Mathematische Strukturen

Lineare Algebra I

Kapitel 3

18. April 2012

Logistik

Dozent: Olga Holtz, MA 378, Sprechstunden Freitag 14-16

Webseite: www.math.tu-berlin.de/˜holtz Email: holtz@math.tu-berlin.de

Assistent: Sadegh Jokar, MA 620, Sprechstunden ???

Tutoren: Cronjäger, Guzy, Kourimska, Rudolf

Anmeldung: über MOSES

Fragen? Studentische Studienfachberatung, MA 847

Telefon: (030) 314-21097 Email: studber@math.tu-berlin.de

Vorlesungen: VL am Dienstag 10-12 im MA004, Mittwoch 8-10 im H0104

Der Kurs gilt mit 50% Punkten für Hausaufgaben als bestanden

Gruppen.

Eine Gruppe ist eine Menge G mit einer „Operation“ oder Verknüpfung $*$, die jeweils zwei Elemente von G zu einem neuen Element von G verknüpft und für die die folgenden Regeln (Axiome) erfüllt sind.

- Es gilt das Assoziativgesetz, d.h.

$$(a * b) * c = a * (b * c) \quad \text{für alle } a, b, c \in G.$$

- Es gibt ein neutrales Element $e \in G$ mit den folgenden Eigenschaften:
  a) $e * a = a$ für alle $a \in G$.
  b) für alle $a \in G$ gibt es $a' \in G$, so dass $a' * a = e$.

  Das Element a' heißt inverses Element von a.

- Eine Gruppe heißt kommutativ oder abelsch, falls außerdem das Kommutativgesetz gilt, d.h.

$$a * b = b * a \quad \text{für alle } a, b \in G.$$

Was ist eigentlich $*$?

Die Verknüpfung $*$ ist dabei z.B. die Addition $+$, dann nennen wir die Gruppe additiv oder die Multiplikation $\cdot$, dann nennen wir die Gruppe multiplikativ. Es kann aber auch eine andere Verknüpfung sein.

Was ist eigentlich $*$?

Die Verknüpfung $*$ ist dabei z.B. die Addition $+$, dann nennen wir die Gruppe additiv oder die Multiplikation $\cdot$, dann nennen wir die Gruppe multiplikativ. Es kann aber auch eine andere Verknüpfung sein.

Beispiele:

- Die ganzen Zahlen $\mathbb{Z}$ bilden eine additive kommutative Gruppe.

Was ist eigentlich $*$?

Die Verknüpfung $*$ ist dabei z.B. die Addition $+$, dann nennen wir die Gruppe additiv oder die Multiplikation $\cdot$, dann nennen wir die Gruppe multiplikativ. Es kann aber auch eine andere Verknüpfung sein.

Beispiele:

- Die ganzen Zahlen $\mathbb{Z}$ bilden eine additive kommutative Gruppe.
- Die rationalen Zahlen $\mathbb{Q}$ bilden auch eine additive kommutative Gruppe.

Was ist eigentlich $*$?

Die Verknüpfung $*$ ist dabei z.B. die Addition $+$, dann nennen wir die Gruppe additiv oder die Multiplikation $\cdot$, dann nennen wir die Gruppe multiplikativ. Es kann aber auch eine andere Verknüpfung sein.

Beispiele:

- Die ganzen Zahlen $\mathbb{Z}$ bilden eine additive kommutative Gruppe.
- Die rationalen Zahlen $\mathbb{Q}$ bilden auch eine additive kommutative Gruppe.
- Aber $\mathbb{Q} \setminus \{0\}$ bildet auch eine multiplikative kommutative Gruppe.

Fragen:

- Bildet die Menge $\mathbb{N}$ eine additive Gruppe?

Was ist eigentlich $*$?

Die Verknüpfung $*$ ist dabei z.B. die Addition $+$, dann nennen wir die Gruppe additiv oder die Multiplikation $\cdot$, dann nennen wir die Gruppe multiplikativ. Es kann aber auch eine andere Verknüpfung sein.

Beispiele:

- Die ganzen Zahlen $\mathbb{Z}$ bilden eine additive kommutative Gruppe.
- Die rationalen Zahlen $\mathbb{Q}$ bilden auch eine additive kommutative Gruppe.
- Aber $\mathbb{Q} \setminus \{0\}$ bildet auch eine multiplikative kommutative Gruppe.

Fragen:

- Bildet die Menge $\mathbb{N}$ eine additive Gruppe?
- Bildet die Menge $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ eine multiplikative Gruppe?

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Beweis. Sei $e \in G$ ein neutrales Element und sei $a \in G$ beliebig. Es gibt ein inverses Element $a_1 \in G$, so dass $a_1 * a = e$. Sei $a_2 \in G$ ein inverses Element zu a_1, d.h. $a_2 * a_1 = e$. Dann:

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Beweis. Sei $e \in G$ ein neutrales Element und sei $a \in G$ beliebig. Es gibt ein inverses Element $a_1 \in G$, so dass $a_1 * a = e$. Sei $a_2 \in G$ ein inverses Element zu a_1, d.h. $a_2 * a_1 = e$. Dann:

$$\begin{aligned} a * a_1 &= e * (a * a_1) = (a_2 * a_1) * (a * a_1) = a_2 * (a_1 * (a * a_1)) \\ &= a_2 * ((a_1 * a) * a_1) = a_2 * (e * a_1) = a_2 * a_1 = e \,. \end{aligned}$$

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Beweis. Sei $e \in G$ ein neutrales Element und sei $a \in G$ beliebig. Es gibt ein inverses Element $a_1 \in G$, so dass $a_1 * a = e$. Sei $a_2 \in G$ ein inverses Element zu a_1, d.h. $a_2 * a_1 = e$. Dann:

$$
\begin{aligned}
a * a_1 &= e * (a * a_1) = (a_2 * a_1) * (a * a_1) = a_2 * (a_1 * (a * a_1)) \\
&= a_2 * ((a_1 * a) * a_1) = a_2 * (e * a_1) = a_2 * a_1 = e\,.
\end{aligned}
$$

Somit $a * e = a * (a_1 * a) = (a * a_1) * a = e * a = a\,.$

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Beweis. Sei $e \in G$ ein neutrales Element und sei $a \in G$ beliebig. Es gibt ein inverses Element $a_1 \in G$, so dass $a_1 * a = e$. Sei $a_2 \in G$ ein inverses Element zu a_1, d.h. $a_2 * a_1 = e$. Dann:

$$\begin{aligned} a * a_1 &= e * (a * a_1) = (a_2 * a_1) * (a * a_1) = a_2 * (a_1 * (a * a_1)) \\ &= a_2 * ((a_1 * a) * a_1) = a_2 * (e * a_1) = a_2 * a_1 = e\,. \end{aligned}$$

Somit $a * e = a * (a_1 * a) = (a * a_1) * a = e * a = a$. Ist $a_3 \in G$ ein weiteres inverses Element zu a, so folgt $a_3 = a_3 * e = a_3 * (a * a_1) = (a_3 * a) * a_1 = e * a_1 = a_1$, also ist das inverse Element zu a eindeutig.

Eindeutigkeit von Inversen / neutralem Element

Theorem. Für jede Gruppe $(G, *)$ gelten:

(1) Zu jedem $a \in G$ existiert genau ein inverses Element $\widetilde{a} \in G$. Für dieses gilt $\widetilde{a} * a = a * \widetilde{a} = e$.

(2) G enthält genau ein neutrales Element e. Für dieses gilt $e * a = a * e = a$ für alle $a \in G$.

Beweis. Sei $e \in G$ ein neutrales Element und sei $a \in G$ beliebig. Es gibt ein inverses Element $a_1 \in G$, so dass $a_1 * a = e$. Sei $a_2 \in G$ ein inverses Element zu a_1, d.h. $a_2 * a_1 = e$. Dann:

$$\begin{aligned} a * a_1 &= e * (a * a_1) = (a_2 * a_1) * (a * a_1) = a_2 * (a_1 * (a * a_1)) \\ &= a_2 * ((a_1 * a) * a_1) = a_2 * (e * a_1) = a_2 * a_1 = e\,. \end{aligned}$$

Somit $a * e = a * (a_1 * a) = (a * a_1) * a = e * a = a$. Ist $a_3 \in G$ ein weiteres inverses Element zu a, so folgt $a_3 = a_3 * e = a_3 * (a * a_1) = (a_3 * a) * a_1 = e * a_1 = a_1$, also ist das inverse Element zu a eindeutig.

Ist nun $\widetilde{e} \in G$ ein weiteres neutrales Element, dann $\widetilde{e} = e * \widetilde{e} = e$ (die erste Gleichung gilt, weil e ein neutrales Element ist; die zweite Gleichung gilt, weil $a * \widetilde{e} = a$ für alle $a \in G$ gilt).

Ringe.

Ein kommutativer Ring mit Eins-Element $(R, +, \cdot)$ ist eine Menge R mit zwei „Operationen“ $+$ („Addition“) und $\cdot$ („Multiplikation“), für die folgende Gesetze gelten:

(Ass $+$)	$(a+b)+c = a+(b+c)$ für alle $a, b, c \in R$ (Assoziativgesetz),
(Komm $+$)	$a+b = b+a$ für alle $a, b \in R$ (Kommutativgesetz),
(Null)	Es gibt ein $e_0 \in R$ mit $e_0 + a = a + e_0 = a$ für alle $a \in R$ (Existenz eines Null-Elements),
(Inv $+$)	für alle $a \in R$ gibt es $a' \in R$ mit $a + a' = e_0$ (Existenz eines inversen Elements, wir schreiben $-a$ anstatt a'),
(Ass $\cdot$)	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$ (Assoziativgesetz),
(Komm $\cdot$)	$a \cdot b = b \cdot a$ für alle $a, b \in R$ (Kommutativgesetz),
(Eins)	Es gibt ein $e_1 \in R$ mit $e_1 \cdot a = a \cdot e_1 = a$ für alle $a \in R$ (Existenz eines Eins-Elements),
(Distr)	$(a+b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in R$ (Distributivgesetz).

NB. Wir schreiben 0 für e_0 und 1 für e_1.

Beispiel: Die rationalen Zahlen bilden einen solchen kommutativen Ring mit Eins-Element. Dabei haben wir in $\mathbb{Q}$ aber noch etwas mehr, nämlich dass auch Inverse bezüglich der Multiplikation (außer für 0) existieren. Damit kommen wir zur dritten Struktur:

NB. Wir schreiben 0 für e_0 und 1 für e_1.

Beispiel: Die rationalen Zahlen bilden einen solchen kommutativen Ring mit Eins-Element. Dabei haben wir in $\mathbb{Q}$ aber noch etwas mehr, nämlich dass auch Inverse bezüglich der Multiplikation (außer für 0) existieren. Damit kommen wir zur dritten Struktur:

Körper.

(i) Es sei R ein kommutativer Ring mit Eins-Element und $r \in R$. Dann heißt r invertierbar, falls es ein $\tilde{r} \in R$ mit $r \cdot \tilde{r} = 1$ gibt. Wir schreiben dann r^{-1} oder $\frac{1}{r}$ für $\tilde{r}$.

(ii) Ein kommutativer Ring mit Eins-Element heißt Körper, wenn $0 \neq 1$ und zusätzlich das weitere Gesetz gilt:

$$(\text{Inv } \cdot) \quad \text{Jedes Element } r \in R \text{ mit } r \neq 0 \text{ ist invertierbar.}$$

Der kleinste Körper $\mathbb{F}_2$.

$\mathbb{F}_2 = (\{0,1\},+,\cdot)$, wobei $+$ und $\cdot$ wie folgt definiert sind:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Die Multiplikation ist die übliche. Die Addition geht „modulo“ 2, das heißt, man nimmt die übliche Addition und verwendet immer den ganzzahligen Rest nach Division durch 2 als Ergebnis:

$$\begin{aligned} 1+1+1+1+1+1 &= 0 \quad (6:2=3\ \underline{\text{Rest } 0}), \\ 1+1+1 &= 1 \quad (3:2=1\ \underline{\text{Rest } 1}). \end{aligned}$$

Der kleinste Körper F_2.

$\mathrm{F}_2 = (\{0,1\},+,\cdot)$, wobei $+$ und $\cdot$ wie folgt definiert sind:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Die Multiplikation ist die übliche. Die Addition geht „modulo“ 2, das heißt, man nimmt die übliche Addition und verwendet immer den ganzzahligen Rest nach Division durch 2 als Ergebnis:

$$\begin{aligned} 1+1+1+1+1+1 &= 0 \quad (6:2=3 \ \underline{\text{Rest } 0}),\\ 1+1+1 &= 1 \quad (3:2=1 \ \underline{\text{Rest } 1}). \end{aligned}$$

Frage 1. Warum ist das ein Körper?

Der kleinste Körper $\mathbb{F}_2$.

$\mathbb{F}_2 = (\{0, 1\}, +, \cdot)$, wobei $+$ und $\cdot$ wie folgt definiert sind:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Die Multiplikation ist die übliche. Die Addition geht „modulo“ 2, das heißt, man nimmt die übliche Addition und verwendet immer den ganzzahligen Rest nach Division durch 2 als Ergebnis:

$$\begin{aligned} 1+1+1+1+1+1 &= 0 \quad (6:2 = 3 \ \underline{\text{Rest } 0}), \\ 1+1+1 &= 1 \quad (3:2 = 1 \ \underline{\text{Rest } 1}). \end{aligned}$$

Frage 1. Warum ist das ein Körper?

Frage 2. Gibt es Körper mit weniger als 2 Elementen?

Weitere Beispiele.

Sei

$$
\begin{aligned}
V &= \{v = a + \sqrt{2}\, b \mid a, b \in \mathbb{Q}\}, \\
v_1 + v_2 &= (a_1 + \sqrt{2}\, b_1) + (a_2 + \sqrt{2}\, b_2) \\
&= (a_1 + a_2) + \sqrt{2}\,(b_1 + b_2), \\
v_1 \cdot v_2 &= (a_1 + \sqrt{2}\, b_1) \cdot (a_2 + \sqrt{2}\, b_2) \\
&= a_1 a_2 + \sqrt{2}\, a_1 b_2 + \sqrt{2}\, a_2 b_1 + 2 b_1 b_2 \\
&= (a_1 a_2 + 2 b_1 b_2) + \sqrt{2}\,(a_1 b_2 + a_2 b_1).
\end{aligned}
$$

Ist $\{V, +, \cdot\}$ ein Körper (oder nur ein „Ring“)?

Weitere Beispiele.

Sei

$$
\begin{aligned}
V &= \{v = a + \sqrt{2}\, b \mid a, b \in \mathbb{Q}\}, \\
v_1 + v_2 &= (a_1 + \sqrt{2}\, b_1) + (a_2 + \sqrt{2}\, b_2) \\
&= (a_1 + a_2) + \sqrt{2}\,(b_1 + b_2), \\
v_1 \cdot v_2 &= (a_1 + \sqrt{2}\, b_1) \cdot (a_2 + \sqrt{2}\, b_2) \\
&= a_1 a_2 + \sqrt{2}\, a_1 b_2 + \sqrt{2}\, a_2 b_1 + 2 b_1 b_2 \\
&= (a_1 a_2 + 2 b_1 b_2) + \sqrt{2}\,(a_1 b_2 + a_2 b_1).
\end{aligned}
$$

Ist $\{V, +, \cdot\}$ ein Körper (oder nur ein „Ring“)?

$$
\frac{1}{v} = \frac{1}{a + \sqrt{2}\, b} = \frac{a - \sqrt{2}\, b}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \sqrt{2}\, \frac{b}{a^2 - 2b^2}.
$$

Weitere Beispiele.

Sei

$$
\begin{aligned}
V &= \{v = a + \sqrt{2}\,b \mid a, b \in \mathbb{Q}\}, \\
v_1 + v_2 &= (a_1 + \sqrt{2}\,b_1) + (a_2 + \sqrt{2}\,b_2) \\
&= (a_1 + a_2) + \sqrt{2}\,(b_1 + b_2), \\
v_1 \cdot v_2 &= (a_1 + \sqrt{2}\,b_1) \cdot (a_2 + \sqrt{2}\,b_2) \\
&= a_1 a_2 + \sqrt{2}\,a_1 b_2 + \sqrt{2}\,a_2 b_1 + 2 b_1 b_2 \\
&= (a_1 a_2 + 2 b_1 b_2) + \sqrt{2}\,(a_1 b_2 + a_2 b_1).
\end{aligned}
$$

Ist $\{V, +, \cdot\}$ ein Körper (oder nur ein „Ring“)?

$$
\frac{1}{v} = \frac{1}{a + \sqrt{2}\,b} = \frac{a - \sqrt{2}\,b}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \sqrt{2}\,\frac{b}{a^2 - 2b^2}.
$$

Da $\sqrt{2} \notin \mathbb{Q}$, ist $a^2 - 2b^2 \neq 0$ für alle $v \in V$, $v \neq 0$. Damit ist $\frac{1}{v} \in V$ für alle $v \in V$, $v \neq 0$. Damit folgt, dass $\{V, +, \cdot\}$ ein Körper ist!

Komplexe Zahlen.

Sei $\mathbb{C} = \{z = a + ib \mid a, b \in \mathbb{R}\}$, wobei $i = \sqrt{-1}$ die imaginäre Einheit ist, mit den Operationen

$$
\begin{aligned}
z_1 + z_2 &= (a_1 + ib_1) + (a_2 + ib_2) &= (a_1 + a_2) + i(b_1 + b_2), \\
z_1 \cdot z_2 &= (a_1 + ib_1) \cdot (a_2 + ib_2) &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2).
\end{aligned}
$$

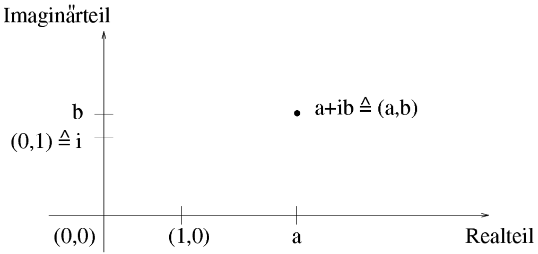
Komplexe Zahlen.

Sei $\mathbb{C} = \{z = a + ib \mid a, b \in \mathbb{R}\}$, wobei $i = \sqrt{-1}$ die imaginäre Einheit ist, mit den Operationen

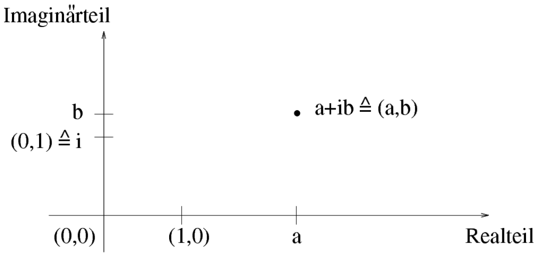
$$\begin{aligned} z_1 + z_2 &= (a_1 + ib_1) + (a_2 + ib_2) &&= (a_1 + a_2) + i(b_1 + b_2), \\ z_1 \cdot z_2 &= (a_1 + ib_1) \cdot (a_2 + ib_2) &&= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2). \end{aligned}$$

Für $z = a + ib$ heißt a Realteil und b Imaginärteil von z.

Null-Element	$0 = 0 + i0$	$(0, 0)$
Eins-Element	$1 = 1 + i0$	$(1, 0)$
imaginäre Einheit	$i = 0 + i1$	$(0, 1)$



Die konjugiert komplexe Zahl zu $z = a + ib$ ist die Zahl $\bar{z} = a - ib$.



Die konjugiert komplexe Zahl zu $z = a + ib$ ist die Zahl $\bar{z} = a - ib$.

$\mathbb{C}$ ist ein Körper, denn das inverse Element zu $z \neq 0$ ist

$$\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{\bar{z}}{z\bar{z}} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} \in \mathbb{C},$$

da $a^2 + b^2 > 0$ für $(a, b) \neq (0, 0)$.