Grundwissen Lineare Algebra
Zusammenfassung der 3.Vorlesungswoche

Dozent: Dr. Jan-David Hardtke

Universität Leipzig, Institut für Mathematik

26. bis 30. April 2021

Zusammenfassung der 3.Vorlesungswoche

Auf den folgenden Seiten werden die wesentlichen Inhalte der 3.Vorlesungswoche zusammengefasst.
Dies kann und soll **kein Ersatz für die Lektüre des Skriptes** sein.
Insbesondere wird für die Beweise hier meist nur auf das Skript verwiesen.

In dieser Woche geht es um den Euklidischen Algorithmus zur Berechnung des ggT und eine Einführung in das Thema Gruppen.
Das sind die **Abschnitte II.3 und III.1 im Skript**.

Der Euklidische Algorithmus

Division mit Rest:
Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann existieren eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $a = qb + r$ und $r < |b|$.

Definition

Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ oder $b \neq 0$. Dann bezeichnet

$$\mathrm{ggT}(a, b) := \max\{c \in \mathbb{N} : c \mid a \text{ und } c \mid b\}$$

den **größten gemeinsamen Teiler** von a und b (max steht für Maximum, also das größte Element der Menge).

Der Euklidische Algorithmus

Zur Bestimmung des ggT verwendet man üblicherweise das folgende Verfahren (für den Beweis siehe Satz II.3.3. im Skript).

Euklidischer Algorithmus:
Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Bestimme zuerst $q_0, r_0 \in \mathbb{Z}$ mit

$$a = q_0 b + r_0, \quad 0 \leq r_0 < |b|.$$

Ist $r_0 = 0$, so ist $\mathrm{ggT}(a, b) = b$.
Anderenfalls finden wir $q_1, r_1 \in \mathbb{Z}$ mit

$$b = q_1 r_0 + r_1, \quad 0 \leq r_1 < r_0.$$

Ist $r_1 = 0$, so ist $\mathrm{ggT}(a, b) = r_0$.

Der Euklidische Algorithmus

Euklidischer Algorithmus (Fortsetzung):
Anderenfalls gibt es $q_2, r_2 \in \mathbb{Z}$ mit

$$r_0 = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Ist $r_2 = 0$, so ist $\mathrm{ggT}(a, b) = r_1$.
Anderenfalls bestimme $q_3, r_3 \in \mathbb{Z}$ mit

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

So fortfahrend erhalten wir $q_0, \ldots, q_n, r_0 \ldots, r_n \in \mathbb{Z}$ mit

$$r_{i-1} = q_{i+1} r_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i$$

für $i = 1, \ldots, n-1$, wobei $r_0, \ldots, r_{n-1} \neq 0$ und $r_n = 0$.
Dann gilt $\mathrm{ggT}(a, b) = r_{n-1}$, der größte gemeinsame Teiler von a und b ist also gleich dem letzten nicht verschwindenden Rest.

Der Euklidische Algorithmus

Beispiel:
Wir suchen $\mathrm{ggT}(2331, 987)$. Der Euklidische Algorithmus ergibt Folgendes:

$$\begin{aligned}
2331 &= 2 \cdot 987 + 357 \\
987 &= 2 \cdot 357 + 273 \\
357 &= 1 \cdot 273 + 84 \\
273 &= 3 \cdot 84 + 21 \\
84 &= 4 \cdot 21 + 0
\end{aligned}$$

Also ist $\mathrm{ggT}(2331, 987) = 21$.

Zwei weitere Beispiele finden Sie im Skript.

Der Euklidische Algorithmus

Wichtige Folgerungen:

Lemma

Seien $a, b \in \mathbb{Z}$ *mit* $a \neq 0$ *oder* $b \neq 0$. *Dann gilt für alle* $c \in \mathbb{N}$*:*

$$1) \quad c \mid a \text{ und } c \mid b \;\Rightarrow\; c \mid \mathrm{ggT}(a, b)$$

$$2) \quad \mathrm{ggT}(ca, cb) = c \cdot \mathrm{ggT}(a, b)$$

Lemma

Seien $a, b \in \mathbb{Z}$ *und sei* p *eine Primzahl mit* $p \mid ab$. *Dann gilt* $p \mid a$ *oder* $p \mid b$.

Beweise im Skript (Korollar II.3.4., Lemmata II.3.5. und II.3.6.)

Der Euklidische Algorithmus

Als Konsequenz erhält man die Eindeutigkeit der Primfaktorzerlegung (bis auf Reihenfolge der Faktoren).

Satz (Eindeutigkeit der Primfaktorzerlegung):
Seien $p_1, \ldots, p_n$ und $q_1, \ldots, q_m$ Primzahlen mit $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$.
Dann gilt $n = m$ und nach einer eventuellen Umsortierung $q'_1, \ldots, q'_n$ von $q_1, \ldots, q_n$ gilt $p_i = q'_i$ für $i = 1, \ldots, n$.

Beweis: Siehe Skript Satz II.3.7.

Der Euklidische Algorithmus

Definition

Seien $a, b \in \mathbb{N}$. Dann heißt

$$\mathrm{kgV}(a, b) := \min\{c \in \mathbb{N} : a \mid c \text{ und } b \mid c\}$$

das **kleinste gemeinsame Vielfache** von a und b (min steht für Minimum).

Satz:
Für alle $a, b \in \mathbb{N}$ gilt

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

Beweis: Siehe Skript Satz II.3.9.

Gruppen

Definition

Sei G eine nicht leere Menge und $* : G \times G \to G$ eine Verknüpfung (Abbildung).
1) $(G, *)$ heißt **Halbgruppe**, falls das **Assoziativgesetz**

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$$

gilt.
2) $(G, *)$ heißt **Monoid**, falls $(G, *)$ eine Halbgruppe ist und zusätzlich ein **neutrales Element** $e \in G$ existiert, d. h. ein Element e mit

$$e * a = a = a * e \quad \forall a \in G.$$

Bemerkung: Ein Monoid $(G, *)$ besitzt **genau ein** neutrales Element (siehe Bemerkung III.1.2. im Skript).

Gruppen

Definition

Ein Monoid $(G, *)$ heißt **Gruppe**, falls es zu jedem $a \in G$ ein **inverses Element** gibt, d. h. ein Element $b \in G$ mit $b * a = e = a * b$, wobei e das neutrale Element von $(G, *)$ ist.

Bemerkung: Sei $(G, *)$ eine Gruppe und sei $a \in G$.
Dann besitzt a **genau ein** inverses Element, welches üblicherweise mit a^{-1} bezeichnet wird (siehe Bemerkung III.1.4. im Skript).

Lemma

Sei $(G, *)$ eine Gruppe und seien $a, b \in G$.
Dann gilt $(a * b)^{-1} = b^{-1} * a^{-1}$.

Beweis: Siehe Lemma III.1.5. im Skript.

Definition

Eine Gruppe $(G, *)$ heißt **kommutative** oder **abelsche Gruppe**, falls das **Kommutativgesetz**

$$a * b = b * a \quad \forall a, b \in G$$

gilt.

Bemerkung: In vielen Fällen bezeichnet man die Verknüpfung einer Gruppe mit $\cdot$ oder $+$ anstelle von $*$ und schreibt dann 1 bzw. 0 für das neutrale Element. In einer Gruppe $(G, +)$ wird das inverse Element zu a mit $-a$ bezeichnet.

Gruppen

Beispiele:
1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ bilden jeweils eine kommutative Gruppe, $(\mathbb{N}, +)$ dagegen nur eine Halbgruppe ($+$ bezeichnet hier die übliche Addition in $\mathbb{R}$).

2) Mit der üblichen Multiplikation $\cdot$ bilden $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ jeweils eine kommutative Gruppe, $(\mathbb{Z} \setminus \{0\}, \cdot)$ dagegen nicht.

3) Wir erklären auf der Menge $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$ eine Addition durch

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2) \quad \forall (a_1, b_1), (a_2, b_2) \in \mathbb{R}^2.$$

Dann ist $(\mathbb{R}^2, +)$ eine kommutative Gruppe. Neutrales Element ist $(0, 0)$, inverses Element zu (a, b) ist $(-a, -b)$.