Mitschrieb

Algebra und Zahlentheorie

Emma Bach

Basierend auf:

Vorlesung Algebra und Zalentheorie von
Prof. Dr. Wolfgang Soergel

October 14, 2025

Inhalt

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 $r = n \mod m \neq 0$ 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 $p_1, \ldots, p_r$ 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:*

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

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. □

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

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

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

$$ggT(a, b) = ra + sb$$

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

Beweis. Die Menge

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

bildet eine Untergruppe von 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. □

Die Existenz der Darstellung $\mathrm{ggT}(a, b) = ra + sb$ ist auch als das **Lemma von Bézout** oder die **Bézoutsche Identät** 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 $\mathrm{ggT}(p, a) = 1$. 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 $p \mid rpb + sab = b$. □

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. □