

MITSCHRIEB

# Algebra und Zahlentheorie

*Emma Bach*

Basierend auf:

Vorlesung Algebra und Zahlentheorie von  
Prof. Dr. Wolfgang SOERGEL

2025-10-28

# Inhalt

<b>1</b>	<b>Primzahlen</b>	<b>2</b>
<b>2</b>	<b>Gruppen</b>	<b>5</b>

# Chapter 1

## Primzahlen

**Definition 1.1.**  $H \subseteq \mathbb{Z}$  heißt Untergruppe von  $\mathbb{Z}$ , wenn

$$n \in H \implies -n \in H,$$

und

$$m, n \in H \implies m + n \in H$$

**Satz 1.2.** Es gibt eine Bijektion

$$\begin{aligned} \mathbb{N} &\leftrightarrow \{\text{Untergruppen von } (\mathbb{Z},+)\} \\ n &\mapsto n\mathbb{Z} \end{aligned}$$

*Beweis.* Sei  $H \subseteq \mathbb{Z}$  eine Untergruppe. Entweder  $H = \{0\} = 0\mathbb{Z}$ , oder  $H \neq \{0\}$ .

Sei also  $H \neq \{0\}$ . Dann gibt es ein kleinstes Element  $m$  der Menge  $\{n \in H \mid n > 0\}$ . Aus den Untergruppenaxiomen folgt  $m\mathbb{Z} \subseteq H$ . Gleichzeitig kann kein Element  $n \notin m\mathbb{Z}$  in  $H$  enthalten sein, denn sonst wäre auch  $r = n \bmod m \neq 0$  in  $H$  enthalten. Dann hätten wir aber  $r < m$ , was ein Widerspruch ist.

Als Umkehrfunktion wählen wir das kleinste positive Element von  $H$ . □

**Definition 1.3.** Eine **Primzahl** ist eine natürliche Zahl  $p \in \mathbb{N}_{\geq 2}$ , die nicht als Produkt zweier Zahlen  $a, b < p$  geschrieben werden kann.

**Satz 1.4.** Es gibt unendlich viele Primzahlen.

*Beweis.* Angenommen, es gäbe endlich viele Primzahlen. Sei also  $p_1, \dots, p_r$  eine vollständige Liste aller Primzahlen. Dann wäre aber

$$q = 1 + \prod_{i=1}^r p_i$$

durch keine Primzahl teilbar, also selbst eine Primzahl. Widerspruch! □

**Satz 1.5.** Jede Zahl  $n \in \mathbb{N}$  kann als Produkt von Primzahlen geschrieben werden:

$$n = p_1 \cdot \dots \cdot p_r \quad (r \geq 0)$$

*Beweis.* Der Fall  $n = 1$  gilt per Konvention durch das leere Produkt.

Sei  $n \geq 2$  gegeben. Es gilt entweder:

- $n$  ist eine Primzahl.
- $n$  ist von der Gestalt  $n = a \cdot b$ , mit  $a, b < n$ .

Der Satz folgt durch Induktion über die entstehende Baumstruktur - nach Induktionsannahme haben  $a$  und  $b$  eine Primfaktorzerlegung. Also hat auch  $n$  eine Primfaktorzerlegung.  $\square$

**Definition 1.6.** Der **größte gemeinsame Teiler** von  $a, b \in \mathbb{Z}$  mit  $a \neq 0$  oder  $b \neq 0$  ist die Zahl:

$$\text{ggT}(a, b) = \max\{d \in \mathbb{N} : d \mid a \wedge d \mid b\}$$

**Satz 1.7. Über den größten gemeinsamen Teiler:** Seien  $a, b \in \mathbb{Z}$ . So gibt es  $r, s \in \mathbb{N}$  mit

$$\text{ggT}(a, b) = ra + sb$$

Gegeben  $d \mid a$  und  $d \mid b$  gilt außerdem  $d \mid \text{ggT}(a, b)$ .

*Beweis.* Die Menge

$$H := \{ra + sb \mid r, s \in \mathbb{Z}\} = a\mathbb{Z} + b\mathbb{Z}$$

bildet eine Untergruppe von  $\mathbb{Z}$ , ist also eine Gruppe der Form  $m\mathbb{Z}$  mit  $m > 0$ . Da  $a \in m\mathbb{Z}$  und  $b \in m\mathbb{Z}$  ist  $m$  ein gemeinsamer Teiler. Da  $m$  ein Element in  $H$  ist existiert außerdem per Definition eine Darstellung  $m = r'a + s'b$ . Es gilt also

$$(d \mid a) \wedge (d \mid b) \implies d \mid r'a + s'b \implies d \mid m.$$

Aus  $(d \mid a) \wedge (d \mid b) \implies d \mid m$  folgt nun, dass jeder Teiler von  $a$  und  $b$   $m$  teilt, also kann es keinen Teiler von  $a$  und  $b$  geben, welcher größer als  $m$  ist.  $\square$

Die Existenz der Darstellung  $\text{ggT}(a, b) = ra + sb$  ist auch als das **Lemma von Bézout** oder die **Bézoutsche Identität** bekannt.

**Lemma 1.8. Lemma von Euklid:** Sei  $p$  eine Primzahl und  $a, b \in \mathbb{Z}$ . Dann gilt:

$$p \mid ab \implies (p \mid a) \vee (p \mid b)$$

*Beweis.* Es reicht zu Zeigen:

$$(p \nmid a) \wedge (p \mid ab) \implies p \mid b$$

Aus  $p \nmid a$  folgt  $\text{ggT}(p, a) = 1$ . Nach dem Lemma von Bézout können wir also 1 darstellen als:

$$1 = rp + sa$$

also:

$$b = rpb + sab$$

Es gilt trivial  $p \mid prb$ , außerdem gilt per Annahme  $p \mid ab$ . Es folgt  $p \mid rpb + sab = b$ .  $\square$

**Satz 1.9. Eindeutigkeit der Primfaktorzerlegung im Ring  $\mathbb{Z}$ :** Sei  $n \in \mathbb{N}_{\geq 1}$  und

$$n = \prod_{i=1}^r p_i = \prod_{i=1}^s q_i$$

wobei alle  $q_i$  und  $r_i$  Primzahlen sind. So gilt  $r = s$  und es gilt eine Permutation  $\sigma \in S_r$  mit  $p_i = q_{\sigma(i)}$ .

Äquivalente Formulierungen:

- Falls die  $p_i$  und  $q_i$  Aufsteigend oder Absteigend sortiert sind, gilt  $\forall i : p_i = q_i$
- Es existiert eine Bijektion zwischen endlichen Multimengen von Primzahlen und  $\mathbb{N}_{\geq 1}$ .

*Beweis.* Per Induktion folgt aus dem Lemma von Euklid schnell:

$$p_1 \mid p_1 \implies \bigvee_{i=1}^s p_1 \mid q_i$$

Also existiert ein  $q_i$  mit  $p_1 = q_i$ . Teilen wir nun beide Seiten durch  $p_1$ , folgt die Aussage durch die Induktionsannahme.  $\square$

**Definition 1.10.** Euklidischer Algorithmus

# Chapter 2

## Gruppen

### Definition 2.1.

1. Eine Menge  $M$  mit Verknüpfung  $\top : M \times M \rightarrow M$  heißt **Magma**.
2. Ein Magma mit neutralem Element heißt **unitäres Magma**.
3. Ein unitäres Magma mit assoziativer Verknüpfung heißt **Monoid**.
4. Ein Monoid mit inversen Elementen heißt **Gruppe**.
5. Eine Gruppe mit kommutativer Gruppe heißt **kommutative Gruppe** oder **abelsche Gruppe**.

### Beispiel 2.2.

1.  $(\mathbb{Z}, -)$  ist ein nichtunitäres Magma.
2. ?
3.  $(\mathbb{N}, +)$  und  $(\mathbb{N}, \cdot)$  sind Monoide.
4.  $(\mathbb{Z}, +)$  ist eine abelsche Gruppe.

**Satz 2.3.** Das neutrale Element einer Gruppe ist eindeutig.

- Es gibt keine Gruppe mit 0 Elementen, da die Leere Menge kein neutrales Element hat.
- Es gibt genau eine Gruppe mit einem Element, die Gruppe  $\{e\}$ .

**Satz 2.4.** Es gibt genau eine Gruppe mit zwei Elementen, nämlich die Gruppe  $\{e, a\}$ , mit Verknüpfungstabelle:

	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

*Beweis.* Durch die Definition von  $e$  sind drei Teile der Tabelle schon eindeutig festgelegt.  $a \cdot a = e$ , da sonst  $a$  kein Inverses hätte.  $\square$

**Satz 2.5.** Gilt für ein Gruppenelement  $a \in G$   $a^2 = a$ , so gilt  $a = e$ .

*Beweis.*

$$a = ae = aaa^{-1} = aa^{-1} = e$$

□

**Satz 2.6.** Aus  $a \cdot x = a \cdot y$  folgt  $x = y$ .

*Beweis.*

$$\begin{aligned} ax &= ay \\ a^{-1}ax &= a^{-1}ay \\ ex &= ey \\ x &= y \end{aligned}$$

□

Es folgt, dass in einer Gruppentabelle in jeder Spalte und jeder Zeile kein Element doppelt vorkommen kann.

**Korollar 2.7.** Es gibt nur eine Gruppe mit drei Elementen, nämlich:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

**Satz 2.8.** Es gibt zwei Gruppen mit vier Elementen, nämlich:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

**Definition 2.9.** Ein Gruppenhomomorphismus ist eine Abbildung

$$\varphi : (G, \top) \rightarrow (H, \perp)$$

mit

$$\varphi(a \top b) = \varphi(a) \perp \varphi(b)$$

Wir schreiben die Menge der Gruppenhomomorphismen von  $G$  nach  $H$  als  $\text{Grp}(G, H)$ .

**Satz 2.10.**  $\text{Grp}((\mathbb{Z}, +), G) \simeq G$

*Beweis.* Ordne jedem Gruppenelement  $g$  die Abbildung  $\varphi(n) : g \rightarrow g^n$  zu. □

**Satz 2.11.** Sind  $G$  und  $H$  Gruppen, so gilt  $\text{Mag}(G, H) = \text{Mon}(G, H) = \text{Grp}(G, H)$ .

**Definition 2.12.** Eine Teilmenge  $H \subseteq G$  einer Gruppe  $G$  heißt **Untergruppe**, wenn sie so mit einer Gruppenstruktur versehen werden kann, dass die Einbettungsabbildung  $i : H \rightarrow G$  ein Gruppenhomomorphismus ist.

Dies ist eine sehr allgemeine Definition, die analog für Untervektorräume, Untermagmas etc. funktioniert. In der Praxis verwendet man meistens folgendes Kriterium:

**Satz 2.13.**  $H$  ist genau dann eine Untergruppe, wenn  $e \in H$  und wenn für jedes  $a, b \in H$  auch  $ab \in H$  und  $a^{-1}, b^{-1} \in H$ .

**Satz 2.14. Satz von Lagrange:** Sei  $G$  eine endliche Gruppe und  $H$  eine Untergruppe. So ist die Zahl der Elemente von  $H$  ein Teiler der Zahl der Elemente von  $G$ .

Der Beweis folgt nach einigen weiteren Definitionen und Sätzen.

**Definition 2.15.** Sei  $G$  eine Gruppe mit Untergruppe  $H$ . Wir definieren:

$$\begin{aligned} gH &= \{gh \mid h \in H\} \subseteq G \\ G/H &= \{gH \mid g \in G\} \subseteq \mathcal{P}(G) \end{aligned}$$

**Lemma 2.16.** Sei  $h \in H$ . Dann gilt  $hH = H$ .

**Lemma 2.17.** Je zwei Nebenklassen  $gH$  und  $g'H$  sind entweder gleich oder disjunkt.

Aus diesen beiden Lemmas folgt  $|G| = |G/H| \cdot |H|$ , was den Satz von Lagrange impliziert.

**Satz 2.18.** Der Schnitt beliebig vieler Untergruppen bildet eine Untergruppe.

**Definition 2.19.** Sei  $G$  eine Gruppe und  $T \subseteq G$  eine Teilmenge. Die **durch  $T$  erzeugte Untergruppe**  $\langle T \rangle$  ist die kleinste Untergruppe, welche  $T$  enthält.

$\langle T \rangle$  besteht aus allen Elementen von  $G$ , welche durch beliebig häufige Anwendung von Inversionen und Gruppenoperationen entstehen kann, wobei wir die "leere Gruppenoperation" als  $e$  definieren (für den Fall  $\langle \emptyset \rangle = \{e\}$ ).

**Satz 2.20.** Sei  $\varphi : G \rightarrow H$  ein Gruppenhomomorphismus. Sei  $A$  eine Untergruppe von  $G$  und  $B$  eine Untergruppe von  $H$ . So ist  $\varphi(A)$  eine Untergruppe von  $H$  und  $\varphi^{-1}(B)$  eine Untergruppe von  $G$ .

**Satz 2.21. Universelle Eigenschaft surjektiver Gruppenhomomorphismen:** Sei  $\varphi : G \rightarrow H$  ein surjektiver Gruppenhomomorphismus. Sei  $\psi : G \rightarrow K$  ein Gruppenhomomorphismus, sodass  $\ker \psi \supseteq \ker \varphi$ . So existiert genau ein Gruppenhomomorphismus  $\bar{\psi}$ , sodass:

$$\psi = \bar{\psi} \circ \varphi$$

Also sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ & \searrow \psi & \downarrow \exists! \bar{\psi} \\ & & K \end{array}$$

*Beweis.* Sei  $\varphi(x) = \varphi(y)$ , also  $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(\varphi(y))$ . Dann gilt

$$\varphi(xy^{-1}) = \varphi(1) = 1,$$

also  $xy^{-1} \in \ker \varphi$ , also  $y \in x \cdot \ker \varphi$ . Somit gilt

$$\varphi^{-1}(\varphi(g)) = g \cdot \ker \varphi.$$

Es gilt außerdem

$$\psi(g \cdot \ker \varphi) = \psi(g) \cdot \psi(\ker \varphi) = \varphi(g),$$

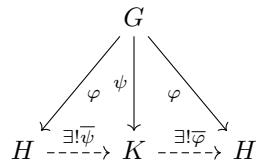
also ist  $\psi$  konstant auf den Fasern (also den Urbildern einzelner Elemente) von  $\varphi$ . Somit existiert ein  $\bar{\psi}$  Aufgrund der "universellen Eigenschaft surjektiver Funktionen", welche noch nicht eingeführt wurde :), folgt die Existenz eines  $\bar{\psi}$  mit den gefragten Eigenschaften.

Zu zeigen ist noch, dass  $\bar{\psi}$  ein Gruppenhomomorphismus ist.

Wähle hierfür  $g \in G, g' \in G$  und  $\varphi(g) = h$  und  $\varphi(g') = h'$ . Dann gilt

$$\bar{\psi}(hh') = \bar{\psi}(\varphi(gg')) = \psi(gg') = \psi(g) \cdot \psi(g') = \bar{\psi}(h) \cdot \bar{\psi}(h')$$

□



Die "Moral" dieses Satzes: Ein surjektiver Gruppenhomomorphismus  $\varphi : G \rightarrow H$  wird durch  $(G, \ker \varphi)$  "im wesentlichen eindeutig" festgelegt.

Die Frage ist nun, ob jede Untergruppe einer Gruppe  $G$  als Kern eines surjektiven Gruppenhomomorphismus festgelegt ist. Die Antwort auf diese Frage: Nein! Die einzigen Untergruppen, welche als solche Kerne auftreten, sind sogenannte **Normalteiler**.

**Definition 2.22.** Sei  $G$  eine Gruppe. Eine Untergruppe  $N \subseteq G$  heißt **Normalteiler**, falls

$$\forall g \in G : gN = Ng$$

**Beispiel 2.23.** Wir betrachten die Gruppe  $Q \subset GL(2, \mathbb{R})$  aller linearen Abbildungen, welche ein Quadrat auf sich selbst abbilden. Prof. Soergel nennt diese Gruppe auch gerne die "Bierdeckelgruppe  $B$ ". Die Gruppe hat acht Elemente:

- Die Rotationen  $d_0, d_1, d_2$  und  $d_3$  um Vielfache von  $90^\circ$ ,
- die Spiegelungen  $s_x$  und  $s_y$  an den Koordinatenachsen,
- und die Spiegelungen  $s_+$  und  $s_-$  an den Diagonalachsen.

Diese Gruppe ist nicht kommutativ! Zum Beispiel ist  $d_1s_+ = s_y$ , aber  $s_+d_1 = s_x$  (Wir notieren die Elemente als Abbildungen, also wird links zuerst  $s_+$  und dann  $d_1$  angewandt).

Wir betrachten nun die Untergruppe  $H = \langle s_+ \rangle$ . So gilt  $d_1 H = \{s_y, d_1\}$ , aber  $H d_1 = \{s_x, d_1\}$

**Satz 2.24.** *Der Kern eines Gruppenhomomorphismus ist immer ein Normalteiler.*

*Beweis.* Sei  $\varphi : G \rightarrow H$ . So ist  $(\ker \varphi)x = \varphi^{-1}(\varphi(x)) = x(\ker \varphi)$ .  $\square$

**Satz 2.25.** *Für jeden Normalteiler  $N \subseteq G$  gibt es einen surjektiven Gruppenhomomorphismus  $\varphi : G \rightarrow H$  mit  $\ker \varphi = N$ .*

*Beweis.* Wir wählen  $H := G/N = \{xN : x \in G\}$ . Für je zwei Teilmengen  $A, B \subseteq G$  definieren wir  $AB = \{ab : a \in A, b \in B\}$  und erhalten eine assoziative Verknüpfung auf  $\mathcal{P}(G)$ . Für einen Normalteiler  $N \subseteq G$  ist  $G/N$  unter dieser Verknüpfung stabil (geschlossen), denn durch Abuse of Notation folgt  $xNyN = xyNN = xyN$ . Unter dieser Verknüpfung wird  $G/N$  eine Gruppe mit neutralem Element  $1N = N$  und  $x^{-1}N = (xN)^{-1}$ .

Dadurch wird dann  $\varphi : G \rightarrow G/N$ ,  $x \mapsto xN$  ein Gruppenhomomorphismus mit  $\ker \varphi = N$ .  $\square$

**Beispiel 2.26.** Die Menge  $D \subsetneq Q$  der Drehungen eines Quadrats ist ein Normalteiler der vollen Symmetriegruppe  $Q$ .

*Beweis.* Sei  $s$  eine beliebige Spiegelung. So gilt  $Ds = \{s_+, s_-, s_x, s_y\} = sD$ . Einzelne Spiegelungen kommutieren also nicht mit einzelnen Gruppenelementen, es ist jedoch trotzdem eine Art "Kommutativität mit der Gruppe als Ganzes" vorhanden.  $\square$

Die Menge der Drehungen ist desweiteren gegeben als der Kern der Determinante, welche ein Gruppenhomomorphismus in die Gruppe mit zwei Elementen ist (genauer in die Gruppe  $\{\pm 1, \cdot\}$ ).

**Satz 2.27.** *Sei  $\varphi : G \rightarrow H$  ein Gruppenhomomorphismus. So induziert  $\varphi$  einen Isomorphismus  $G/\ker \varphi \rightarrow \text{im } \varphi$ .*

Sei  $G$  eine Gruppe mit  $|G| = 5$ . Gemäß Lagrange hat  $G$  nur die triviale Gruppe und sich selbst als Untergruppe. Sei  $g \in G \setminus \{1\}$ . So haben wir einen Gruppenhomomorphismus

$$\begin{aligned}\varphi : (\mathbb{Z}, +) &\rightarrow G \\ n &\mapsto g^n\end{aligned}$$

Wir wissen nun, dass das Bild von  $\varphi$  eine Untergruppe von  $G$  bildet. Da  $g \neq 1$  handelt es sich nicht um die triviale Gruppe, also ist  $G = \text{im } \varphi$ .

$\ker \varphi \subsetneq \mathbb{Z}$  ist eine Untergruppe, also existiert genau ein  $n \in \mathbb{N}$ , sodass  $\ker \varphi = \mathbb{Z}n$ . Da  $G$  5 Elemente hat, muss  $n = 5$ . Die einzige Gruppe mit 5 Elementen ist also  $\mathbb{Z}/5\mathbb{Z}$ .

**Korollar 2.28.** *Ist  $p$  eine Primzahl, so ist jede Gruppe mit  $p$  Elementen isomorph zu  $\mathbb{Z}/p\mathbb{Z}$ .*

**Lemma 2.29.** *Sei  $\pi : G \rightarrow H$  ein surjektiver Gruppenhomomorphismus und  $N \subseteq G$  ein Normalteiler. So ist  $\pi(N)$  ein Normalteiler von  $H$ .*

**Satz 2.30. Noetherscher Isomorphiesatz:** Sei  $G$  eine Gruppe und seien  $H$  und  $K$  Normalteiler. So ist  $H/K$  ein Normalteiler von  $G/K$  und die Komposition kanonischer Abbildungen  $G \rightarrow G/K \rightarrow (G/K)/(H/K)$  induziert einen Isomorphismus  $G/H \rightarrow (G/K)/(H/K)$

**Definition 2.31.** Sei  $G$  eine Gruppe und  $g \in G$ . Wir definieren die Ordnung eines Elements als:

$$\text{ord}(g) = \inf\{n \in \mathbb{N}_{\geq 1} \mid g^n = e\}$$

Erinnerung: Das Infimum der leeren Menge ist  $\infty$ , also gilt  $\text{ord}(g) = \infty$  falls kein solches  $n$  existiert.

**Proposition 2.32.** Sei  $G$  eine Gruppe und  $g \in G$ .

1.  $\text{ord}(g) = |\langle g \rangle|$
2.  $\langle g \rangle$  ist isomorph zu  $\mathbb{Z}/(\text{ord}(g))\mathbb{Z}$ , falls die Ordnung endlich ist, und zu  $\mathbb{Z}$ , falls die Ordnung unendlich ist.
3. Falls  $\text{ord}(g) < \infty$ , so gilt  $g^n = e \Leftrightarrow \text{ord}(g) \mid n$

**Definition 2.33.** Sei  $G$  eine Gruppe. So heißt  $|G|$  die **Ordnung** der Gruppe.

**Satz 2.34.** Sei  $g \in G$  ein Element einer endlichen Gruppe. So ist  $\text{ord}(g)$  ein Teiler von  $|G|$ .

*Beweis.*  $\text{ord}(g) = |\langle g \rangle|$ . Nach Lagrange teilt die Größe der Untergruppe  $\langle g \rangle$  die Größe der Gruppe  $G$ .  $\square$

Im Allgemeinen gibt es aber nicht für jeden Teiler ein Element mit der jeweiligen Ordnung. Zum Beispiel fehlt bei jeder nicht zyklischen Gruppe bereits die Ordnung selbst. Wohl aber gilt:

**Satz 2.35. Cauchy:** Sei  $p$  eine Primzahl mit  $p \mid |G|$ . So gibt es ein  $g \in G$  mit  $\text{ord}(g) = p$ .

Ein Beweis folgt aber erst später.

**Korollar 2.36.** Sei  $g \in G$  ein Element einer endlichen Gruppe. So gilt

$$g^{|G|} = e.$$

*Beweis.*  $g^{|G|} = g^{r \cdot |\text{ord}(g)|} = e^r = e$ .  $\square$

**Satz 2.37. Kleiner Satz von Fermat:** Sei  $p$  eine Primzahl und  $a \in \mathbb{Z}$ . So gilt

$$a^p \equiv a \pmod{p}$$

*Beweis.* Wir betrachten  $\mathbb{Z}/p\mathbb{Z}$ . Falls  $\alpha \equiv 0 \pmod{p}$  ist die Aussage trivial. Außerdem hat die Multiplikative Gruppe die Ordnung  $p-1$ , also gilt für  $\alpha \not\equiv 0$   $\alpha^{p-1} \equiv 1 \pmod{p}$ , also  $\alpha^p \equiv \alpha \pmod{p}$ .  $\square$

*Beweis.* (Ohne Gruppentheorie): Sei  $a \in \{0, \dots, p-1\}$ . So sind die Zahlen  $a, 2a, 3a, \dots, (p-1)a$  paarweise verschieden, also ist nach Schubfachprinzip ein Element jeder Restklasse  $\pmod{p}$  enthalten. Also gilt:

$$\prod_{k=1}^{p-1} ka \equiv \prod_{k=1}^{p-1} k \pmod{p}$$

$$\implies (p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Allerdings ist  $(p-1)!$  teilerfremd zu  $p$ , also können wir durch  $(p-1)!$  teilen und erhalten  $a^{p-1} \equiv 1 \pmod{p}$ .  $\square$

**Satz 2.38.** Seien  $a, b \in \mathbb{N}_{\geq 1}$  teilerfremd. So induziert

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ n &\mapsto (n + a\mathbb{Z}, n + b\mathbb{Z})\end{aligned}$$

einen Isomorphismus:

$$\mathbb{Z}/ab\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

*Beweis.* Nach Bézout gibt es  $x, y \in \mathbb{Z}$  mit

$$xa + yb = 1.$$

Nun gilt:

$$\begin{aligned}n = xy &= 1 - yb \xrightarrow{\varphi} (0, 1) \\ m = yb &= 1 - xy \xrightarrow{\varphi} (1, 0)\end{aligned}$$

Diese Tupel bilden eine Basis des Bildraums, also ist  $\varphi$  surjektiv:

$$\begin{aligned}\varphi(\alpha n + \beta m) &= \varphi(\alpha n) + \varphi(\beta m) \\ &= \alpha\varphi(n) + \beta\varphi(m) \\ &= (\beta, \alpha)\end{aligned}$$

Da beide Seiten gleich viele Elemente haben handelt es sich sogar um einen Isomorphismus.  $\square$

**Beispiel 2.39.** Das Kongruenzensystem

$$\begin{aligned}n &\equiv 3 \pmod{17} \\ n &\equiv 5 \pmod{9} \\ n &\equiv 1 \pmod{12}\end{aligned}$$

hat keine Lösung, denn aus  $n \equiv 5 \pmod{9}$  folgt  $n \equiv 2 \pmod{3}$ , also  $n \not\equiv 1 \pmod{12}$ . Ersetzen wir jedoch 12 durch 13, so sind die Teiler teilerfremd und der chinesische Restsatz garantiert eine Lösung.

**Satz 2.40. Chinesischer Restsatz / Satz von Sunzi / Satz von Aryabhata:** Satz 2.38 funktioniert auch für mehr als zwei Zahlen - sind  $q_1, \dots, q_r \in \mathbb{N}_{\geq 1}$  teilerfremd, so

ist

$$\mathbb{Z} \rightarrow \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$$

surjektiv und induziert einen Isomorphismus

$$\mathbb{Z}/q_1 \dots q_r \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$$

Genauer kann man isomorph jedem Element  $n$  das Tupel  $(n \pmod{q_1}, \dots, n \pmod{q_r})$  zuordnen - so kommt man zurück zur "klassischen" Formulierung des Chinesischen Restsatzes.

**Korollar 2.41.** Die Gruppe  $\mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$  wird durch das Element  $(1, \dots, 1)$  erzeugt und ist somit zyklisch.

**Lemma 2.42. Zentrales Lemma der RSA-Verschlüsselung:** Seien  $p$  und  $q$  prim und  $st \equiv 1 \pmod{(p-1)(q-1)}$ . So ist  $(a^t)^s \equiv a \pmod{pq}$ .

*Beweis.* Wir wissen  $a^x = a \pmod{p}$  falls  $x \equiv 1 \pmod{(p-1)}$ .

Also  $a^x = a \pmod{pq}$ , wenn  $x \equiv 1 \pmod{(p-1)}$  und  $x \equiv 1 \pmod{(q-1)}$ , also insbesondere  $a^x = a \pmod{p}$  wenn  $x \equiv 1 \pmod{(p-1)(q-1)}$ .  $\square$

In der RSA-Verschlüsselung werden dann letztendlich  $pq$  und  $t$  veröffentlicht,  $a^t$  als Nachricht zurückgeschickt, und dann durch Exponentiation mit  $s$  die Nachricht entschlüsselt.

**Definition 2.43.** Sei  $A$  eine abelsche Gruppe und  $p$  eine Primzahl. Wir definieren:

$$A(p) = \{a \in A \mid \exists n \in \mathbb{N} : \text{ord}(a) = p^n\}$$

**Satz 2.44.** Sei  $(A, +)$  eine abelsche Gruppe. Für jede Primzahl  $p$  ist  $A(p) \subseteq A$  eine Untergruppe.

*Beweis.* Seien  $x, y \in A(p)$ . So existieren  $r, s \in \mathbb{N}_{\geq 0}$ , sodass  $p^r x = p^s y = 0$ . Da  $A$  abelsch ist folgt

$$p^{r+s}(x+y) = p^r x + p^s y = 0$$

Also  $x+y \in A(p)$ .

Es gilt außerdem  $p0 = 0$ , also  $0 \in A(p)$ , und  $p^r(-x) = -(p^r x) = -0 = 0$ , also  $-x \in A(p)$ .  $\square$

**Satz 2.45.** Sei  $(A, +)$  eine abelsche Gruppe und seien  $p_1, \dots, p_r$  paarweise verschiedene Primzahlen. So liefert die Gruppenverknüpfung eine Injektion

$$A(p_1) \times \dots \times A(p_r) \hookrightarrow A$$

mit Bild alle Elemente endlicher Ordnung, in deren Ordnung nur die Primfaktoren  $p_1, \dots, p_r$  vorkommen.

*Beweis.* Sei sonst  $(a_1, \dots, a_r) \neq (0, \dots, 0)$  ein Tupel mit  $a_i \in A(p_i)$  und

$$a_1 + \dots + a_r = 0.$$

Sei OBdA  $a_1 \neq 0$ . So gilt:

$$-a_1 = a_2 + \dots + a_r$$

Für hinreichend großes  $n$  gilt nun

$$-(p_2 \dots p_r)^n a_1 = (p_2 \dots p_r)^n (a_2 + \dots + a_r) = 0$$

Allerdings gilt

$$(p_2 \dots p_r)^n a_1 \neq 0$$

Da die Primzahlen  $p_2, \dots, p_r$  alle die Ordnung von  $a_1$  nicht teilen. Widerspruch!

Sei nun  $a \in A$ ,  $\text{ord}(a) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ . So gilt:

$$\begin{aligned} \langle a \rangle &\cong \mathbb{Z}/\text{ord}(a)\mathbb{Z} \\ &= \mathbb{Z}/p_1^{\alpha_1} \dots p_r^{\alpha_r}\mathbb{Z} \\ &\cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} \end{aligned}$$

□

Dieser Satz ist analog zur Hauptraumzerlegung eines Vektorraums - wir zerlegen  $A$  in eine direkte Summe aus Untergruppen. Es gibt in der kommutativen Algebra einen Satz über Module über Ringe, welcher sowohl diesen Satz als auch die Hauptraumzerlegung gemeinsam verallgemeinert.

**Korollar 2.46.** *Sei  $E$  eine endliche abelsche Gruppe. Seien  $p_1, \dots, p_r$  die Primfaktoren der Kardinalität  $|E|$  von  $E$ . So gilt:*

1. Die Verknüpfung liefert eine Bijektion

$$E(p_1) \times \dots \times E(p_r) \xrightarrow{\sim} E$$

2. Für alle  $i$  ist  $|E(p_i)|$  eine Potenz von  $p_i$ .

*Beweis.*

1. Folgt direkt aus dem vorherigen Satz, da die Elemente endlicher Ordnung, in deren Ordnung nur die Primfaktoren  $p_1, \dots, p_r$  vorkommen, nun die ganze Gruppe ausmachen.

2. Folgt aus Induktion über  $|E_p|$ . Der Fall  $|E_p| = 1$  ist klar:

$$|E_p| = 1 = p^0$$

Für  $|E_p| > 1$  existiert ein Element  $x \neq 0$ . Es gilt  $|\langle x \rangle| = p^r$  nach Annahme. Dann folgt

$$|E(p)/\langle x \rangle| = p^s$$

nach Induktionsannahme, da der Quotient kleiner ist. Somit folgt nach Lagrange

$$|E_p| = |E(p)/\langle x \rangle| \cdot |\langle x \rangle| = p^s \cdot p^r$$

□

**Proposition 2.47.** Sei  $E$  eine endliche abelsche Gruppe, sodass die Ordnung jedes  $x \in E$  eine Potenz von  $p$  prim ist. So ist  $|E|$  ebenfalls eine  $p$ -Potenz.

**Proposition 2.48.** Es existiert eine Bijektion zwischen der Menge der endlichen abelschen Gruppen bis auf Isomorphismus und den endlichen Multimengen echter Primpotenzen. Genauer hat jede endliche abelsche Gruppe die Form

$$\mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_r\mathbb{Z}$$

Für  $p_1, \dots, p_r$  prim.

Zum Beispiel ist jede abelsche Gruppe der Ordnung 8 isomorph zu  $\mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , oder  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

**Satz 2.49.** Sei  $K$  ein Körper und  $K^\times$  dessen multiplikative Gruppe. So ist jede endliche Untergruppe von  $K^\times$  zyklisch.

**Definition 2.50.** Sei  $G$  eine Gruppe und  $X$  eine Menge. Eine Operation von  $G$  auf  $X$  ist eine Abbildung

$$\begin{aligned} G \times G &\rightarrow X \\ (g, x) &\mapsto gx \end{aligned}$$

Sodass:

1.  $\forall g, h \in G : (gh)x = g(hx)$
2.  $1x = x$

**Beispiel 2.51.** Sei  $X$  eine Menge und

$$\text{Ens}^\times(X) := \{f : X \rightarrow X \mid f \text{ bijektiv}\}$$

So ist  $\text{Ens}^\times$  eine Gruppe, welche durch Anwendung der jeweiligen Funktion auf kanonische Weise auf  $X$  operiert:

$$\begin{aligned} \text{Ens}^\times(X) \times X &\rightarrow X \\ (f, x) &\mapsto f(x) \end{aligned}$$

**Beispiel 2.52.**  $\mathcal{S}_n$  operiert durch Anwendung der jeweiligen Permutation auf  $\{1, \dots, n\}$ .

**Beispiel 2.53.** Analog operiert  $\text{GL}(n, \mathbb{R})$  auf  $\mathbb{R}^n$ .

**Definition 2.54.** Sei  $G$  eine Gruppe, welche auf eine Menge  $X$  operiert. So nennen wir für  $x \in X$  die Menge

$$Gx = \{gx \mid g \in G\}$$

die **Bahn** von  $x$ .

**Beispiel 2.55.** Wir lassen die Gruppe  $\text{SO}(2)$  der zweidimensionalen Rotationsmatrizen auf  $\mathbb{R}^2$  operieren. So ist die Bahn eines Vektors  $\vec{v}$  der Kreis mit Radius  $\|\vec{v}\|$ .

**Beispiel 2.56.** Sei  $H$  eine Untergruppe einer Gruppe  $G$ . So operiert  $H$  durch die Gruppenoperation auf  $G$  und die Bahnen  $Hg$  sind genau die Nebenklassen.

**Proposition 2.57.** Die Bahnen der Operation einer Gruppe auf einer Menge sind paarweise disjunkt.

**Proposition 2.58.** Die Bahnen der Operation eines Monoids auf einer Menge sind nicht unbedingt paarweise disjunkt.