

Tutorium: Diskrete Mathematik

Vorbereitung der ersten Abschlussklausur

Teil 1

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Algebraische Strukturen

Algebraische Strukturen I

Eine *algebraische Struktur* ist ein Paar

$$\left(A, (f_i) \right),$$

bestehend aus einer nichtleeren Menge A , der *Trägermenge* der Algebra, und einer Familie (Menge) von (endlichstelligen) Verknüpfungen auf A , die auch *fundamentale Operationen* genannt werden.

Meistens hat eine Algebra nur endlich viele Verknüpfungen f_1, \dots, f_n ; man schreibt dann für die Algebra einfach nur

$$\left(A, f_1, \dots, f_n \right).$$

Algebraische Strukturen II

Die Trägermenge A der Algebra ist *abgeschlossen* bezüglich der definierten Operationen, d.h., die Verknüpfung von zwei Elementen $a, b \in A$ (im Fall einer binären Verknüpfung) liefert stets ein Element $c \in A$. a , b und c müssen dabei nicht notwendigerweise verschieden sein.

Halbgruppen I

Eine *Halbgruppe* ist eine algebraische Struktur

$$\mathcal{H} = (H, \star)$$

mit der Trägermenge H und einer zweistelligen Verknüpfung \star .

Für alle Elemente in H gilt das Assoziativgesetz, d.h., für alle $a, b, c \in H$ gilt stets

$$a \star (b \star c) = (a \star b) \star c.$$

Halbgruppen II

Häufig wird für die Verknüpfung \star das Symbol \cdot benutzt, man spricht dann von einer *multiplikativ geschriebenen Halbgruppe*. Wie auch bei der gewöhnlichen Multiplikation, kann in vielen Situationen der Malpunkt weggelassen werden.

Eine Halbgruppe lässt sich auch *additiv* notieren, indem für die Verknüpfung \star das Symbol $+$ benutzt wird.

Halbgruppen III

Da das Assoziativgesetz gilt, kann eine vereinfachte, klammerfreie Notation verwendet werden:

$$a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

Monoide I

Ein *Monoid* ist eine algebraische Struktur

$$\mathcal{M} = (M, \star)$$

mit der Trägermenge M und einer zweistelligen Verknüpfung \star .

Ein Monoid ist eine Halbgruppe mit einem *neutralen Element* e .

Monoide II

Für Monoide gelten also die folgenden Eigenschaften:

- Für die Verknüpfung \star gilt das Assoziativgesetz:

$$\forall a, b, c \in M : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e , für das gilt:

$$\forall a \in M : e \star a = a \star e = a.$$

Das Element e ist also sowohl links- als auch rechtsneutral bzgl. der definierten Operation \star .

Monoide III

Aufgabe 1

Welche der folgenden algebraischen Strukturen sind Monoide?
Begründe deine Antworten.

a) $(\mathbb{N}, +)$

b) $(\mathbb{N}_0, :)$

c) $(\mathbb{Z}, -)$

d) $(\mathbb{R}^{4 \times 4}, \cdot)$

Gruppen I

Eine *Gruppe* ist eine algebraische Struktur

$$\mathcal{G} = (G, \star)$$

mit der Trägermenge G und einer zweistelligen Verknüpfung \star .

Eine Gruppe ist ein Monoid, in dem für jedes Element $a \in G$ das zugehörige *inverse Element* a^{-1} in G enthalten ist.

Gruppen II

Für Gruppen gelten also die folgenden Eigenschaften:

- Für die Verknüpfung \star gilt das Assoziativgesetz:

$$\forall a, b, c \in G : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e , für das gilt:

$$\forall a \in G : e \star a = a \star e = a.$$

- Existenz inverser Elemente:

$$\forall a \in G : \exists a^{-1} \in G \text{ mit } a \star a^{-1} = a^{-1} \star a = e.$$

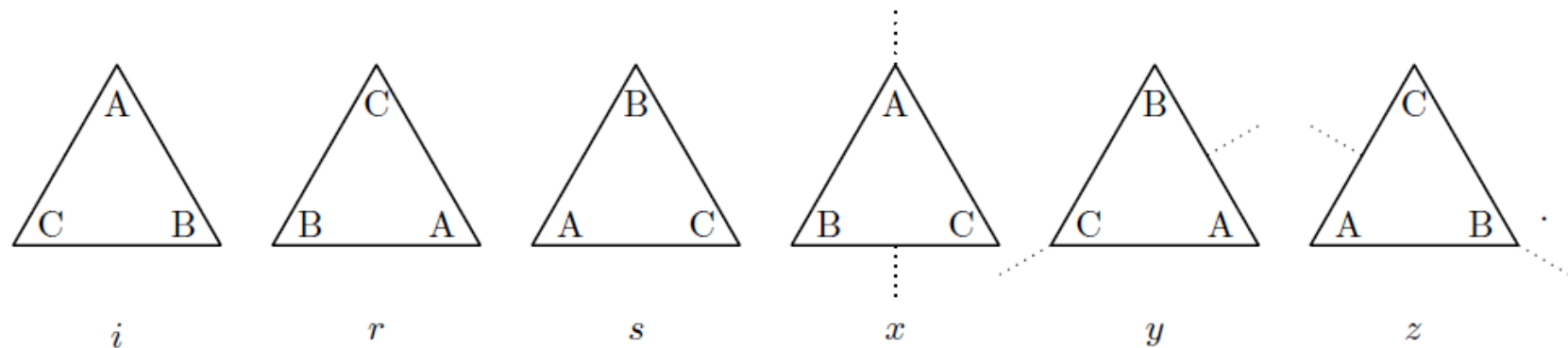
Gruppen III

Beispiele für Gruppen

- $(\mathbb{Z}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$
- $(\mathbb{R}, +)$
- Kleinsche Vierergruppe
- Dreiecksgruppe

Die Dreiecksgruppe I

Die Dreiecksgruppe G_{Δ} ist eine Gruppe, die die folgenden Elemente enthält:



i , r und s sind dabei Drehungen um 0° , 120° bzw. 240° . x , y und z sind Spiegelungen an den Winkelhalbierenden des Dreiecks.

Die Dreiecksgruppe II

Diese Gruppe besitzt die folgende *Gruppentafel*, in der die Ergebnisse der Verknüpfung der Elemente tabellarisch notiert sind:

	<i>i</i>	<i>r</i>	<i>s</i>	<i>x</i>	<i>y</i>	<i>z</i>
<i>i</i>	<i>i</i>	<i>r</i>	<i>s</i>	<i>x</i>	<i>y</i>	<i>z</i>
<i>r</i>	<i>r</i>	<i>s</i>	<i>i</i>	<i>y</i>	<i>z</i>	<i>x</i>
<i>s</i>	<i>s</i>	<i>i</i>	<i>r</i>	<i>z</i>	<i>x</i>	<i>y</i>
<i>x</i>	<i>x</i>	<i>z</i>	<i>y</i>	<i>i</i>	<i>s</i>	<i>r</i>
<i>y</i>	<i>y</i>	<i>x</i>	<i>z</i>	<i>r</i>	<i>i</i>	<i>s</i>
<i>z</i>	<i>z</i>	<i>y</i>	<i>x</i>	<i>s</i>	<i>r</i>	<i>i</i>

Die Rechteckgruppe

Aufgabe 2

Bestimme die Elemente der Rechteckgruppe und stelle die Gruppentafel dieser Gruppe auf.

Die Ordnung einer Gruppe

Die Mächtigkeit (Kardinalität) $|G|$ der Trägermenge der Gruppe nennt man die *Ordnung der Gruppe* oder auch die *Gruppenordnung*.

Für endliche Mengen G ist dies einfach die Anzahl der Elemente in G .

Die Ordnung eines Gruppenelements

Unter der *Ordnung eines Elements* $a \in G$ einer Gruppe $\mathcal{G} = (G, \star)$ versteht man die kleinste natürliche Zahl $m > 0$, für die $a^m = e$ gilt; e ist dabei das neutrale Element der Gruppe.

Gibt es keine derartige Zahl m , so hat a *unendliche Ordnung*.

Man definiert die Potenzen eines Gruppenelements wie folgt:

$$\begin{aligned} a^0 &:= e \\ a^{n+1} &:= a^n \star a. \end{aligned}$$

Untergruppen I

Ist U eine Teilmenge der Trägermenge G einer Gruppe $\mathcal{G} = (G, \star)$ (also $U \subseteq G$) und ist $\mathcal{U} = (U, \star)$ selbst eine Gruppe, so nennt man \mathcal{U} eine Untergruppe von \mathcal{G} .

Um zu zeigen, dass \mathcal{U} eine Untergruppe von \mathcal{G} ist, genügt es zu zeigen, dass Folgendes gilt:

- $a, b \in U \Rightarrow a \star b, b \star a \in U$;
- $a \in U \Rightarrow a^{-1} \in U$.

Untergruppen II

Aufgabe 3

Gegeben seien die beiden Gruppen $\mathcal{G} = (G, \star)$ und $\mathcal{H} = (H, \star)$.
Zeige, dass $(G \cap H, \star)$ eine Untergruppe sowohl von \mathcal{G} als auch von \mathcal{H} ist.

Untergruppen III

Jedes Element $a \in G$ einer Gruppe \mathcal{G} erzeugt eine Untergruppe \mathcal{H} .

Die durch $a \in G$ erzeugte Untergruppe wird mit $\langle a \rangle$ bezeichnet.

Der Satz von Lagrange I

Der *Satz von Lagrange* wurde nach dem italienischen Mathematiker Joseph-Louis Lagrange benannt.

Der Satz besagt, dass die Mächtigkeit (oder Ordnung) einer Untergruppe stets die Mächtigkeit der Gruppe teilt.

Es sei \mathcal{G} eine endliche Gruppe:

- Ist \mathcal{H} eine Untergruppe von \mathcal{G} , so ist die Mächtigkeit $|H|$ ein Teiler von $|G|$.
- Insbesondere teilt die Ordnung eines Elements $a \in G$ die Mächtigkeit $|G|$ von G .

Der Satz von Lagrange II

Aufgabe 4

Gegeben seien die beiden Gruppen $\mathcal{G} = (G, \star)$ und $\mathcal{H} = (H, \star)$. Es gelte $|G| = 48$ und $|H| = 56$. Es gelte $|G \cap H| \geq 2$. Zeige, dass in $(G \cap H, \star)$ stets ein Element der Ordnung 2 existiert.

Die symmetrische Gruppe

Als *symmetrische Gruppe* bezeichnet man die Gruppe S_n aller möglichen Permutationen über n Elementen.

Die Operation der Gruppe ist die Nacheinanderausführung von Permutationen.

Da es $n!$ verschiedene Permutationen über n Elementen gibt, gilt

$$|S_n| = n!$$

Permutationsgruppen

Als *Permutationsgruppe* bezeichnet man eine Untergruppe einer symmetrischen Gruppe S_n .

Isomorphie von Gruppen I

Zwei Gruppen heißen *isomorph* oder *strukturgleich*, wenn ihre Gruppentafeln bis auf die Bezeichnungen der Elemente übereinstimmen.

Eine wichtige Voraussetzung für Isomorphie ist, dass die Gruppen gleichviele Elemente einer jeweiligen Ordnung besitzen.

Isomorphie von Gruppen II

Aufgabe 5

Zeige, dass (bis auf Isomorphie) genau 2 verschiedene Gruppen der Ordnung 4 existieren.

Zyklische Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *zyklisch*, wenn sie mindestens ein Element enthält, aus dem sämtliche Elemente der Gruppe erzeugt werden können.

Mit anderen Worten: In G muss mindestens ein Element der Ordnung $|G|$ existieren.

Abelsche Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *abelsch* oder *kommutativ*, wenn zusätzlich zu den bisher genannten Gruppeneigenschaften das Kommutativgesetz gilt, d.h.:

$$\forall a, b \in G : a \star b = b \star a.$$

Nebenklassen I

Es sei \mathcal{H} eine Untergruppe einer Gruppe \mathcal{G} und a sei ein Element von G . Mithilfe von a und \mathcal{H} definieren wir eine Teilmenge von \mathcal{G} wie folgt:

$$a\mathcal{H} := \left\{ g \in G : \text{Es gibt ein } h \in H \text{ mit } g = a \star h \right\}.$$

Man nennt eine solche Teilmenge $a\mathcal{H}$ eine *Linksnebenklasse* von \mathcal{H} in \mathcal{G} .

Analog werden die *Rechtsnebenklassen* $\mathcal{H}a$ definiert.

Nebenklassen II

Aufgabe 6

Es sei \mathcal{G} die symmetrische Gruppe S_3 und \mathcal{H} die durch das Element $(1, 2)$ erzeugte Untergruppe von \mathcal{G} . Bestimme die Linksnebenklassen von \mathcal{H} .

Ringe I

Ein *Ring* ist eine algebraische Struktur

$$\mathcal{R} = (R, +, \cdot)$$

mit der Trägermenge R und zwei zweistelligen Verknüpfungen $+$ und \cdot .

Ringe II

In einem Ring gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(R, +)$ eine kommutative Gruppe.
- Bezüglich der Operation \cdot bildet (R, \cdot) einen Monoid.
- Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c;$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Körper I

Ein *Körper* ist eine algebraische Struktur

$$\mathcal{K} = (K, +, \cdot)$$

mit der Trägermenge K und zwei zweistelligen Verknüpfungen $+$ und \cdot .

Körper II

In einem Körper gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(K, +)$ eine kommutative Gruppe.
- Bezüglich der Operation \cdot bildet $(K \setminus \{e_+\}, \cdot)$ eine kommutative Gruppe.
- Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c;$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Körper III

Beispiele für Körper

- $(\mathbb{Q}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$
- $(\mathbb{C}, +, \cdot)$
- der *Galoiskörper* GF_2 (oder auch \mathbb{F}_2)

Relationen

Eigenschaften von Relationen I

Es sei R eine Relation über einer Menge A . Die Relation R ist

- *symmetrisch*, falls gilt:

$$\forall a, b \in A : (a, b) \in R \rightarrow (b, a) \in R.$$

- *nicht symmetrisch*, falls gilt:

$$\exists a, b \in A : (a, b) \in R \rightarrow (b, a) \notin R.$$

- *antisymmetrisch*, falls gilt:

$$\forall a, b \in A, a \neq b : (a, b) \in R \rightarrow (b, a) \notin R.$$

- *nicht antisymmetrisch*, falls gilt:

$$\exists a, b \in A : (a, b) \in R \rightarrow (b, a) \in R.$$

Eigenschaften von Relationen II

Es sei R eine Relation über einer Menge A . Die Relation R ist

- *reflexiv*, falls gilt:

$$\forall a \in A : (a, a) \in R.$$

- *nicht reflexiv*, falls gilt:

$$\exists a \in A : (a, a) \notin R.$$

- *irreflexiv*, falls gilt:

$$\forall a \in A : (a, a) \notin R.$$

- *nicht irreflexiv*, falls gilt:

$$\exists a \in A : (a, a) \in R.$$

Eigenschaften von Relationen III

Es sei R eine Relation über einer Menge A . Die Relation R ist

- *transitiv*, falls gilt:

$$\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R.$$

- *intransitiv*, falls gilt:

$$\exists a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \notin R.$$

- *antitransitiv*, falls gilt:

$$\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \notin R.$$

Eigenschaften von Relationen IV

Es sei R eine Relation über einer Menge A . Man nennt R eine

- *Äquivalenzrelation*, falls gilt:

R ist symmetrisch, reflexiv und transitiv.

- *Ordnungsrelation*, falls gilt:

R ist antisymmetrisch, reflexiv und transitiv.

Eigenschaften von Matrizen

Die Fundamentalräume einer Matrix I

Gegeben sei eine (reellwertige) $n \times m$ - Matrix A .

- Der *Zeilenraum* $Z(A)$ ist der durch die Zeilenvektoren der Matrix A aufgespannte Vektorraum:

$$\begin{aligned} Z(A) &= \text{Lin}(z_1, \dots, z_m) \\ &= \left\{ c_1 z_1 + \dots + c_m z_m \mid c_1, \dots, c_m \in \mathbb{R} \right\}. \end{aligned}$$

- Der *Spaltenraum* $S(A)$ ist der durch die Spaltenvektoren der Matrix A aufgespannte Vektorraum:

$$\begin{aligned} S(A) &= \text{Lin}(s_1, \dots, s_n) \\ &= \left\{ c_1 s_1 + \dots + c_n s_n \mid c_1, \dots, c_n \in \mathbb{R} \right\}. \end{aligned}$$

Die Fundamentalräume einer Matrix II

Gegeben sei eine (reellwertige) $n \times m$ - Matrix A .

- Der *Nullraum* $N(A)$ ist die Lösungsmenge des homogenen linearen Gleichungssystems $Ax = 0$:

$$N(A) = \{x \mid Ax = 0\}.$$

- Der *Nullraum der Transponierten* $N(A^T)$ ist die Lösungsmenge des homogenen linearen Gleichungssystems $A^T x = 0$:

$$N(A^T) = \{x \mid A^T x = 0\}.$$

Die Fundamentalräume einer Matrix III

Gegeben sei eine (reellwertige) $n \times m$ - Matrix A . Es gelten die folgenden Zusammenhänge:

- $Z(A) = S(A^T)$
- $S(A) = Z(A^T)$
- $\dim(Z(A)) = \dim(S(A))$
- $\dim(Z(A)) + \dim(N(A)) = n$
- $\dim(S(A)) + \dim(N(A^T)) = m$
- $\text{rg}(A) = \dim(Z(A)) = \dim(S(A))$

Zusammenhänge mit Determinanten

Im Folgenden sei eine quadratische $n \times n$ - Matrix A betrachtet:

- $\det(A) = 0 \iff \text{rg}(A) < n$
- $\det(A) = 0 \iff \dim(N(A)) > 0$
- $\det(A) \neq 0 \iff \text{rg}(A) = n$
- $\det(A) \neq 0 \iff \dim(N(A)) = 0$
- $\det(A) = 0 \iff A^{-1}$ existiert nicht
- $\det(A) \neq 0 \iff A^{-1}$ existiert

Zusammenhänge mit LGS

Im Folgenden sei eine quadratische $n \times n$ - Matrix A betrachtet:

- $\text{rg}(A) \neq \text{rg}(A | b) \implies Ax = b$ ist nicht lösbar
- $\text{rg}(A) = \text{rg}(A | b) = n \implies Ax = b$ ist eindeutig lösbar
- $\text{rg}(A) = \text{rg}(A | b) < n \implies Ax = b$ hat unendlich viele Lösungen