** ‘$(i) \Longleftrightarrow (ii)$’: Es gibt eine Menge $M'$ mit einer bijektiven Abbildung $g : M \to M'$ und eine Menge $K$ mit $\#K = k$, die zu $M'$ disjunkt ist. Nach $(i)$ gibt es ferner eine bijektive Abbildung $f : M' \cup K \to N$. Dann ist offenbar $f \circ g : M \to N$ injektiv.

’$(ii) \Longleftrightarrow (i)$’: Sei $N' \subset N$ das Bild von $f$ und $K = N - N'$. Da $f$ injektiv ist, gilt $\#N' = \#M$. Offenbar ist $K \cap N' = \emptyset$ und deshalb $m + k = n$, wo $k := \#K$ sei. □

**Definition: 16.21** *Wir schreiben $m \leq n$ und sagen $m$ ist kleiner (als oder) gleich $n$, wenn $m$ und $n$ die Aussage $(i)$ obigen Satzes erfüllen.*

**Satz: 16.22** *Die Relation ‘$\leq$’ definiert eine totale Anordnung auf $\mathbb{N}$.*

**Beweis:** a) Da die Identität auf einer Menge bijektiv, also injektiv ist, gilt $n \leq n$ für alle $n \in \mathbb{N}$, d.h. ‘$\leq$’ ist reflexiv.
b) Die Verkettung injektiver Abbildungen ist injektiv. Deshalb impliziert $k \leq m$, $m \leq n$, dass $k \leq n$ ist. Die Relation ‘$\leq$’ ist somit transitiv.
c) Sei $m \leq n$ und $n \leq m$. Dann gibt es $k, k' \in \mathbb{N}$ mit $m + k = n$ und $n + k' = m$. Es folgt $m + k + k' = m$. D.h. es gibt untereinander disjunkte Mengen $M, K, K'$ mit $\#M = m$, $\#K = k$, $\#K' = k'$, so dass $M$ zu $M \cup$

$K \cup K'$ gleichmächtig ist. Die Identität auf $M$ gibt eine injektive Abbildung $f : M \to M \cup K \cup K'$,deren Bild gleich $M$ ist. Da $f$ nach Satz **??** bijektiv ist, müssen die Elemente von $K \cup K'$ auch im Bild liegen. Da aber $K \cup K'$ disjunkt zum Bild ist, muss es leer sein. Es folgt $K = \emptyset$, also $k = 0$ und schließlich $m = n$. Das bedeutet die Antisymmetrie.
d) Um die Totalität zu zeigen, d.h., dass für je zwei natürliche Zahlen $m \leq n$ oder $n \leq m$ gilt, beweisen wir, dass für endliche Mengen aus der Nichtexistenz einer injektiven Abbildung $N \to M$, die Existenz einer solchen $M \to N$ folgt. Dies geschieht mit Induktion nach $\#M$, wobei der Fall $\#M = 0$ trivial ist. Sei $\#M \neq 0$ und $p \in M$. Dann gibt es auch keine injektive Abbildung $N \to M - \{p\}$, da eine solche auch eine injektive Abbildung $N \to M$ wäre. Nach Induktionsvoraussetzung gibt es eine injektive Abbildung $f : M - \{p\} \to N$. Ist $f$ nicht surjektiv, etwa $q \neq f(M)$, so kann man $f$ durch $p \mapsto q$ zu einer injektiven Abbildung $M \to N$ fortsetzen. Ist hingegen $f$ surjektiv, also bijektiv, so ist $f^{-1} : N \to M - \{p\}$ injektiv, was – wie oben gesehen – nicht geht. $\square$

**Definitionen: 16.23** *a)* $m < n :\iff m \leq n$ *und* $m \neq n$ .
*b)* $m \geq n :\iff n \leq m$ .
*c)* $m > n :\iff n < m$ .

**16.24 Korollar** (*Dirichlets* Schubfachprinzip):
*Sei $f : M \longrightarrow N$ eine Abbildung endlicher Mengen und $\#M > \#N$. Dann ist $f$ nicht injektiv.*
*(Wenn man in $n$ Schubfächern mehr als $n$ Gegenstände verstaut hat, enthält mindestens ein Schubfach mehr als einen Gegenstand.)*

**Beweis:** Aus der Injektivität würde $\#M \leq \#N$ folgen. Dieses stünde im Widerspruch zu $\#M > \#N$, was ja $\#M \geq \#N$ und $\#M \neq \#N$ bedeutet. Man hätte zugleich $\#M = \#N$ (wegen der Antisymmetrie von „$\leq$“) und $\#M \neq \#N$. $\square$

**16.25** *Wenn die Ordnungsgesetze Reflexivität, Transitivität und Antisymmetrie für eine Relation „$\leq$“ (auf irgendeiner Menge) erfüllt sind, gilt:*

$$\begin{aligned} &a \leq b,\ b < c \Rightarrow a < c \quad \textit{und} \\ &a < b,\ b \leq c \Rightarrow a < c. \end{aligned}$$

Denn zunächst folgt $a \leq c$. Wäre $a = c$, so ergäbe sich aus der Antisymmetrie $a = b = c$ im Widerspruch zu den jeweiligen Voraussetzungen.

**Lemma: 16.26** *Sei $n \in \mathbb{N}$, $n \neq 0$. So ist $n \geq 1$.*

**Beweis:** Es genügt, das folgende zu zeigen: Seien $M, P$ endliche Mengen mit $M \neq \emptyset$, $\#P = 1$; dann gibt es eine injektive Abbildung $P \to M$. Sei nämlich $P = \{p\}$ und $M = \{S\}$ mit einem Element $p$ und einer Sequenz $S = s_1, s_2, \ldots$. So definiere man $f : P \to M$ durch $f(p) := s_1$. (Man braucht kein Auswahlaxiom, da $M$ konstruktiv gegeben ist.) □

**Korollar: 16.27** *Seien $m, n, r \in \mathbb{N}$. Aus $m \leq n$ (bzw. $m < n$) folgt $m + r \leq n + r$ (bzw. $m + r < n + r$).*

**Beweis:** Sei $m \leq n$, also $m + k = n$ für ein $k \in \mathbb{N}$. Dann ist $(m + r) + k = n + r$, also $m + r \leq n + r$.
Sei nun $m < n$, also $m \leq n$ und $m \neq n$, d.h. $m + k = n$ für ein $k \in \mathbb{N}$ mit $k \neq 0$. Nach ist $k \geq 1$. Es folgt $(m + r) + 1 \leq (m + r) + k = n + r$. Nun ist $m + r \neq (m + r)| = (m + r) + 1$, also $m + r < (m + r) + 1$.
Mit 16.24 folgt $m + r < n + r$. □

**Korollar: 16.28** *Aus $m + r \leq n + r$ folgt $m \leq n$.*
*Insbesondere folgt aus $m + r = n + r$ die Gleichheit $m = n$ (Kürzungsregel für die Addition).*

**Beweis:** Wäre $n < m$, so auch $n + r < m + r$.
Die Behauptung für die Gleichheit folgt mit der Antisymmetrie. □

**16.29** a) *Seien $m, n \in \mathbb{N}$. Wir definieren das Produkt $m \cdot n$ (auch $mn$ geschrieben) wie folgt:*
*Wähle endliche Mengen $M, N$ mit $m = \#M$, $n = \#N$. Setze dann*

$$m \cdot n := \#(M \times N).$$

(Mit der üblichen Schreibweise $mn$ ist natürlich hier nicht gemeint, man solle $m, n$ als Strichfiguren schreiben und dann nebeneinandersetzen.)

Dies ist wohldefiniert. Denn aus bijektiven Abbildungen

$$M \longrightarrow M', \quad N \longrightarrow N'$$

bekommt man leicht eine solche

$$M \times N \longrightarrow M' \times N'.$$

b) Da $M \times N$ zu $N \times M$ gleichmächtig ist (16.13), folgt sofort die Kommutativität der Multiplikation.

c) Ebenso sind trivialerweise $(K \times M) \times N$ und $K \times (M \times N)$ gleichmächtig. Es folgt die Assoziativität der Multiplikation.

d) Auch die Distributivität sieht man ganz einfach. Seien $K, M, N$ endliche Mengen, $M \cap N = \emptyset$. Dann ist auch $(K \times M) \cap (K \times N) = \emptyset$. Und es gilt

$$(K \times M) \cup (K \times N) = K \times (M \cup N).$$

e) Schließlich sieht man noch

$$mn = 0 \Longleftrightarrow [m = 0 \text{ oder } n = 0].$$

**16.30** Es gilt folgendes Monotoniegesetz:

*Seien $k, m, n \in \mathbb{N}$, $0 < k$ und $m < n$. Dann ist $km < kn$.*

Denn da $m \leq n$ ist, gibt es ein $r \in \mathbb{N}$ mit $m + r = n$. Wegen $m \neq n$ ist $r \neq 0$ und deshalb $kr \neq 0$ nach 6.27 e), also $kr > 0$. Mit 16.25 folgt

$$km < km + kr = k(m + r) = kn. \qquad \square$$

**Korollar: 16.31** *Seien $k, m, n \in \mathbb{N}$, $k \neq 0$. Aus $km = kn$ folgt $m = n$ (Kürzungsregel für die Multiplikation).*

**Beweis:** Wäre etwa $m < n$, so wäre $km < kn$. $\square$

**16.32** $\mathbb{N}$ zusammen mit Addition und Multiplikation erfüllt alle Axiome eines Ringes mit Ausnahme der Existenz von additiv Inversen.

Es gilt sogar (in $\mathbb{N}$):

$$m+n=0 \Longleftrightarrow m=n=0.$$

Denn die Vereinigung zweier Mengen $M, N$ ist genau dann leer, wenn $M$ und $N$ es sind. Also besitzt nur die Null ein Inverses (bzgl. $+$), nämlich sich selbst.
($\mathbb{N}$ ist sogenannter Halbring.)

Um aus $\mathbb{N}$ einen Ring zu machen, hat man zwei Möglichkeiten:

1. Man nimmt zu $\mathbb{N}$ für jedes $n \in \mathbb{N}_1$ ein neues Element $-n$ hinzu, definiert dann $+$, $\cdot$, $\leq$ und prüft die in §0 angegebenen Gesetze eines geordneten Ringes nach.

2. Man betrachtet die Paarmenge $\mathbb{N} \times \mathbb{N}$, führt auf ihr eine Äquivalenzrelation ein, macht diese durch Abstraktion zu einer Gleichheit, definiert $+$, $\cdot, \leq$, prüft die Ringgesetze nach und zeigt dann, dass sich $\mathbb{N}$ in diese Menge einbetten lässt.

Das zweite Verfahren ist – obwohl es auf den ersten Blick komplizierter aussieht – eleganter und verallgemeinerungsfähiger.
(Der Halbring der Isomorfietypen von Vektorbündeln (bzw. projektiven Moduln) über einem topologischen Raum (bzw. Ring) lässt sich nach der ersten Metode nicht zu einem Ring machen. Auch wenn man für $\mathbb{N}$ oder $\mathbb{Z}$ multiplikativ Inverse, also rationale Zahlen einführen will, muss man analog zur zweiten Metode vorgehen.)

**16.33** a) Auf $\mathbb{N} \times \mathbb{N}$ definiert man eine Äquivalenzrelation „$\sim$“ wie folgt:

$$(m,n) \sim (m',n') :\Longleftrightarrow m+n' = m'+n.$$

(Das Paar $(m,n)$ wird später gleich der Differenz $m-n$.)

Nur die Transitivität ist nicht völlig trivial. Aus $(m,n) \sim (m',n')$ und $(m',n') \sim (m'',n'')$ folgt

$$m+n' = m'+n \ \text{ und } \ m'+n'' = m''+n',$$

also
$$m + n' + n'' = m' + n + n'' = m'' + n' + n.$$
Indem man $n'$ wegkürzt (16.26), erhält man $m + n'' = m'' + n$, d.h. $(m, n) \sim (m'', n'')$.

$\Big($Falls ein Halbring ohne Kürzungsregel für die Addition vorliegt, wie z.B. oft bei Vektorbündeln, muss man die Relation „$\sim$" wie folgt definieren:
$$(m, n) \sim (m', n') :\Longleftrightarrow \text{ es gibt ein } k \text{ mit } m + n' + k = m' + n + k.\Big)$$

b) Wir definieren jetzt auf $\mathbb{N} \times \mathbb{N}$ eine Addition und eine Multiplikation durch:
$$\begin{array}{rcl} (a, b) + (c, d) & := & (a + c,\ b + d) \\ (a, b) \cdot (c, d) & := & (ac + bd,\ ad + bc) \\ (a, b) \leq (c, d) & :\Longleftrightarrow & a + d \leq b + c. \end{array}$$

(Diese Definitionen werden verständlich, wenn man $(a, b)$ als – möglicherweise noch nicht definierte – Differenz $a - b$ ansieht.)

c) Die Verknüpfungen „$+$" und „$\cdot$" sind mit der Äquivalenzrelation „$\sim$" verträglich. Das heißt folgendes: Für
$a, b, c, d, a', b', c', d' \in \mathbb{N}$ mit $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$ gilt:

(i) $(a, b) + (c, d) \sim (a', b') + (c', d')$,

(ii) $(a, b) \cdot (c, d) \sim (a', b') \cdot (c', d')$.

**Beweis:** (i): Es ist $(a, b) + (c, d) = (a + c, b + d) \sim (a' + c', b' + d')$, da $a + b' = a' + b$ und $c + d' = c' + d$, also
$$a + c + b' + d' = b + d + a' + c'$$
ist.

(ii): $(a, b)(c, d) = (ac + bd,\ ad + bc) \sim (a'c + b'd,\ a'd + b'c)$, da wegen $a + b' = a' + b$ die Gleichungen
$$ac + b'c = a'c + bc \text{ und } a'd + bd = ad + b'd$$

gelten und hieraus (durch Addition dieser Gleichungen)

$$(ac+bd)+(a'd+b'c)=(ad+bc)+(a'c+b'd)$$

folgt.
Deshalb ist

$$(a,b)\cdot(c,d)\sim(a',b')\cdot(c,d).$$

Ebenso erhält man

$$(a',b')(c,d)\sim(a',b')\cdot(c',d').$$

Insgesamt folgt (ii).

□

**16.34** a) Wir abstrahieren jetzt bezüglich der Relation „∼“ und nennen die abstrakten Objekte ganze Zahlen und ihre Menge $\mathbb{Z}$. Wegen der Verträglichkeitsaussagen aus 16.31 haben wir auf $\mathbb{Z}$ Verknüpfungen $+$ und $\cdot$ definiert.

b) Wir wollen jetzt zeigen, dass $\mathbb{Z}$ ein Ring ist, werden allerdings nicht alle Einzelheiten ausführen:

Da die Addition von Paaren „komponentenweise“ definiert war, sind Kommutativität und Assoziativität der Addition trivial.

c) Ein additiv neutrales Element wird durch das Paar (0,0) gegeben, aber auch durch jedes Paar $(m,m)$.

d) Zur durch $(m,n)$ gegebenen Zahl ist die durch $(n,m)$ gegebene additiv invers. Denn

$$(m,n)+(n,m)=(m+n,n+m)\sim(0,0).$$

e) Die Kommutativität der Multiplikation ist auch trivial. Ferner liefert (1,0) ein neutrales Element für die Multiplikation.
Zur Assoziativität der Multiplikation:

$$\begin{aligned}&(a_1,a_2)\cdot((b_1,b_2)\cdot(c_1,c_2))\\&=(a_1,a_2)(b_1c_1+b_2c_2,b_1c_2+b_2c_1)\\&=(a_1b_1c_1+a_1b_2c_2+a_2b_1c_2+a_2b_2c_1,\ a_1b_1c_2+a_1b_2c_1+a_2b_1c_1+a_2b_2c_2);\end{aligned}$$

$$\begin{aligned}
&((a_1, a_2) \cdot (b_1, b_2))\,(c_1, c_2) \\
&= (a_1b_1 + a_2b_2, a_2b_1 + a_1b_2)(c_1, c_2) \\
&= (a_1b_1c_1 + a_2b_2c_1 + a_2b_1c_2 + a_1b_2c_2,\ a_1b_1c_2 + a_2b_2c_2 + a_2b_1c_1 + a_1b_2c_1).
\end{aligned}$$

Man sieht, beidesmal kommt das gleiche heraus.

Zur Distributivität:

$$\begin{aligned}
&(a_1, a_2)\,((b_1, b_2) + (c_1, c_2)) = (a_1, a_2)(b_1 + c_1, b_2 + c_2) \\
&= (a_1b_1 + a_1c_1 + a_2b_2 + a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1) \\
&= (a_1b_1 + a_2b_2, a_1b_2 + a_2b_1) + (a_1c_1 + a_2c_2, a_1c_2 + a_2c_1) \\
&= (a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2).
\end{aligned}$$

(Anstelle von Paaren $(a, b)$ kann man auch Matrizen $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ betrachten. Das oben definierte Produkt entspricht dem üblichen Matrizenprodukt. Setzt man nun voraus, dass man für Matrizen über Halbringen die Assoziativität des Produktes und die Distributivität weiß, kann man sich obige Verifikationen schenken.)

**16.35** Seien $a_1, a_2 \in \mathbb{N}$. Wenn $a_1 \geq a_2$ ist, gilt $a_1 = a_2 + r$ für ein $r \in \mathbb{N}$. Dann ist also

$$(a_1, a_2) = (a_2 + r, a_2) \sim (r, 0).$$

Ist hingegen $a_1 \leq a_2$, etwa $a_1 + s = a_2$, so gilt

$$(a_1, a_2) = (a_1, a_1 + s) \sim (0, s).$$

Jedes Element aus $\mathbb{Z}$ wird also gegeben durch ein Paar vo einer der Formen $(r, 0)$ oder $(0, s)$.
Die Abbildung

$$\begin{aligned}
i : \mathbb{N} &\longrightarrow \mathbb{Z} \\
r &\longmapsto \text{die durch } (r, 0) \text{ gegebene Zahl}
\end{aligned}$$

ist injektiv, da

$$(r, 0) \sim (r', 0) \Longleftrightarrow r = r'.$$

Ferner ist sie mit „+“ und „·“ verträglich (d.h. ein Halbringhomomorfismus). Für die Ordnungsrelationen gilt *Wir können und werden also* $\mathbb{N}$ *als Teilhalbring von* $\mathbb{Z}$ *auffassen.*
Wir bezeichnen mit $r$ die durch $(r, 0)$ gegebene Zahl. Die durch $(0, r)$ gegebene Zahl wird mit $-r$ bezeichnet. Da $(0, r)$ die zu $r$ additiv inverse Zahl gibt (16.32 d)), ist diese Schreibweise konsistent.
**16.36** Mit $-\mathbb{N}$ sei die Menge $\{-n \mid n \in \mathbb{N}\}$ bezeichnet. Dann gilt:

1. $\mathbb{N} \cup -\mathbb{N} = \mathbb{Z}$
2. $\mathbb{N} \cap -\mathbb{N} = \{0\}$
3. $m, n \in \mathbb{N} \Rightarrow m + n, mn \in \mathbb{N}$.

Wir definieren für ganze Zahlen $m, n$:

$$m \leq n :\iff n - m \in \mathbb{N}.$$

Wie im ‘Forster’ folgen dann die üblichen Regeln für Ungleichungen.

**16.37** In $\mathbb{Z}$ gilt – wie in $\mathbb{N}$ – die Kürzungsregel für die Multiplikation:

- (1) $\quad ab = ac$ und $a \neq 0 \quad \Longrightarrow \quad b = c$ .

Im Falle „$a > 0$“ folgt dies sofort aus der Monotonie – wie in 16.29. Falls aber $a < 0$ ist, ist $-a > 0$ und aus $ab = ac$ folgt $(-a)b = -(ab) = -(ac) = (-a)c$, also $b = c$.

In jedem Ring ist die Kürzungsregel äquivalent zur Nullteilerfreiheit, d.h. zu:

- (2) $\quad ab = 0 \quad \Longrightarrow \quad a = 0$ oder $b = 0$.

Denn (2) folgt aus (1), indem man $c = 0$ setzt, (1) aus (2), indem man $ab = ac$ zu $a(b - c) = 0$ umformt.

**16.38** Die Konstruktion von $\mathbb{Z}$ als angeordneter Ring ist damit abgeschlossen. Es bleibt noch die Eigenschaft $(M)$ aus (0.11) zu zeigen:

Sei $M \subset \mathbb{Z}$ durch $s$ nach unten beschränkt. Ist $s \geq 0$, so gilt $M \subset \mathbb{N}$. Andernfalls betrachten wir die Menge

$$M' := M - s = \{x - s \mid x \in M\}.$$

Da $s \leq x$ für alle $x \in M$ gilt, ist $M' \subset \mathbb{N}$.
Die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}, \quad x \longmapsto x - s$$

ist bijektiv und erhält die Anordnung. Es genügt also, den Satz für $M'$ anstelle von $M$ zu zeigen. Mit anderen Worten, wir dürfen $M \subset \mathbb{N}$ annehmen. Nach Voraussetzung ist $M$ nicht leer. Wir zeigen mit Induktion nach $n$ die folgende

**Behauptung:** *Wenn $n \in M$ ist, besitzt $M$ ein kleinstes Element.*

**Beweis:** Der Induktionsanfang $n = 0$ ist trivial.
Sei $n > 0$. Ist $n \leq x$ für alle $x \in M$, so ist $n$ das kleinste Element. Gibt es hingegen ein $m \in M$ mit $m < n$, so gilt die Behauptung nach Induktionsvoraussetzung. □

(Der Beweis ist nicht konstruktiv.)

**16.39** Wir haben oben – ab 16.30 – den Halbring $\mathbb{N}$ zum Ring $\mathbb{Z}$ erweitert. Bezüglich der Addition ist $\mathbb{Z}$ (wie jeder Ring eine Gruppe. Wir wollen jetzt den Ring $\mathbb{Z}$ zu einem Körper erweitern, den wir $\mathbb{Q}$ nennen werden. Es soll also $\mathbb{Q} - \{0\}$ bezüglich der Multiplikation eine Gruppe sein. Die Metode ist großenteils analog zu unserem obigen Vorgehen und so allgemein, dass man mit ihr jeden (kommutativen) nullteilerfreien Ring zu einem Körper erweitern kann.

**16.40** a) Auf $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ definiert man eine Äquivalenzrelation „$\sim$" durch

$$(m, n) \sim (m', n') \;:\Longleftrightarrow\; mn' = m'n.$$

(Das Paar $(m, n)$ wird später der Bruch $m/n$.)
Nur die Transitivität ist nicht völlig trivial. Aus $(m, n) \sim (m', n')$ und $(m', n') \sim (m'', n'')$ folgt

$$mn' = m'n \text{und} m'n'' = m''n', \text{also} mn'n'' = m'nn'' = m''nn'.$$

Indem man $n'$ wegkürzt (16.35), erhält man $mn'' = m''n$, d.h. $(m, n) \sim (m'', n'')$.

b) Wir definieren jetzt auf $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ eine Addition und eine Multiplikation durch:

$$(a, b) + (c, d) := (ad + bc, bd) \text{ und } (a, b) \cdot (c, d) := (ac, bd).$$

c) Die Verknüpfungen „ + “ und „ · “ sind mit der Äquivalenzrelation „ ∼ “ verträglich. Das heißt folgendes: Für $a,\ a',\ c,\ c' \in \mathbb{Z},\ \ b,\ b',\ d,\ d' \in \mathbb{Z} - \{0\}$ mit $(a, b) \sim (a', b'),\ (c, d) \sim (c', d')$ gilt:

$$(i) \quad (a, b) + (c, d) \sim (a', b') + (c', d')$$

$$(ii) \quad (a, b) \cdot (c, d) \sim (a', b') \cdot (c', d').$$

**Beweis:** : Für (i) ist zu zeigen:

$$(ad + bc,\ bd) \sim (a'b' + b'c',\ b'd'),\ \text{ d.h. } (ad + bc)b'd' = (a'd' + b'c')bd,$$

$$\text{d.h. } ab'dd' + cd'bb' = a'bdd' + c'dbb'.$$

Dies gilt aber, da nach Voraussetzung $ab' = a'b$ und $cd' = c'd$ ist.
Der Beweis von (ii) ist noch einfacher und sei dem Leser überlassen. □

**16.41** a) Wir abstrahieren jetzt bezüglich der Relation „∼“ und und nennen die entstehenden abstrakten Objekte rationale Zahlen und ihre Menge $\mathbb{Q}$.
Das abstrakte Objekt, das durch $(a, b)$ repräsentiert wird, wird mit $\frac{a}{b}$ oder $a/b$ bezeichnet. Es gilt:

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

b) Wir wollen jetzt zeigen, dass $\mathbb{Q}$ ein Körper ist, werden allerdings nicht alle Einzelheiten ausführen.

c) Die Kommutativität der Addition ist trivial.
Zu ihrer Assoziativität errechnet man:

$$\frac{a}{a'} + \left(\frac{b}{b'} + \frac{c}{c'}\right) = \frac{ab'c' + bc'a' + ca'b'}{a'b'c'}$$

Der Ausdruck auf der rechten Seite ändert sich nicht, wenn man die drei Paare $(a, a')$, $(b, b')$, $(c, c')$ beliebig vertauscht. So ist es klar oder zumindest kein Wunder, dass er auch gleich

$$\left(\frac{a}{a'} + \frac{b}{b'}\right) + \frac{c}{c'} \text{ist.}$$

d) Das neutrale Element bezüglich der Addition ist $\dfrac{0}{1}$. Natürlich ist $\dfrac{0}{1} = \dfrac{0}{n}$ für jedes $n \in \mathbb{Z} - \{0\}$.

Das additiv Inverse zu $\dfrac{m}{n}$ ist $\dfrac{-m}{n}$.

e) Die Kommutativität und Assoziativität der Multiplikation gelten trivialerweise, da diesmal die Multiplikation komponentenweise definiert ist. Vgl. 16.32 b).

f) Zur Distributivität:

$$\frac{a}{a'}\left(\frac{b}{b'} + \frac{c}{c'}\right) = \frac{abc' + acb'}{a'b'c'} = \frac{a}{a'} \cdot \frac{b}{b'} + \frac{a}{a'} \cdot \frac{c}{c'}.$$

g) Es gilt $\dfrac{m}{n} \neq \dfrac{0}{1}$ genau dann, wenn $m \neq 0$ ist. Für $m, n \in \mathbb{Z} - \{0\}$ ist $\dfrac{n}{m}$ zu $\dfrac{m}{n}$ multiplikativ invers.

h) Nach b) bis f) ist $\mathbb{Q}$ ein Ring und wegen g) sogar ein Körper.

i) Schließlich ist die Abbildung

$$f: \mathbb{Z} \longrightarrow \mathbb{Q},\ m \longmapsto \frac{m}{1}$$

mit Addition und Multiplikation verträglich, wie man unmittelbar sieht. (D.h. $f(m+n) = f(m) + f(n)$, $f(mn) = f(m)f(n)$ und $f(1) = 1/1$, die 1 in $\mathbb{Q}$.) Ferner ist $f$ offenbar injektiv. Wir fassen deshalb $\mathbb{Z}$ als Unterring von $\mathbb{Q}$ auf und schreiben $\dfrac{m}{1} = m$ für $m \in \mathbb{Z}$.

**16.42** Wir zeigen noch, dass man auf $\mathbb{Q}$ eine totale Anordnung angeben kann, die $\mathbb{Q}$ zu einem angeordneten Körper macht. Ein angeordneter Körper ist ein angeordneter Ring, der ein Körper ist. (S. 0.10.)

a) Sei $P := \left\{\frac{m}{n} | m \in \mathbb{N},\ n \in \mathbb{N}_1\right\}$. Man sieht sofort, dass Summe und Produkt zweier Elemente aus $P$ wieder in $P$ liegen; symbolisch:
(i) $P + P \subset P$, (ii) $P \cdot P \subset P$.

b) Sei $-P := \{-a \mid a \in P\}$. Dann gilt:

(iii) $P \cup -P = \mathbb{Q}$ und (iv) $P \cap -P = \{0\}$.

Denn wegen $\frac{m}{n} = \frac{-m}{-n}$ kann man jede rationale Zahl in der Form $\frac{m}{n}$ mit $n > 0$ schreiben. Für positive $n$ gilt:

$$\frac{m}{n} \in P \iff m \geq 0 \text{ und } \frac{m}{n} \in -P \iff m \leq 0.$$

Es folgt sofort (iii). Ist $a \in P \cap -P$, so lässt sich $a$ auf zweierlei Weise schreiben:

$$a = \frac{m}{n} = \frac{m'}{n'} \text{ mit } n, n' > 0,\ m \geq 0,\ m' \leq 0.$$

Dann ist aber $mn' = m'n = 0$, d.h. $m = m' = 0$.

Man nennt eine Teilmenge $P$ eines Körpers, die (i) bis (iv) erfüllt, einen Positivbereich. (Es gibt Körper, z.B. $\mathbb{Z}/p$ und $\mathbb{C}$, die keinen Positivbereich besitzen.)

c) Wir definieren: $a \leq b :\iff b - a \in P$.
Die in 0.8 und 0.10 aufgelisteten Eigenschaften eines angeordneten Ringes ergeben sich dann, wie folgt:

(iv) $\Longrightarrow$ 0.8 (i)

(i) $\Longrightarrow$ 0.8 (ii)

(iv) $\Longrightarrow$ 0.8 (iii)

(iii) $\Longrightarrow$ 0.8 (iv)

(i) $\Longrightarrow$ 0.10 (i)

(ii) $\longrightarrow$ 0.10 (ii)

**16.43 Bemerkungen:** a) Seien $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ und $n_1, n_2 > 0$. Dann gilt:

$$\frac{m_1}{m_1} \leq \frac{m_2}{n_2} \iff m_1 n_2 \leq m_2 n_1.$$

Man kann also die Anordnung von $\mathbb{Q}$ auch anders definieren als hier geschehen.

b) Für $m, n \in \mathbb{N}_1$ erhält man somit:

$$\frac{1}{n} \leq \frac{m}{n} \leq m.$$

c) Aus $0 < a$ folgt $0 < a^{-1}$. Sonst wäre $0 < -a^{-1}$, also $0 < (a^{-1})a = -1$ und deshalb $-1 \in P \cap -P$ im Widerspruch zu (iv) in 16.40.

d) Aus $0 < a \leq b$ folgt $1 \leq ba^{-1}$, also $b^{-1} \leq a^{-1}$. Ebenso folgt $b^{-1} < a^{-1}$ aus $0 < a < b$.

*In der folgenden Bemerkung und im nächsten Paragrafen wird der Satz 2.6 über die eindeutige Primfaktorzerlegung gebraucht.*

**16.44 Bemerkung:** Jede rationale Zahl ist *eindeutig* in der Form $\frac{m}{n}$ mit $m \in \mathbb{Z}$, $n \in \mathbb{N}_1$ und $\mathrm{ggt}(m, n) = 1$ darstellbar. Der Leser möge sich einen Beweis hierfür überlegen.

## AUFGABEN UND HINWEISE

**1)** Bitte machen Sie sich ein paar Gedanken über den Sinn und Nutzen negativer Zahlen. Die Gleichung

$$x^2 + 312 = 37x$$

hat die Lösungen 13 und 24, wie man leicht durch Rechnen in $\mathbb{N}$ nachprüft. Das bekannte Lösungsverfahren – mit quadratischer Ergänzung – benutzt jedoch mit Gewinn das Rechnen mit negativen Zahlen. An diesem Beispiel sieht man auch, wie richtig und wichtig es ist, das Produkt negativer Zahlen so zu definieren, dass z.B. $(-13)(-24) = 312 (> 0)$ ist.

**2)** Die Farey-Folge der Ordnung $n (\geq 1)$ ist die nach aufsteigender Größe geordnete Folge derjenigen rationalen Zahlen aus dem Intervall $[0, 1]$ , deren Nenner in der Standardform $\leq n$ ist. Z.B. ist die Farey-Folge der Ordnung 4 die Folge:

$$\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, frac34, \frac{1}{1}.$$

Für die Farey-Folge der Ordnung $n$ gilt:

a) Wenn $a_1/b_1$, $a_2/b_2$ aufeinanderfolgende Glieder dieser Folge in der Standardform sind, so ist

- 1. $a_2b_1 - a_1b_2 = 1$,
- 2. $b_1 + b_2 > n$,
- 3. $b_1 \neq b_2$ im Falle $n > 1$.

b) Wenn $a_1/b_1$, $a_2/b_2$, $a_3/b_3$ drei aufeinanderfolgende Glieder der Farey-Folge (in ihrer Standardform) sind, so ist $a_2/b_2 = (a_1 + a_3)/(b_1 + b_3)$. (Der letzte Bruch ist nicht notwendig gekürzt.)

Um a) und b) zu beweisen, sollten Sie zunächst c) bis e) zeigen:

c) Aus $a_1/b_1 < a_2/b_2$ folgt $a_1/b_1 < (a_1 + a_2)/(b_1 + b_2) < a_2/b_2$.

d) Wenn $a_2b_1 - a_1b_2 = 1$ ist, gilt auch

$$(a_1 + a_2)b_1 - a_1(b_1 + b_2) = 1 und a_2(b_1 + b_2) - (a_1 + a_2)b_2 = 1.$$

Sind $a_i, b_i \in \mathbb{Z}$, so folgt also insbesondere: Der Bruch $(a_1 + a_2)/(b_1 + b_2)$ ist gekürzt.

e) Aus $a_i, b_i, u, v \in \mathbb{Z},\ b_i, v > 0,\ a_2 b_1 - a_1 b_2 = 1$ und $a_1/b_1 < u/v < a_2/b_2$ folgt $v \geq b_1 + b_2$.

Anschließend konstruieren Sie eine Folge von Brüchen auf folgende Weise: Beginnen Sie mit $0/1,\ 1/1$. Ist $n > 1$, fügen Sie $1/2 = (0+1)/(1+1)$ ein, usw.: Solange es in Ihrer Folge noch zwei aufeinanderfolgende Glieder $a_1/b_1,\ a_2/b_2$ mit $b_1 + b_2 \leq n$ gibt, fügen Sie $(a_1 + a_2)/(b_1 + b_2)$ gemäß c) zwischen ihnen ein.
Für die am Ende erhaltene Folge ist a) 2. offenbar erfüllt, und a) 1. folgt aus d). Aus a) 1. kann man leicht b) folgern. Ferner folgt a) 3. aus den Ungleichungen $a/b < a/(b-1) < (a+1)/b$ für $a + 1 < b$. Schließlich sieht man mit e), dass man die Farey-Folge der Ordnung $n$ konstruiert hat.

**3)** Seien $n$, $p \in \mathbb{N}_1$ derart, dass $p > 2n^2$ und $p$ zu $n!$ teilerfremd (etwa eine Primzahl) ist. Sei

$$M := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ -n \leq a \leq n,\ 1 \leq b \leq n \right\}.$$

Zeigen Sie:

a) Durch

$$a/b \longmapsto (a \bmod p)(b \bmod p)^{-1}$$

wird eine injektive Abbildung

$$f : M \longrightarrow \mathbb{Z}/p$$

definiert.

b) Ist „$\circ$“ eine der Verknüpfungen „$+,\ -,\ \cdot,\ :$“ und $x,\ y,\ x \circ y \in M$, so gilt $f(x \circ y) = f(x) \circ f(y)$.

(Sei $S$ die Menge der zu $p$ teilerfremden ganzen Zahlen. Man kann leicht einen Homomorfismus $S^{-1}\mathbb{Z} \to \mathbb{Z}/p$ angeben. S. 2.A12.)

**4)** (Ägyptische Brüche) Die alten Ägypter neigten dazu, rationale Zahlen als Summen von Stammbrüchen mit verschiedenen Nennern darzustellen. Zeigen Sie dazu: Sei $r$ eine rationale Zahl mit $0 < r < 1$. Dann ist $r$ als Summe von Stammbrüchen — d.h. solchen der Form $1/n$ mit $n \in \mathbb{N}_1$ — mit verschiedenen Nennern darstellbar.

(Ist $1/n_1$ der größte Stammbruch $\leq r$, so besitzt $r - 1/n_1$ einen kleineren Zähler als $r$ in der Standardform.)

# § 17

# Reelle und $p$–adische Zahlen

**17.1 Vorbemerkungen:** a) Die rationalen Zahlen wurden aus den ganzen Zahlen gewonnen, indem man für jedes Paar ganzer Zahlen $(a, b)$ $(b \neq 0)$ den fehlenden Quotienten von $a$ durch $b$ schlicht durch das Paar $(a, b)$ ersetzte. Dabei muss man allerdings zwei Paare $(a, b)$ und $(a', b')$ als die gleiche rationale Zahl betrachten, wenn sie „vernünftigerweise“ denselben Quotienten haben sollten.
Bei der Konstruktion reeller Zahlen geht man analog vor: Den eventuell fehlenden Limes einer Folge $(a_\nu)_{\nu\in\mathbb{N}}$ rationaler Zahlen, die „vernünftigerweise“ einen Limes haben sollte – d.h. eine sogenannte Cauchy-Folge ist – ersetzt man durch diese Folge selbst. Man muss dann zwei solche Folgen als dieselbe reelle Zahl betrachten, wenn sie „vernünftigerweise“ den gleichen Limes haben sollten, d.h. wenn ihre Differenz eine Nullfolge ist.

b) Was ist überhaupt eine Folge $(a_\nu)_{\nu\in\mathbb{N}}$ rationaler Zahlen? Formal gesehen ist sie eine Abbildung $a :\ \mathbb{N} \longrightarrow \mathbb{Q}$, wobei $a_\nu$ für $a(\nu)$ geschrieben wird. Wir schreiben auch kürzer $(a_\nu)_\nu$ statt $(a_\nu)_{\nu\in\mathbb{N}}$. (Im Fall von mehrfachen Indizes ist die Angabe des „Lauf“-Indexes außerhalb der Klammer zumindest nützlich, wenn nicht notwendig.)

c) Es ergibt sich eine Grundlagenschwierigkeit. (Der hieran uninteressierte Leser fahre mit d) fort.) Die Menge „aller“ Folgen ist „indefinit“, d.h. nicht konstruktiv fassbar. Jede Folge, mit der man konkret etwas anfangen will, muss durch eine Definition (die sich mit endlich vielen Symbolen schreiben lässt) gegeben werden, die für jedes $n$ das Folgenglied $a_n$ festlegt. Es gibt aber nur abzählbar viele Möglichkeiten solcher Definitionen. (Es sei denn,

man hätte ein überabzählbares Alfabet, welches sicher für den einen oder anderen etwas mühsam zu lernen wäre.) Trotzdem gewinnt man durch das Cantorsche Diagonalverfahren zu abzählbar unendlich vielen Folgen rationaler Zahlen sofort eine von all diesen verschiedene Folge. (Nämlich so: Für $\mu \in \mathbb{N}$ sei die $\mu$-te Folge $(a_{\mu\nu})_\nu$. Dann ist die Folge $(a_{\mu\mu} + 1)_\mu$ an der $\mu$-ten Stelle von der $\mu$-ten Folge verschieden, also von jeder der Folgen $(a_{\mu\nu})_\nu$.) Konstruktiv erfassbar sind jeweils nur abzählbar viele Folgen auf einmal. Aber man kann die Konstruktion immer weiter treiben – nur ist die Art und Weise, wie man das tut, nicht festgelegt.
Trotz der Indefinitheit der Menge aller (Cauchy-)Folgen kann man Sätze beweisen, die für alle Cauchy-Folgen oder alle reellen Zahlen stimmen, auf welcher Konstruktionsstufe diese auch definiert sind. Deshalb sind die folgenden Ausführungen in der Sprache der üblichen Mengenlehre gehalten. Der an Grundlagenfragen interessierte Leser möge [*Lorenzen 1965*] §4 zu Rate ziehen, ferner §7 jenes Buches, wo die konstruktive Interpretation unseres Theorems 17.25 zu finden ist.

d) Die Begriffe „Konvergenz“, „Limes“, „Cauchy-Folge“ beruhen auf dem Begriff des Absolutbetrages. Neben diesem „anschaulichen“ Betrag gibt es auf $\mathbb{Q}$ noch weitere, zahlentheoretisch definierte Beträge – und zwar für jede Primzahl (im wesentlichen) einen. Bezüglich dieser sogenannten $p$-adischen Beträge kann man analog zur Konstruktion des Körpers $\mathbb{R}$ der reellen Zahlen für jede Primzahl $p$ den Körper $\mathbb{Q}_p$ der sogenannten $p$-adischen Zahlen konstruieren. Hier wird die Konstruktion von $\mathbb{R}$ und allen $\mathbb{Q}_p$ auf einen Schlag durchgeführt. Wer sich dadurch verwirrt fühlt, mag sich beim ersten Lesen auf den bekannten Absolutbetrag und die reellen Zahlen konzentrieren.

e) Dieser Paragraf ist weniger vom Rest des Buches unabhängig als der vorangegangene. Zum Beispiel benutzen wir den Begriff des Restklassenringes aus §6 Die Einführung der $p$-adischen Beträge benötigt die Eindeutigkeit der Primfaktorzerlegung. Für die Ausführungen ab 17.26, welche nur die $p$-adischen Zahlen betreffen, braucht man einige elementaralgebraische Kenntnisse, nämlich 6.29 und §11.

**17.2** Für rationale Zahlen $a$ definiert man bekanntlich den Absolutbetrag $|a|$ durch

$$|a| := \max\{a, -a\}.$$

Für diesen gilt:

(i) $|a| \geq 0$,

(ii) $|a| = 0 \iff a = 0$,

(iii) $|ab| = |a| \cdot |b|$,

(iv) $|a+b| \leq |a| + |b|$.

Diese Eigenschaften sind leicht zu zeigen.

**17.3** Denselben Gesetzen genügen auch andere sogenannte Beträge. Sei nämlich $p$ eine Primzahl. Für $m, n \in \mathbb{Z} - \{0\}$ definieren wir:

$$v_p(m/n) := v_p(m) - v_p(n),$$

wobei $v_p$ auf $\mathbb{Z} - \{0\}$ wie in 2.11 definiert ist. (D.h. es ist $v_p(p^r \cdot m/n) = r$, wenn $r \in \mathbb{Z}$ und $p \nmid mn$ gilt.)
Setze noch $v_p(0) := \infty$. Dann gilt:

(i) $v_p(a) \in \mathbb{Z} \cup \{\infty\}$ für alle $a \in \mathbb{Q}$,

(ii) $v_p(a) = \infty \iff a = 0$,

(iii) $v_p(ab) = v_p(a) + v_p(b)$,

(iv) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$.

(Dabei ist $m + n$ und $\min\{m, n\}$ für $m, n \in \mathbb{Z} \cup \{\infty\}$ sinnvoll zu definieren. Wie?)
Nur (iv) ist nicht völlig trivial, folgt aber leicht, nachdem man es zunächst für $a, b \in \mathbb{Z}$ gezeigt hat.

**Definition: 17.4** *Der $p$-adische Betrag $|a|_p$ einer rationalen Zahl $a$ ist definiert durch:*

$$|0|_p = 0, \quad |a|_p := p^{-v_p(a)} \text{ für } a \neq 0.$$

**17.5** a) Es gilt also z.B. $|1023|_2 = 1$, $|1024|_2 = 1/1024$, $|1023/1024|_2 = 1024$.
b) Verschiedene ganze Zahlen können „$p$–adisch beliebig nahe beieinander liegen“, d.h. der $p$–adische Betrag ihrer Differenz kann beliebig klein sein, nämlich dann, wenn sie modulo einer genügend hohen Potenz von $p$ zueinander kongruent sind. Dies ist der zahlentheoretische Sinn des $p$–adischen Betrages.
c) Aus den Eigenschaften (i) bis (iv) von $v_p$ folgt für $|\ |_p$ :

(i) $|a|_p \in \mathbb{Q}$, $|a|_p \geq 0$;

(ii) $|a|_p = 0 \iff a = 0$;

(iii) $|ab|_p = |a|_p \cdot |b|_p$;

(iv') $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

Aus (iv') folgt a fortiori:

(iv) $|a + b|_p \leq |a|_p + |b|_p$.

Es gelten also dieselben grundlegenden Gesetze wie für den Absolutbetrag. Aus (iii) folgt übrigens $|-1|_p = 1$ und somit auch $|-a|_p = |a|_p$. Wie?

**17.6** Es würde sich nichts wesentliches ändern, wenn man (für $a \neq 0$) definierte:

$$|a|_p := \rho^{v(p)},$$

wo $\rho$ eine beliebige rationale Zahl mit $0 < \rho < 1$ ist. (Für $\rho > 1$ wäre (iv) nicht erfüllt. Was ergäbe sich für $\rho = 1$ ?)
Die in 17.3 gewählte Definition hat jedoch den Vorteil, dass für sie die nützliche Formel:

$$|a| \cdot \prod_{p \in \mathbb{P}} |a|_p \ = \ 1$$

für alle $a \in \mathbb{Q}^*$ gilt. (In dem Produkt sind nur endlich viele Faktoren von 1 verschieden. Der Beweis der Formel ist trivial.)

**17.7** Sei im Folgenden $|\ |$ einer der oben definierten Beträge, also der Absolutbetrag, den wir jetzt mit „$|\ |_\infty$“ bezeichnen wollen, oder einer der

$p$-adischen Beträge $|\ |_p$, wo $p$ eine Primzahl ist.

**Definitionen: 17.8** *Sei* $(a_\nu)_\nu = (a_\nu)_{\nu\in\mathbb{N}}$ *eine Folge rationaler Zahlen.*
*a) Man sagt, die Folge* $(a_\nu)_\nu$ *konvergiert (bezüglich* $|\ |$*) gegen* $a$*, oder, sie hat den Grenzwert (Limes)* $a$*, und schreibt* $\lim_{\nu\to\infty} a_\nu = a$*, wenn zu jeder rationalen Zahl* $\varepsilon > 0$ *eine natürliche Zahl* $n$ *existiert, so dass* $|a_\nu - a| < \varepsilon$ *für alle* $\nu \geq n$ *gilt.*
*b) Ist* $\lim_{\nu\to\infty} a_\nu = 0$ *(bezüglich* $|\ |$*), so heißt* $(a_\nu)_\nu$ *eine Nullfolge (bezüglich* $|\ |$*).*
*c) Die Folge* $(a_\nu)_\nu$ *heißt (bezüglich* $|\ |$*) eine Cauchy-Folge, wenn zu jeder rationalen Zahl* $\varepsilon > 0$ *eine natürliche Zahl* $n$ *existiert, so dass* $|a_\nu - a_\mu| < \varepsilon$ *für alle* $\nu, \mu \geq n$ *gilt.*

**17.9 Bemerkungen:** a) Natürlich hängen die Definitionen von dem gewählten Betrag $|\ |$ ab: Z.B. ist die Folge $(1/(\nu+1))_\nu$ eine Nullfolge bezüglich $|\ |_\infty$. Ist nämlich $\varepsilon = m/n > 0$ also $m, n \in \mathbb{N}_1$, so gilt $|1/\nu|_\infty = 1/\nu < m/n$ für $\nu > n$. Bezüglich $|\ |_p$ mit $p \in \mathbb{P}$ hat die Folge $(1/(\nu+1))_\nu$ keinen Grenzwert, da sie offenbar unbeschränkt (Definition?) ist.
b) Eine Folge kann höchstens einen Grenzwert haben. Denn der Beweis zu [*Forster*] §4 Satz 2 nutzt nur die formalen Eigenschaften (i) bis (iv) und gilt deshalb für jeden Betrag.

**17.10** Man sieht leicht, dass jede konvergente Folge auch eine Cauchy-Folge ist. (Vgl. [*Forster*] §5 Satz 1.) Die Umkehrung dieses Satzes gilt in $\mathbb{Q}$ für keinen der Beträge $|\ |_p$, $p \in \mathbb{P} \cup \{\infty\}$. Unser Ziel ist es, $\mathbb{Q}$ samt $|\ |$ zu einem solchen Körper mit Betrag zu erweitern, dass die Umkehrung gültig wird.

**17.11** a) Die Menge aller Folgen rationaler Zahlen wird zu einem Ring, wenn man Addition und Multiplikation „komponentenweise" definiert, d.h.:

$$(a_\nu)_\nu + (b_\nu)_\nu := (a_\nu + b_\nu)_\nu \text{ und } (a_\nu)_\nu \cdot (b_\nu)_\nu := (a_\nu b_\nu)_\nu.$$

b) Sind $(a_\nu)_\nu$ und $(b_\nu)_\nu$ konvergente Folgen mit $\lim_{\nu\to\infty} a_\nu = a$ und $\lim_{\nu\to\infty} b_\nu = b$, so sind auch die Folgen $(a_\nu + b_\nu)_\nu$ und $(a_\nu b_\nu)_\nu$ konvergent, und es gilt:

$$\lim_{\nu\to\infty}(a_\nu + b_\nu) = a + b \text{ und } \lim_{\nu\to\infty}(a_\nu b_\nu) = ab.$$

**Lemma: 17.12** *a) Cauchy-Folgen sind beschränkt, d.h. zu jeder Cauchy-Folge $(a_\nu)_\nu$ gibt es ein $s \in \mathbb{N}$ mit $|a_\nu| \leq s$ für alle $\nu$.*

*b) Ist $(a_\nu)_\nu$ eine Cauchy-Folge, aber keine Nullfolge, so gibt es eine rationale Zahl $\delta > 0$ und ein $n \in \mathbb{N}$, so dass $|a_\nu| \geq \delta$ für alle $\nu \geq n$ ist.*

**Beweis:** a) Nach Definition ($\varepsilon = 1$) gibt es ein $n \in \mathbb{N}$, so dass $|a_\nu - a_\mu| < 1$ für alle $\nu, \mu \geq n$ ist. Für $s = \max\left\{|a_\nu| \;\middle|\; \nu \leq n\right\} + 1$ gilt $|a_\nu| \leq s - 1 < s$, wenn $\nu \leq n$, und $|a_\nu| \leq |a_n| + |a_\nu - a_n| \leq (s-1) + 1 = s$, wenn $\nu > n$ ist.
b) Wir zeigen: Wenn es kein solches $\delta$ gäbe, wäre $(a_\nu)_\nu$ eine Nullfolge – im Widerspruch zur Voraussetzung.
Sei nämlich $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$. Dann gibt es ein $n \in \mathbb{N}$ mit $|a_\nu - a_\mu| < \varepsilon/2$ für alle $\nu, \mu \geq n$. Es gibt ferner ein $\mu \geq n$ mit $|a_\mu| < \varepsilon/2$; sonst würde $\delta = \varepsilon/2$ die Aussage erfüllen. Für alle $\nu \geq n$ ist dann
$|a_\nu| \leq |a_\mu| + |a_\nu - a_\mu| < 2 \cdot \varepsilon/2$. □

**Satz: 17.13** *a) Die Cauchy-Folgen bilden einen Unterring $\mathcal{C}$ des Ringes aller Folgen rationaler Zahlen.*

*b) Die Nullfolgen bilden ein Ideal $\mathcal{N}$ von $\mathcal{C}$.*

*c) Der Restklassenring $\mathcal{C}/\mathcal{N}$ ist ein Körper.*

**Beweis:** a) Konstante Folgen sind Cauchy-Folgen, insbesondere die Folgen $(a_\nu)_\nu$ mit $a_\nu = 0$, bzw. $= 1$ für alle $\nu$. Diese Folgen sind die neutralen Elemente des Ringes aller Folgen. Mit $(a_\nu)_\nu$ ist auch $-(a_\nu)_\nu = (-a_\nu)_\nu$ offenbar eine Cauchy-Folge.
Man sieht auch ganz leicht, dass die Summe zweier Cauchy-Folgen wieder eine solche ist.
Wir haben noch das gleiche für das Produkt von Cauchy-Folgen $(a_\nu)_\nu$ und $(b_\nu)_\nu$ zu zeigen. (Hierbei wird, wie so oft, die Identität $ab - a'b' = a(b - b') + (a - a')b'$ benutzt.)
Sei $s \in \mathbb{N}$ eine obere Schranke für die $|a_\nu|$, $\nu \in \mathbb{N}$, und $t$ eine solche für die $|b_\nu|$. Solche Schranken existieren nach 17.11 a). Zu $\varepsilon > 0$ existieren dann $m, n \in \mathbb{N}$, so dass $|a_\nu - a_\mu| < \varepsilon/2t$ für $\nu, \mu \geq m$ und $|b_\nu - b_\mu| < \varepsilon/2s$ für $\nu, \mu \geq n$ gilt. Für $\nu, \mu \geq \max\{m, n\}$ ist dann

$$|a_\nu b_\nu - a_\mu b_\mu| \leq |a_\nu| \cdot |b_\nu - b_\mu| + |a_\nu - a_\mu| \cdot |b_\mu| \;<\; s \cdot \varepsilon/2s + t \cdot \varepsilon/2t \;=\; \varepsilon.$$

b) Die konstante Folge $(0)_\nu$ gehört offenbar zu $\mathcal{N}$. Ebenso ist das additiv Inverse einer Nullfolge eine solche. Nach 17.10 b) gilt dies auch für die Summe zweier Nullfolgen. Wir haben noch zu zeigen: Ist $(a_\nu)_\nu$ eine Cauchy-Folge und $(b_\nu)_\nu$ eine Nullfolge, so ist $(a_\nu b_\nu)_\nu$ eine Nullfolge. Mithilfe der Beschränktheit von $(a_\nu)_\nu$ wird der Leser das alleine schaffen.

c) Sei $(a_\nu)_\nu \in \mathcal{C} - \mathcal{N}$. Es genügt, ein Inverses modulo $\mathcal{N}$, d.h. eine Cauchy-Folge $(b_\nu)_\nu$ zu finden, derart dass die Folge $(a_\nu b_\nu)_\nu$ modulo $\mathcal{N}$ zur konstanten Folge $(1)_\nu$ kongruent ist. Die gesuchte Folge wird durch

$$b_\nu \;=\; \begin{cases} 0 & \text{im Falle } a_\nu = 0 \\ a_\nu^{-1} & \text{sonst} \end{cases}$$

definiert.
Zunächst ist nämlich $a_\nu = 0$ nur für endlich viele $\nu$ nach 17.11 b). D.h. es ist $a_\nu b_\nu = 1$ bis auf endlich viele $\nu$. Deshalb ist $(a_\nu b_\nu - 1)_\nu$ eine Nullfolge, also

$$(a_\nu)_\nu \cdot (b_\nu)_\nu \;\equiv\; (1)_\nu \pmod{\mathcal{N}}.$$

Es bleibt zu zeigen, dass $(b_\nu)_\nu$ eine Cauchy-Folge ist. Sei also $\varepsilon > 0$. Es gibt ein $n \in \mathbb{N}$ und ein $\delta > 0$, so dass $|a_\nu| \geq \delta$, also auch $|a_\nu^{-1}| = |a_\nu|^{-1} \leq \delta^{-1}$ für alle $\nu \geq n$ ist. (S. 16.41 d))
Da $(a_\nu)_\nu$ eine Cauchy-Folge ist, gibt es ein $m \in \mathbb{N}$ mit $|a_\mu - a_\nu| < \varepsilon\delta^2$ für alle $\mu, \nu \geq m$. Für $\mu, \nu \geq \max\{n, m\}$ erhält man dann

$$|b_\nu - b_\mu| \;=\; |a_\nu^{-1} - a_\mu^{-1}| \;=\; |a_\nu^{-1}| \cdot |a_\mu^{-1}| \cdot |a_\mu - a_\nu| \;<\; \delta^{-2}\varepsilon\delta^2 \;=\; \varepsilon.$$

□

**Definition: 17.14** *Sei $|\;| = |\;|_p$, wo $p$ eine Primzahl oder $\infty$ ist. Wir schreiben dann $\mathbb{Q}_p := \mathcal{C}/\mathcal{N}$. Der Körper $\mathbb{Q}_\infty$ wird auch mit $\mathbb{R}$ bezeichnet. Die Elemente von $\mathbb{R} = \mathbb{Q}_\infty$ heißen reelle Zahlen. Die von $\mathbb{Q}_p$ mit einer Primzahl $p$ heißen $p$-adische Zahlen.*

**17.15** Indem man jeder rationalen Zahl die entsprechende konstante Folge zuordnet, erhält man für jedes $p \in \mathbb{P} \cup \{\infty\}$ einen injektiven Homomorfismus

$$\mathbb{Q} \longrightarrow \mathbb{Q}_p.$$

Wir fassen somit $\mathbb{Q}$ als Teilkörper von $\mathbb{Q}_p$ auf. (Zwischen den verschiedenen $\mathbb{Q}_p$ gibt es keine kanonischen Homomorfismen.)

**17.16** Was ist noch zu tun? Wir müssen für jedes $p \in \mathbb{P} \cup \{\infty\}$ den Betrag $|\ |_p$ auf $\mathbb{Q}_p$ fortsetzen und zeigen, dass bezüglich des fortgesetzten Betrages Cauchy-Folgen in $\mathbb{Q}_p$ konvergieren. Ferner wollen wir die Anordnung von $\mathbb{Q}$ auf $\mathbb{R} = \mathbb{Q}_\infty$ fortsetzen, so dass $\mathbb{R}$ zu einem angeordneten Körper wird, d.h. dass die in 16.40 oder 0.8, 0.10 genannten Bedingungen erfüllt sind. Dies ist für $\mathbb{Q}_p$ mit $p \in \mathbb{P}$ nicht möglich.

**17.17 Lemma:** *a) Für alle $p \in \mathbb{P} \cup \{\infty\}$ und alle rationalen Zahlen $a$, $b$ gilt:*

$$\Big| |a|_p - |b|_p \Big|_\infty \leq |a-b|_p.$$

*b) Ist also $(a_\nu)_\nu$ eine Cauchy-Folge in $\mathbb{Q}$ bezüglich $|\ |_p$, so ist $(|a_\nu|_p)_\nu$ eine solche bezüglich $|\ |_\infty$.*

*c) Seien $(a_\nu)_\nu$, $(b_\nu)_\nu$ Cauchy-Folgen bezüglich $|\ |_p$ und ist $(a_\nu - b_\nu)_\nu$ eine Nullfolge bezüglich $|\ |_p$, so ist $(|a_\nu|_p - |b_\nu|_p)_\nu$ eine Nullfolge bezüglich $|\ |_\infty$.*

*d) Für $p \neq \infty$ gilt sogar: Wenn $(a_\nu)_\nu$ eine Cauchyfolge, aber keine Nullfolge bezüglich $|\ |_p$ ist, so ist die Folge $(|a_\nu|_p)_\nu$ im wesentlichen konstant; d.h. es gibt ein $n \in \mathbb{N}$, so dass $|a_\nu|_p = |a_\mu|_p$ für alle $\nu$, $\mu \geq n$ gilt.*

**Beweis:** a) Aus $|a|_p = |a-b+b|_p \leq |a-b|_p + |b|_p$ erhält man

$$|a|_p - |b|_p \leq |a-b|_p.$$

Ebenso gilt

$$|b|_p - |a|_p \leq |b-a|_p = |a-b|_p.$$

Es folgen a) und damit auch b), c).

d) Die möglichen Werte des $p$-adischen Betrages sind 0 oder von der Form $p^r$ mit $r \in \mathbb{Z}$. Da $(a_\nu)_\nu$ keine Nullfolge ist, gibt es nach 17.12 b) ein $\delta \geq 0$ und ein $N \in \mathbb{N}$ mit $|a_\nu|_p \geq \delta$ für alle $\nu \geq N$.

*Behauptung:* Für $\nu, \mu \geq N$ ist $\Big| |a_\nu|_p - |a_\mu|_p \Big|_\infty \geq \delta$ oder $|a_\nu|_p = |a_\mu|_p$.

Denn sei $|a_\nu|_p \neq |a_\mu|_p$, also etwa $|a_\nu|_p = p^r \geq \delta,\ |a_\mu|_p = p^{r+i}$ mit $r, i \in \mathbb{Z},\ i > 0$. Dann ist

$$\Big| |a_\nu|_p - |a_\mu|_p \Big|_\infty = p^r(p^i - 1) \geq \delta,$$

da $p^i - 1 \geq 1$ ist. Es folgt die Behauptung.

Da nun $(|a_\nu|_p)_\nu$ eine Cauchy-Folge bezüglich $|\ |_\infty$ ist, gibt es ein $M \in \mathbb{N}$, so dass $\Big||a_\nu|_p - |a_\mu|_p\Big|_\infty < \delta$ für alle $\nu, \mu \geq M$ gilt. Für $\nu, \mu \geq \max\{N, M\}$ muss dann $|a_\nu|_p = |a_\mu|_p$ sein. □

**Definition: 17.18** *Sei $p \in \mathbb{P} \cup \{\infty\}$. Auf $\mathbb{Q}_p$ wird nun ein Betrag, ebenfalls $|\ |_p$ genannt, mit Werten in $\mathbb{R} = \mathbb{Q}_\infty$ wie folgt definiert. Sei $\alpha \in \mathbb{Q}_p$ gegeben durch die Cauchy-Folge rationaler Zahlen $(a_\nu)_\nu$. Dann sei $|\alpha|_p$ diejenige* reelle *Zahl, welche durch die Folge $(|a_\nu|_p)_\nu$ gegeben ist, die ja nach 17.17 b) eine Cauchy-Folge bezüglich $|\ |_\infty$ ist.*

**Bemerkungen: 17.19** a) Der oben genannten Betrag auf $\mathbb{Q}_p$ ist wegen 17.17 c) wohldefiniert.

b) Ist $p \in \mathbb{P}$, so sind wegen 17.17 d) die Betragswerte $|\alpha|_p$ für $\alpha \in \mathbb{Q}_p$ weiterhin rationale Zahlen, genauer Elemente der Menge $\{0\} \cup p^{\mathbb{Z}} = \{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$. In diesem Falle ($p \neq \infty$) kann man die Gesetze (i), (ii), (iii), (iv') und (iv) aus 17.5 für $|\ |_p$ auf $\mathbb{Q}_p$ leicht nachweisen. Dies sei dem Leser überlassen.

c) Im Falle $p = \infty$, d.h. $\mathbb{Q}_p = \mathbb{R}$ treten irrationale Betragswerte auf. Z.B. ist die reelle Zahl $e$ durch die Cauchy-Folge $(a_\nu)_\nu$ mit $a_\nu = \sum_{k=0}^{\nu} 1/k!$ gegeben. Wegen $a_\nu > 0$ sieht man sofort, dass $|e| = e$ gilt. Und $e$ ist nach 2.A22 irrational. Wir müssen zunächst eine Anordnung auf $\mathbb{R}$ definieren, um die Gesetze (i) und (iv) aus 17.2 überhaupt formulieren zu können.

**Lemma: 17.20** *Sei $(a_\nu)_\nu$ eine Cauchy-Folge rationaler Zahlen bezüglich $|\ |_\infty$, aber keine Nullfolge. Dann gibt es ein $n \in \mathbb{N}$ und ein rationales $\delta > 0$, so dass entweder $a_\nu \geq \delta$ für alle $\nu \geq n$ oder $a_\nu \leq -\delta$ für alle $\nu \geq n$ gilt.*

**Beweis:** Nach 17.12 b) gibt es ein $N \in \mathbb{N}$ und ein rationales $\delta > 0$, so dass $|a_\nu|_\infty \geq \delta$ für alle $\nu \geq N$ gilt. Da $(a_\nu)_\nu$ eine Cauchy-Folge ist, gibt es ein $M \in \mathbb{N}$ mit $|a_\nu - a_\mu|_\infty < \delta$ für alle $\nu, \mu \geq M$. Wäre nun $a_\nu \leq -\delta$, $a_\mu \geq \delta$ für zwei $\nu, \mu \geq \max\{N, M\}$, so wäre $|a_\nu - a_\mu|_\infty \geq 2\delta$. Widerspruch. □

**17.21 Bemerkungen und Definition:** a) Es gibt also drei Sorten von Cauchy-Folgen rationaler Zahlen bezüglich $|\ |_\infty$:

1. solche, für die es ein rationales $\delta > 0$ gibt, so dass $a_\nu \geq \delta$ für große $\nu$ gilt,
2. Nullfolgen,

3. solche, für die es ein rationales $\delta > 0$ gibt, so dass $a_\nu \leq -\delta$ für große $\nu$ gilt.

b) Seien $(a_\nu)_\nu$, $(b_\nu)_\nu$ Cauchy-Folgen (bezüglich $|\ |_\infty$), die modulo $\mathcal{N}$ kongruent sind, d.h. dass $(a_\nu - b_\nu)_\nu$ eine Nullfolge ist, so gilt:
Gehört $(a_\nu)_\nu$ zur 1., bzw. 2., bzw. 3. Sorte, dann ist dies auch für $(b_\nu)_\mu$ so.
Denn sei zum Beispiel $(a_\nu)_\nu$ von der 3. Sorte. Dann gibt es ein $\delta > 0$, so dass $a_\nu \leq -\delta$ für genügend große $\nu$ ist. Da $|a_\nu - b_\nu| < -\delta/2$ für große $\nu$ ist, folgt $b_\nu \leq -\delta/2$, falls nur $\nu$ groß genug ist. Dass mit $(a_\nu)_\nu$ auch $(b_\nu)_\nu$ eine Nullfolge ist, ist uns schon aus 17.11 a) bekannt.

c) Man kann jetzt für $\mathbb{R}$ – wie in 16.40 für $\mathbb{Q}$ – einen Positivbereich $P'$ definieren: $P'$ sei die Menge derjenigen reellen Zahlen, die durch eine Folge der 1. oder 2. Sorte gegeben wird. Eine reelle Zahl gehört genau dann zu $P'$, wennn man sie durch eine Folge rationaler Zahlen darstellen kann, deren sämtliche Glieder $\geq 0$ sind. (Beweis?)

d) Der Leser möge die Eigenschaften (i) bis (iv) aus 16.40 für $P'$ bezüglich $\mathbb{R}$ beweisen. Wie man dort sieht, wird somit $\mathbb{R}$ durch die Definition:

$$\alpha \leq \beta :\Longleftrightarrow \beta - \alpha \in P'$$

ein angeordneter Körper.

e) Man sieht nun leicht, dass die Beziehung

$$|\alpha|_\infty = \max\{\alpha, -\alpha\}$$

auch in $\mathbb{R}$ gilt.
Sei etwa $\alpha < 0$, und $\alpha$ durch die Cauchy-Folge $(a_\nu)_\nu$ gegeben. Dann unterscheiden sich die Folgen $(-a_\nu)_\nu$ und $(|a_\nu|)_\nu$ nur an endlich vielen Stellen voneinander, sind also modulo $\mathcal{N}$ zueinander kongruent. Deshalb gilt $-\alpha = |\alpha|$ im Falle $\alpha < 0$.

f) Man kann dann – etwa mittels e) – die Eigenschaften (i) bis (iv) aus 17.2 für $|\ |_\infty$ auf $\mathbb{R}$ nachweisen.

**17.22 Lemma:** *Zu jeder reellen Zahl $\varepsilon > 0$ gibt es eine rationale Zahl $\delta$ mit $\varepsilon \geq \delta > 0$.*

**Beweis:** Sei $\varepsilon$ durch die Cauchy-Folge $(e_\nu)_\nu$ gegeben. Dann gibt es ein rationales $\delta > 0$ und ein $N \in \mathbb{N}$, so dass $e_\nu \geq \delta$ für $\nu \geq N$ ist. Bis auf endlich viele $\nu$ ist $e_\nu - \delta \geq 0$. Also ist $\varepsilon - \delta \in P'$, d.h. $\varepsilon \geq \delta$. □

**Korollar: 17.23 (Archimedisches Axiom)** *a) Zu jeder reellen Zahl $\alpha$ gibt es ein $n \in \mathbb{N}$ mit $|\alpha|_\infty \leq n$.*
*b) Zu $\alpha, \beta \in \mathbb{R}$ mit $0 < \alpha < \beta$ gibt es ein $n \in \mathbb{N}$ mit $n\alpha > \beta$.*

**Beweis:** a) Ist $\alpha \neq 0$, so gibt es nach 17.22 eine rationale Zahl $\delta = m/n$, $m, n \in \mathbb{N}_1$ mit $\delta \leq |\alpha|^{-1}$. Dann folgt $|\alpha| \leq \delta^{-1} = n/m$ wie in 16.41 c). Dann ist erst recht $|\alpha| \leq n$.

b) Wende a) auf $\beta/\alpha$ anstelle von $\alpha$ an. □

**Satz: 17.24** *Sei $p \in \mathbb{P} \cup \{\infty\}$. Das Element $\alpha \in \mathbb{Q}_p$ sei durch die Cauchy-Folge rationaler Zahlen $(a_\nu)_\nu$ gegeben. Dann konvergiert $(a_\nu)_\nu$ in $\mathbb{Q}_p$ gegen $\alpha$.*

**Beweis:** Sei $\varepsilon' > 0$ eine reelle Zahl und $\varepsilon$ rational mit $0 < \varepsilon \leq \varepsilon'$. Es gibt ein $N \in \mathbb{N}$ mit $|a_\nu - a_\mu| < \varepsilon/2$ für alle $\nu, \mu \geq N$. Für jedes $\mu \geq N$ wird die Folge $(\varepsilon/2 - |a_\nu - a_\mu|)_\nu$ also „schließlich positiv". Da $|\alpha - a_\mu|$ gemäß 17.18 durch die Folge $(|a_\nu - a_\mu|)_\nu$ gegeben wird, folgt $\varepsilon/2 \geq |\alpha - a_\mu|$. Somit ist $|\alpha - a_\mu| < \varepsilon$ für $\mu \geq N$. □

**Satz: 17.25** *Sei $p \in \mathbb{P} \cup \{\infty\}$. Der Körper $\mathbb{Q}_p$ ist (bezüglich $|\ | = |\ |_p$) vollständig. Das heißt: Ist $(\alpha_\nu)_\nu$ (bezüglich $|\ |$) eine Cauchy-Folge in $\mathbb{Q}_p$, so konvergiert sie auch in $\mathbb{Q}_p$ (bezüglich $|\ |$).*

**Beweis:** Jedes Folgenglied $\alpha_\nu$ wird durch eine Cauchy-Folge $(a_{\nu,\mu})_\mu$ rationaler Zahlen gegeben. Für jedes $\nu > 0$ gibt es nach obigem Satz ein $\mu(\nu) \in \mathbb{N}$ mit

$$|a_{\nu,\mu(\nu)} - \alpha_\nu| < 1/\nu.$$

Wir zeigen, dass die Folge $(a_{\nu,\mu(\nu)})_\nu$ eine Cauchy-Folge bezüglich $|\ |$ in $\mathbb{Q}$ und die durch sie gegebene Zahl $\alpha \in \mathbb{Q}_p$ der Limes der Folge $(\alpha_\nu)_\nu$ ist.
Es gilt:

$$|a_{\nu,\mu(\nu)} - a_{\lambda,\mu(\lambda)}| \leq |a_{\nu,\mu(\nu)} - \alpha_\nu| + |\alpha_\nu - \alpha_\lambda| + |\alpha_\lambda - a_{\lambda,\mu(\lambda)}|.$$

Sei nun $\varepsilon > 0$. Wenn nun $n \in \mathbb{N}$ so groß ist, dass einerseits $1/n \leq \varepsilon/3$, andererseits $|\alpha_\nu - \alpha_\lambda| < \varepsilon/3$ für alle $\nu, \lambda \geq n$ gilt, so ergibt sich

$$|a_{\nu,\mu(\nu)} - a_{\lambda,\mu(\lambda)}| < \varepsilon \text{ für } \nu, \lambda \geq n.$$

Also ist $(a_{\nu,\mu(\nu)})_\nu$ eine Cauchy-Folge.
Ferner gilt:
$$|\alpha-\alpha_\nu| \le |\alpha - a_{\nu,\mu(\nu)}| + |a_{\nu,\mu(\nu)} - \alpha_\nu|.$$
Sei $\varepsilon > 0$. Ist $n$ so groß, dass $|\alpha - a_{\nu,\mu(\nu)}| < \varepsilon/2$ für $\nu \ge n$ gemäß 17.23 und $1/n < \varepsilon/2$ ist, so ergibt sich:
$$|\alpha-\alpha_\nu| < \varepsilon \text{ für } \nu \ge n.$$
□

*Die folgenden Ausführungen über $\mathbb{Q}_p$, wo $p$ eine Primzahl ist, haben in Bezug auf $\mathbb{R}$ kein Analogon. Sei also für den Rest des Paragrafen $p$ eine Primzahl und $|\ | = |\ |_p$.*
Es sei daran erinnert, dass die möglichen Werte des Betrages 0 oder $p^r$ mit $r \in \mathbb{Z}$ sind, und dass für $|\ |$ auf $\mathbb{Q}_p$ die verschärfte Dreiecksungleichung (iv') aus 17.5 gilt.

**Satz: 17.26** *a) Für jedes $r \in \mathbb{Z}$ ist die Menge $\left\{x \in \mathbb{Q}_p \,\middle|\, |x| \le p^r\right\}$ eine Untergruppe der additiven Gruppe von $\mathbb{Q}_p$.*
*b) Die Menge*
$$\mathbb{Z}_p := \left\{x \in \mathbb{Q}_p \,\middle|\, |x| \le 1\right\}$$
*ist ein Unterring von $\mathbb{Q}_p$. Insbesondere gilt $\mathbb{Z} \subset \mathbb{Z}_p$.*
*c) Jedes Element $a \in \mathbb{Q}_p^*$ ist von der Form $a = up^r$ mit $u \in \mathbb{Z}_p^*$ (der Einheitengruppe von $\mathbb{Z}_p$) und $r \in \mathbb{Z}$.*
*Dabei ist genau dann $up^r \in \mathbb{Z}_p$, wenn $r \ge 0$ ist. Insbesondere ist jedes $a \in \mathbb{Q}_p$ von der Form $a = b/c$ mit $b, c \in \mathbb{Z}_p$.*
*d) Die Ideale $\neq (0)$ von $\mathbb{Z}_p$ sind die Hauptideale $p^r\mathbb{Z}_p$ mit $r \in \mathbb{N}$. Es gilt:*
$$p^r\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \,\middle|\, |x| \le p^{-r}\right\}.$$
*e) $\mathbb{Z}_p$ ist ein Hauptidealring und $p$ ist bis auf Assoziierte das einzige Primelement in $\mathbb{Z}_p$.*

**Beweis:** a) folgt aus (iv') in 17.5.
b) Wegen a) ist $\mathbb{Z}_p$ eine Untergruppe der additiven Gruppe von $\mathbb{Q}_p$. Die Abgeschlossenheit bezüglich der Multiplikation folgt aus (iii) in 17.5. Wegen $|1| = 1$ ist $1 \in \mathbb{Z}_p$. Übrigens ist auch $p \in \mathbb{Z}_p$.
c) Sei $|a| = p^{-r}$, $r \in \mathbb{Z}$. Für $u := p^{-r}a$ gilt dann

$$|u| = |p^{-r}| \cdot |a| = p^r p^{-r} = 1.$$

Also ist $u \in \mathbb{Z}_p$ und wegen $|u^{-1}| = |u|^{-1} = 1$ auch $u^{-1} \in \mathbb{Z}_p$. Somit ist $u$ eine Einheit in $\mathbb{Z}_p$ und $a = up^r$. Ist $a \notin \mathbb{Z}_p$, d.h. $r < 0$, so ist $p^{-r} \in \mathbb{Z}_p$ und $a = u/p^{-r}$.
d) Sei $I \neq (0)$ ein Ideal von $\mathbb{Z}_p$ und $p^{-r}$ der größte Wert aller Beträge von Elementen aus $I$. (Dass es einen solchen gibt, sieht man daran, dass man $r$ als kleinste unter allen natürlichen Zahlen $s$ mit $|b| = p^{-s}$ für ein $b \in I$ wählen kann.) Es gibt also ein $a \in I$ von der Form $a = p^r u$ mit einem $u \in \mathbb{Z}_p^*$. Dann ist $p^r = au^{-1} \in I$, also $p^r\mathbb{Z}_p \subset I$. Für jedes $b \in I - \{0\}$ gibt es ein $s \geq r$ und ein $v \in \mathbb{Z}_p^*$ mit $b = vp^s$. Damit ist $b \in p^r\mathbb{Z}_p$. Der Rest ist klar. □

**Satz: 17.27** *Sei $r \in \mathbb{N}$. Die Einbettung $\mathbb{Z} \subset \mathbb{Z}_p$ „induziert“ einen Isomorfismus:*

$$\mathbb{Z}/p^r \xrightarrow{\cong} \mathbb{Z}_p/p^r\mathbb{Z}_p.$$

**Beweis:** Es ist

$$\mathbb{Z} \cap p^r\mathbb{Z}_p = \left\{ x \in \mathbb{Z} \,\middle|\, |x| \leq p^{-r} \right\} = p^r\mathbb{Z}.$$

Die Verkettung $f$ der kanonischen Abbildungen

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^r\mathbb{Z}_p$$

hat also den Kern $p^r\mathbb{Z}$ und „induziert“ deshalb nach dem Homomorfiesatz 6.29 einen injektiven Ringhomomorfismus

$$g : \mathbb{Z}/p^r \longrightarrow \mathbb{Z}_p/p^r\mathbb{Z}_p.$$

(Allgemein benutzt man folgenden Sprachgebrauch: Seien $h : A \longrightarrow C$ ein Ringhomomorfismus, und $I, J$ Ideale von $A$, bzw. $C$ mit $h(I) \subset J$. Durch

Verkettung von $h$ mit der kanonischen Abbildung $C \to C/J$ erhält man einen Homomorfismus $f : A \to C/J$ und aus letzterem nach dem Homomorfiesatz 6.29 einen Homomorfismus $g : A/I \to C/J$. Man sagt dann, $h$ induziere $g$. Sind $A, C$ Gruppen und $I, J$ Normalteiler, so benutzt man denselben Ausdruck, etc.)

Zu zeigen bleibt, dass $g$ surjektiv ist.

Sei $\alpha \in \mathbb{Z}_p$ durch die Cauchy-Folge rationaler Zahlen $(a_\nu)_\nu$ gegeben. Da $|\alpha| \leq 1$ ist, gilt für genügend große $\nu$, also ohne Einschränkung der Allgemeinheit für alle $\nu$, auch $|a_\nu| \leq 1$, d.h. $a_\nu \in \mathbb{Z}_p \cap \mathbb{Q}$. Da $(a_\nu)_\nu$ eine Cauchy-Folge ist, gibt es ein $N \in \mathbb{N}$, so dass $|a_\nu - a_\mu| < p^{-r}$ für $\nu, \mu \geq N$ gilt. Das bedeutet aber $a_\nu \equiv a_\mu \pmod{p^r\mathbb{Z}_p}$ für $\nu, \mu \geq N$. Man kann also $\alpha$ modulo $p^r\mathbb{Z}_p$ durch eine konstante Folge repräsentieren, d.h. es gibt ein $a \in \mathbb{Q} \cap \mathbb{Z}_p$ mit $a \equiv \alpha \pmod{p^r\mathbb{Z}_p}$. Wir können $a = m/n$ mit $m, n \in \mathbb{Z}$, $p \nmid n$ schreiben, da $|a| \leq 1$ ist. In $\mathbb{Z}/p^r$ ist $(n \bmod p^r)$ mithin invertierbar. Ist nun $nn' \equiv 1 \pmod{p^r}$, $n' \in \mathbb{Z}$, so gilt $g(mn' \bmod p^r) = (a \bmod p^r\mathbb{Z}_p) = (\alpha \bmod p^r\mathbb{Z}_p)$, da $g$ ein Ringhomomorfismus ist. Somit ist $g$ surjektiv. $\square$

**Definitionen: 17.28** *a) Das unendliche direkte Produkt*

$$\prod_{r\in\mathbb{N}} \mathbb{Z}/p^r$$

*ist die Menge aller Folgen $(a_r)_r$, wo $a_r \in \mathbb{Z}/p^r$ ist. Offenbar ist $\prod \mathbb{Z}/p^r$ vermöge komponentenweiser Addition und Multiplikation ein Ring.*

*b) Wir haben eine (nach links unendliche) Folge von kanonischen Ringhomomorfismen*

$$\ldots \xrightarrow{\kappa_2} \mathbb{Z}/p^2 \xrightarrow{\kappa_1} \mathbb{Z}/p \xrightarrow{\kappa_0} \mathbb{Z}/1.$$

*Der inverse Limes (auch projektiver Limes genannt) dieser Folge:*

$$\varprojlim_r \mathbb{Z}/p^r$$

*ist definiert als die Menge*

$$\left\{ (a_r)_r \in \prod_{r\in\mathbb{N}} \mathbb{Z}/p^r \,\middle|\, \kappa_r(a_{r+1}) = a_r \text{ für alle } r \in \mathbb{N} \right\}.$$

*Offenbar ist $\varprojlim \mathbb{Z}/p^r$ ein Unterring von $\prod_{r\in\mathbb{N}} \mathbb{Z}/p^r$.*

*c) Wir haben für jedes $r$ einen Ringhomomorfismus $f_r$ als Verkettung von*

$$\mathbb{Z}_p \xrightarrow{\kappa} \mathbb{Z}_p/p^r\mathbb{Z}_p \xrightarrow{g^{-1}} \mathbb{Z}/p^r,$$

*also insgesamt einen Ringhomomorfismus:*

$$\mathbb{Z}_p \longrightarrow \prod_{r\in\mathbb{N}} \mathbb{Z}/p^r, \;\; \alpha \mapsto (f_r(\alpha))_r.$$

*Sein Bild liegt offenbar in* $\varprojlim \mathbb{Z}/p^r$. *D.h. wir haben auf kanonische Weise einen Ringhomomorfismus*

$$F : \mathbb{Z}_p \longrightarrow \varprojlim_r \mathbb{Z}/p^r$$

*gefunden.*

**Satz: 17.29** *$F$ ist ein Isomorfismus.*

**Beweis:** a) $F$ ist injektiv; denn

$$\ker F = \bigcap_{r\in\mathbb{N}} p^r\mathbb{Z}_p = \left\{ x \in \mathbb{Z}_p \,\middle|\, |x| \le p^{-r} \text{ für alle } r \in \mathbb{N} \right\}$$

$$= \left\{ x \in \mathbb{Z}_p \,\middle|\, |x| = 0 \right\} = (0).$$

b) $F$ ist surjektiv! Sei $(a_r)_r \in \varprojlim \mathbb{Z}/p^r$. Wähle $b_r \in \mathbb{Z}$ mit $(b_r \bmod p^r) = a_r$.
*Behauptung:* Die Folge $(b_r)_r$ ist bezüglich $|\ |_p$ eine Cauchy-Folge.
*Beweis hierfür:* Sei $\varepsilon > 0$ eine rationale Zahl und $t \in \mathbb{N}$ mit $p^{-t} < \varepsilon$. Für alle $r, s \ge t$ haben $a_r$ und $a_s$ nach Definition von $\varprojlim \mathbb{Z}/p^r$ dasselbe Bild in $\mathbb{Z}/p^t$. Also ist $b_r \equiv b_s \pmod{p^t}$, d.h. $|b_r - b_s| \le p^{-t} < \varepsilon$.
Durch die Folge $(b_r)_r$ wird also ein Element $\alpha \in \mathbb{Z}_p$ gegeben. Und offenbar ist $F(\alpha) = (a_r)_r$. □

AUFGABEN UND HINWEISE

*In den Aufgaben 1) bis ) werden die sogenannten Kettenbrüche behandelt.*

**1)** Ein endlicher Kettenbruch ist ein Ausdruck der Form

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots \atop \qquad a_{n-1} + \cfrac{b_{n-1}}{a_n}}}}$$

Dabei seien die $a_i$, $b_i \in \mathbb{R}$ derart, dass kein Nenner Null ist. (Dies gilt z.B. dann, wenn $a_i > 0$ für $i \geq 1$ und $b_i \geq 0$ für $i \geq 0$ ist.) Wir kürzen diesen Kettenbruch mit

$$[a_0, b_0; a_1, b_1; \ldots; a_{n-1}, b_{n-1}; a_n] \quad \text{ab.}$$

Zeigen Sie: Ist $b_n$ eine weitere reelle Zahl und

$$\begin{pmatrix} a_0 & b_0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_n & b_n \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & b_n p_{n-1} \\ q_n & b_n q_{n-1} \end{pmatrix},$$

so ist

$$[a_0, b_0; \ldots, b_{n-1}; a_n] = \frac{p_n}{q_n} \quad \text{und}$$

$$[a_0, b_0; \ldots, b_{n-2}; a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}.$$

**??)** (Vgl. 16A.4) Sei $\alpha \in \mathbb{R}$ mit $0 < \alpha < 1$. Zeigen Sie: $\alpha$ ist eine – möglicherweise unendliche – Summe von Stammbrüchen mit streng monoton wachsenden Nennern.

(Ist $1/n$ der größte Stammbruch $\leq \alpha$, so ist $\alpha - 1/n < 1/n$.)

Wegen 16A.4 besteht die entstehende Reihe genau dann aus endlich vielen Gliedern, wenn $\alpha \in \mathbb{Q}$ ist.

# Literaturverzeichnis


[1] Bergmann, G.: Über Eulers Beweis des großen Fermatschen Satzes für den Exponenten 3. Math. Annalen **164** (1966) 159–175

[2] Bombieri, E.: The Mordell Conjecture Revisited. Annali della Scuola Norm. Sup. de Pisa S. IV, vol XVII 1990 (615–640)

[3] Brüske, R., Ischebeck, F., Vogel, F.: *Kommutative Algebra.* B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1989

[4] Chandrasekharan, K.: *Introduction to Analytic Number Theory.* Springer–Verlag Berlin/Heidelberg/New York 1968

[5] Davenport, H.: *Multiplicative Number Theory.* 2nd Ed. Springer–Verlag Berlin/Heidelberg/New York 1980

[6] Euler, L.: *Vollständige Anleitung zur niedern und höhern Algebra.* Berlin 1797

[7] Faltings, G., Wüstholz, G. et al.: *Rational Points.* Friedr. Vieweg u. Sohn Braunschweig/Wiesbaden 1984

[8] Forster, O.: *Analysis 1.* Friedr. Vieweg u. Sohn Braunschweig 1976

[9] Gauß, C.F.: *Werke.* Königl. Gesellsch. d. Wissenschaften Göttingen 1876

[10] Heath–Brown, D.R.: The First Case of Fermat's Last Theorem. Math. Intelligencer 7 no.**4** (1985) 40–47, 55

[11] Hilbert, D.: *Gesammelte Abhandlungen* Bd. I. Springer–Verlag Heidelberg

[12] Ischebeck, F.: Primzahlfragen und ihre Geschichte. Math. Semesterber. 40 (1993) 121–132

[13] Ireland, K., Rosen, M.: *A Classical Introduction to Modern Number Theory*. Springer–Verlag Berlin/Heidelberg/New York 1982

[14] Koblitz, N.: *A Course in Number Theory and Cryptography*. 2nd Edition Springer–Verlag New York/Berlin/Heidelberg 1994

[15] Korevaar, J.: On Newman's Quick way to the Prime Number Theorem. Math. Intelligencer **4** (1982) 108–115

[16] Knopp, K.: *Theorie und Anwendung der unendlichen Reihen.* Springer–Verlag Berlin/Heidelberg/New York 1964

[17] Lorenz, F.: *Einführung in die Algebra I.* B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1987

[18] Lorenz, F.: *Algebraische Zahlentheorie.* B.I. Wissenschaftsveerlag Mannheim/Leipzig/Wien/Zürich 1993

[19] Lorenzen, P.: *Einführung in die operative Logik und Mathematik.* Springer–Verlag Berlin/Göttingen/Heidelberg 1955

[20] Lorenzen, P.: *Differential und Integral.* Akademische Verlagsgesellschaft Frankfurt a.M. 1965

[21] Marcus, D.A.: *Number Fields.* Springer–Verlag Berlin/Heidelberg/ New York 1977

[22] Neukirch, J.: *Algebraische Zahlentheorie.* Springer–Verlag Berlin/Heidelberg/New York 1992

[23] Padberg, F.: *Elementare Zahlentheorie.* 2. Aufl. (!) B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1991

[24] Prachar, K.: *Primzahlverteilung.* Springer–Verlag Berlin/ Göttigen/Heidelberg 1957

[25] Remmert, R., Ullrich, P.: *Elementare Zahlentheorie.* Birkhäuser Verlag Basel/Boston 1987

[26] Riesel, H.: *Prime Numbers and Computer Methods for Factorization.* Birkhäuser Verlag Basel/Boston/Stuttgart 1985

[27] Scharlau, W., Opolka, H. oxoxoxoxoxoxoxo

[28] Scheid, H.: *Zahlentheorie.* B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1991

[29] Scholz, A., Schoeneberg, B.: *Einführung in die Zahlentheorie.* Walter de Gruyter Berlin/New York 1973

[30] Schroeder, M.R.: *Number Theory in Science and Communication.* Springer–Verlag, Berlin 1984

[31] Serre, J.P.: *Cours d'Arithmétique.* Presses Universitaires de France Paris 1970 (Engl. Ausgabe: A Course in Arithmetic. Springer–Verlag Berlin/Heidelberg/New York 1973)

[32] Trost, E.: *Primzahlen.* 2. Aufl. Birkhäuser Verlag Basel/ Stuttgart 1968

[33] Weil, A.: *Number Theory for Beginners.* Springer–Verlag Berlin/Heidelberg/New York 1979

# Index