Fakultät für Mathematik
Heinrich Heine-Universität Düsseldorf

PD Dr. Markus Perling
Sommersemester 2014

# Lineare Algebra 1

Vierte Woche, 30.4.2014

## §2 Mengen, Abbildungen und Relationen (Ende)

**Definition:** Es sei $M$ eine Menge und $\sim$ eine Äquivalenzrelation auf $M$. Dann bezeichnen wir mit

$$M/\sim := \{[m] \mid m \in M\}$$

die *Menge der Äquivalenzklassen.*

**Beispiel:** Für eine ganze Zahl $n > 0$ definieren wir eine Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ wie folgt:

$$\forall\, p, q \in \mathbb{Z}:\ p \sim q \ :\Leftrightarrow\ p - q \in n\mathbb{Z}.$$

Jedes $p \in \mathbb{Z}$ können wir per Division mit Rest schreiben als $p = k \cdot n + r$ für ein $k \in \mathbb{Z}$ und $0 \leq r < n$, wobei $r$ sogar eindeutig bestimmt ist. Insbesondere ist also $p \sim r$. Für zwei Zahlen $0 \leq s_1, s_2 < n$ gilt weiterhin: $s_1 \sim s_2 \Leftrightarrow s_1 = s_2$. Somit ist der Rest $r$ von $p$ modulo $n$ sogar eindeutig mit der Eigenschaft, daß $p \sim r$ und $0 \leq r < n$. Somit gilt auch für zwei beliebige Zahlen $p, q \in \mathbb{Z}$: $p \sim q$ genau dann, wenn $p$ und $q$ den gleichen Rest modulo $n$ haben. Es gibt somit genau $n$ Äquivalenzklassen von der Form:

$$n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z},$$

wobei wir für ein $i \in \mathbb{Z}$ schreiben:

$$i + \mathbb{Z} := \{i + kn \mid k \in \mathbb{Z}\}.$$

Mit der am Ende der letzten Vorlesung eingeführten Notation können wir etwas abkürzend schreiben:

$$\mathbb{Z}/\sim\ = \{[0], [1], \ldots, [n-1]\}.$$

**Definition:** Wir schreiben auch $\mathbb{Z}/n\mathbb{Z}$ für $\mathbb{Z}/\sim$.

Diese Bezeichnung deutet an, daß wir uns die Menge $\mathbb{Z}/n\mathbb{Z}$ in einem geeigneten Sinne als *Quotientenmenge* vorstellen sollten. Wir werden in einer späteren Vorlesung darauf zurückkommen.

**Beispiel:** Auf der Menge $M := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definieren wir eine Relation $(p, q) \sim (p', q') :\Leftrightarrow pq' = p'q$. Wir können Addition und Multiplikation auf $M/\sim$ wie folgt definieren:

$$[(p, q)] + [(r, s)] := [(ps + qr, qs)]$$
$$[(p, q)] \cdot [(r, s)] := [(pq, rs)]$$

Abkürzend schreiben wir auch $\frac{p}{q}$ für $[(p, q)]$. Es stellt sich heraus, daß wir auf diese Weise eine Darstellung der rationalen Zahlen als $\mathbb{Q} := M/\sim$ erhalten.

**Definition:** 1. Es seien $I, M$ Mengen. Eine Familie von Elementen in $M$ mit *Indexmenge* $I$ ist eine Abbildung $f : I \to M$, $m \mapsto f(i) =: m_i$. Man schreibt Man schreibt auch $(m_i)_{i\in I}$ für eine Familie von Elementen mit Indexmenge $I$.

2. Zwei Mengen $M, N$ heißen *disjunkt*, falls gilt $M \cap N = \emptyset$.

3. Eine Familie von Mengen $(M_i)_{i\in I}$ heißt *paarweise disjunkt*, wenn für alle $i, j \in I$ mit $i \neq j$ gilt: $M_i \cap M_j = \emptyset$.

4. Es sei $M$ eine Menge. Eine paarweise disjunkte Familie $(M_i)_{i\in I}$ von Teilmengen von $M$ heißt *Zerlegung* von $M$, falls $M = \bigcup_{i\in I} M_i$. Wir schreiben dann $M = \coprod_{i\in I} M_I$.

**Satz:** *Es sei $M$ eine Menge und $\sim$ eine Äquivalenzrelation auf $M$. Dann bilden die Äquivalenzklassen eine disjunkte Zerlegung von $M$, d.h. jedes $m \in M$ liegt in genau einer Äquivalenzklasse. Insbesodere gilt für je zwei Äquivalenzklassen $[m], [n]$, daß entweder $[m] = [n]$ oder $[m] \cap [n] = \emptyset$. Umgekehrt definiert jede Zerlegung $M = \coprod_{i\in I} M_i$ eine Äquivalenzrelation, indem wir für alle $m, n \in M$ setzen $m \sim n :\Leftrightarrow \exists i \in I : m, n \in M_i$.*

# §3 Gruppen

**Definition:** Eine Gruppe ist ein Paar $(G, *)$, wobei $G$ eine Menge ist und $* : G \times G \to G$ $(x, y) \mapsto x * y$ eine Abbildung, so daß folgende Axiome gelten:

(i) Für alle $x, y, z \in G$ gilt: $(x * y) * z = x * (y * z)$ (Assoziativität)

(ii) Es gibt ein $e \in G$, so daß für alle $x \in G$ gilt: $e * x = x$. (Neutrales Element)

(iii) Für alle $x \in G$ gibt es ein $x' \in G$, so daß $x' * x = e$. (Inverses Element)

Eine Gruppe heißt *abelsch*, wenn zusätzlich gilt:

(iv) $x * y = y * x$ für alle $x, y \in G$. (Kommutativität)

**Beispiele:** 1. Folgendes sind Gruppen: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$.

2. Folgendes sind keine Gruppen: $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{R}_{\geq 0}, +)$.

3. Es sei $n \in \mathbb{N}$. Wir definieren eine Verknüpfung $[+]$ auf $\mathbb{Z}/n\mathbb{Z}$ wie folgt:

$$[i] \; [+] \; [j] := [i + j].$$

Somit wird das Paar $(\mathbb{Z}/n\mathbb{Z}, [+])$ eine Gruppe.

Man beachte, daß alle diese Beispiele *abelsche* Gruppen sind.

**Satz:** *Es sei $(G, *)$ eine Gruppe.*

*(i) Das neutrale Element $e \in G$ ist eindeutig bestimmt und hat die zusätzliche Eigenschaft, daß für alle $x \in G$ gilt:*

$$x * e = x.$$

*(ii) Es sei $x \in G$, dann ist das inverse Element $x'$ zu $x$ eindeutig bestimmt und hat zusätzlich die Eigenschaft*

$$x * x' = e$$

**Bemerkung:** Wenn die Verknüpfung aus dem Kontext schon klar ist, schreibt man auch einfach $G$ anstatt $(G, *)$. Es ist gebräuchlich, eine Gruppenverknüpfung multiplikativ zu schreiben, d.h. $x \cdot y$ oder einfach $xy$ anstatt $x * y$. Das neutrale Element wird dann auch mit 1 oder $1_G$ bezeichnet. Das Inverse zu einem $x \in G$ wird dann mit $x^{-1}$ bezeichnet. Oft schreibt man Gruppen auch additiv, d.h. $x + y$. Dann wird das neutrale Element auch mit 0 oder $0_G$ bezeichnet und das Inverse zu einem $x$ mit $-x$.

**Beispiel:** Für eine Menge $M$ bezeichnen wir mit $\mathrm{Sym}(M)$ die Menge der Bijektionen von $M$ nach sich selber. Das Paar $(\mathrm{Sym}(M), \circ)$, wobei $\circ$ die Verknüpfung von Abbildungen bezeichnet, ist dann eine Gruppe. Diese Gruppe nennt man *symmetrische Gruppe*. Im Falle $M = \{1, \ldots, n\}$ schreibt man auch $\mathrm{Sym}(M) =: \mathrm{Sym}_n$. Dabei handelt es sich um die *symmetrische Gruppe auf n Elementen*, bzw. um die *Permutationsgruppe vom Grad n*. Ihre Elemente heißen *Permutationen*. Besitzt $M$ mehr als 2 Elemente, dann ist $\mathrm{Sym}(M)$ nicht abelsch.

**Beispiel:** Es seien $(G, *)$ und $(H, \cdot)$ Gruppen. Dann können wir auf $G \times H$ folgende Verknüpfung definieren: $(x, y)\#(x', y') := (x * x, y \cdot y')$. Somit wird das Paar $(G \times H, \#)$ eine Gruppe, das wir das *direkte Produkt* von $G$ und $H$ nennen.

**Definition:** Es sei $G$ eine Gruppe. Eine nichtleere Teilmenge $H \subset G$ heißt *Untergruppe*, wenn gilt:

(i) Für alle $x, y \in H$ gilt: $xy \in H$.

(ii) Für alle $x \in H$ gilt: $x^{-1} \in H$.

**Satz:** *Es sei $G$ eine Gruppe und $H$ eine Untergruppe von $G$. Dann ist $H$ selber ebenfalls eine Gruppe.*

# Literatur-/Lesevorschläge

S. Bosch, *Lineare Algebra*, §1.2
H. J. Kowalsky, G. O. Michler, *Lineare Algebra*, §1.3