Tutorium:
Diskrete Mathematik

Vorbereitung der Klausur am 09.02.2023
(Teil 1)

25. Januar 2023

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Algebraische Strukturen

Algebraische Strukturen I

Eine *algebraische Struktur* (oder *Algebra*) ist ein Paar

$$\Big(A, (f_i)\Big),$$

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 $f_1, \ldots, f_n$; man schreibt dann für die Algebra einfach nur

$$\Big(A, f_1, \ldots, f_n\Big).$$

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 $c \in A$. Die Elemente a, b und c müssen dabei nicht notwendigerweise verschieden sein.

Magma

Eine *Magma* ist eine algebraische Struktur

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

mit der Trägermenge M und einer zweistelligen Verknüpfung $\star$.

Halbgruppen

Eine *Halbgruppe* ist eine algebraische Struktur

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

mit der Trägermenge H und einer zweistelligen Verknüpfung $\star$.

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

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

Monoide I

Ein *Monoid* ist eine algebraische Struktur

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

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

Zeige, dass das neutrale Element eines Monoids eindeutig bestimmt ist.

Monoide IV

Aufgabe 2

Entscheide für die folgenden Mengen/Verknüpfungen, ob es sich um Monoide handelt. Begründe deine Antworten!

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

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

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

d) $(\mathbb{Q}, \cdot)$

e) $(\mathbb{Z}_m, \cdot)$

Gruppen I

Eine *Gruppe* ist eine algebraische Struktur

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

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:

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

  Das Element a^{-1} ist bzgl. der Operation $\star$ sowohl links- als auch rechtsinvers zum Element a.

Abelsche Gruppen

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

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

Aufgaben

Aufgabe 3

Es seien a, b, c, d Elemente einer Gruppe $\mathcal{G}$.

a) Vereinfache den folgenden Ausdruck:

$$d\Big(b(cdb)^{-1}c^{-1}\Big)^{-1}bd^{-1}c\Big((aa^{-1}bc)^{-1}bd^{-1}c\Big)^{-1}a^{-1}d^{-1}$$

b) Können weitere Vereinfachungen vorgenommen werden, wenn zusätzlich vorausgesetzt wird, dass $\mathcal{G}$ kommutativ ist?

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:

$$a^0 := e$$
$$a^{n+1} := a^n \star a.$$

Nach dem *Satz von Lagrange* ist die Ordnung eines Gruppenelements stets ein Teiler der Ordnung der Gruppe.

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.

Zyklische Gruppen sind stets kommutativ; kommutative Gruppen aber nicht stets zyklisch.

Aufgaben

Aufgabe 4

Stelle die Gruppentafel der Rechteckgruppe auf. Welche Ordnung besitzt die Rechteckgruppe? Welche Ordnungen besitzen die Elemente der Rechteckgruppe? Ist diese Gruppe zyklisch?

Isomorphie von Gruppen I

Zwei Gruppen $\mathcal{G}_1 = (G_1, \star)$ und $\mathcal{G}_2 = (G_2, \diamond)$ heißen *isomorph* oder *strukturgleich*, wenn es zwischen ihren Elementen eine strukturerhaltende, bijektive Abbildung $\varphi : G_1 \to G_2$ gibt, für die gilt:

$$\forall a, b \in G_1 : \varphi(a \star b) = \varphi(a) \diamond \varphi(b).$$

Hieraus folgt u.a., dass die Gruppentafeln bis auf die Bezeichnungen und Reihenfolge der Elemente übereinstimmen. Eine wichtige Voraussetzung für Isomorphie ist, dass die Gruppen gleich viele Elemente einer jeweiligen Ordnung besitzen.

Zyklische Gruppen derselben Ordnung sind stets isomorph.

Isomorphie von Gruppen II

Aufgabe 5

Zeige, dass die folgenden beiden Gruppen der Ordnung 4 isomorph sind:

$(G, \star)$:

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

$(H, \circ)$:

	1	♢	□	△
1	1	♢	□	△
♢	♢	△	1	□
□	□	1	△	♢
△	△	□	♢	1

Isomorphie von Gruppen II

Aufgabe 6

Zeige, dass bis auf Isomorphie nur eine einzige Gruppe der Ordnung 7 existiert.

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:

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

Untergruppen II

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

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

Untergruppen III

Aufgabe 7

Gegeben seien eine Gruppe $(G, \star)$ sowie zwei Untergruppen U_1 und U_2 von G. Zeige, dass es sich bei $U_1 \cap U_2$ ebenfalls um eine Untergruppe von G handelt.

Der Satz von Lagrange

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.

Untergruppen IV

Aufgabe 8

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

Untergruppen V

Aufgabe 9

Gegeben sei eine Untergruppe $\mathcal{U} = (U, \star)$ einer Gruppe $\mathcal{G} = (G, \star)$ sowie eine auf der Menge G definierte Relation $\sim$, für die gilt:

$$\forall a, b \in G : a \sim b \Leftrightarrow \exists u \in U : b = a \star u.$$

Zeige, dass es sich bei der Relation $\sim$ um eine Äquivalenzrelation handelt.

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 $\circ$ von Permutationen.

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

$$|S_n| = n!$$

Permutationsgruppen I

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

Permutationsgruppen II

Aufgabe 10

Bestimme die Ordnungen der folgenden Permutationen in Zyklenschreibweise:

a) $\pi = (123)(48)(5679) \in S_9$

b) $\sigma = (124)(351)(23)(1542)(35) \in S_5$

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:

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

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 11

Es sei $\mathcal{G}$ die symmetrische Gruppe S_3 und $\mathcal{H}$ die durch das Element (132) erzeugte Untergruppe von $\mathcal{G}$. Bestimme die Links- und die Rechtsnebenklassen von $\mathcal{H}$.

Nebenklassen III

Aufgabe 12

Es sei $\mathbb{Z}_{14}^{\times}$ die Einheitengruppe des Rings $\mathbb{Z}_{14}$ und $\mathcal{H}$ die durch das Element 13 erzeugte Untergruppe von $\mathbb{Z}_{14}^{\times}$. Bestimme die Links- und die Rechtsnebenklassen von $\mathcal{H}$.

Ringe I

Ein *Ring* ist eine algebraische Struktur

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

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 $(R, \cdot)$ eine Halbgruppe.
- Es gelten die Distributivgesetze:

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

Ringe III

Gilt in einem Ring zusätzlich das Kommutativgesetz der Multiplikation, so handelt es sich um einen *kommutativen Ring*.

Existiert in einem Ring zusätzlich das neutrale Element der Multiplikation, so handelt es sich um einen *unitären Ring* bzw. um einen *Ring mit Eins*.

Ringe IV

Aufgabe 13

Entscheide, ob es sich bei $(\{0\}, +, \cdot)$ um einen Ring handelt. Begründe deine Antwort!

Die Einheitengruppe I

Als *Einheitengruppe* $E(\mathcal{R})$ bzw. $\mathcal{R}^\times$ eines Rings $\mathcal{R}$ bezeichnet man die Menge derjenigen Elemente, die im Ring $\mathcal{R}$ ein multiplikatives Inverses besitzen.

Die Einheitengruppe II

Aufgabe 14

a) Bestimme die Einheitengruppe des Rings $\mathbb{Z}$.

b) Bestimme die Einheitengruppe des Rings $\mathbb{Z}_{47}$.

Körper I

Ein *Körper* ist eine algebraische Struktur

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

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 $\mathbb{F}_2$)

Polynome

Definition I

Ein *Polynom* ist ein Ausdruck der folgenden Form:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Ein Polynom lässt sich mit dem Summenzeichen auch wie folgt darstellen:

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Als *Grad des Polynoms* bezeichnet man die höchste im Polynom vorkommende Potenz n.

Definition II

Beispiele:

- $a(x) = 2x^2 + 3x - 7$
- $b(x) = -x^3 + 4$
- $c(x) = x^{10} + x^8 - x^6 + 2x^5 + 10x^4 - x + 1$
- $d(x) = 1$

Nullstellen I

Eine *Nullstelle* eines Polynoms p ist ein Wert x_0, für den gilt:

$$p(x_0) = 0.$$

Ein Polynom vom Grad n besitzt höchstens n reelle Nullstellen (und exakt n komplexe Nullstellen) – allerdings besitzt nicht jedes Polynom reelle Nullstellen. Ein Beispiel hierfür ist das folgende *irreduzible Polynom*:

$$x^2 + 1.$$

Hat ein Polynom einen ungeraden Grad, so besitzt es stets mindestens eine reelle Nullstelle.

Nullstellen II

Aufgabe 15

Finde alle (reellen) Nullstellen des folgenden Polynoms:

$$p(x) = 2x^2 - 10x + 12.$$

Nullstellen III

Aufgabe 16

Bestimme ein Polynom $p(x)$ vom Grad 3, dass genau eine reelle Nullstelle, nämlich $x_0 = 42$, besitzt.

Addition & Subtraktion von Polynomen I

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Die Summe $c(x)$ dieser beiden Polynome lässt sich wie folgt berechnen (nicht vorhandene Koeffizienten a_k bzw. b_k haben per Definition den Wert 0):

$$c(x) = a(x) + b(x) = \sum_{k=0}^{\max(m,n)} (a_k + b_k)\, x^k.$$

Addition & Subtraktion von Polynomen II

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Die Differenz $c(x)$ dieser beiden Polynome lässt sich wie folgt berechnen (nicht vorhandene Koeffizienten a_k bzw. b_k haben per Definition den Wert 0):

$$c(x) = a(x) - b(x) = \sum_{k=0}^{\max(m,n)} (a_k - b_k)\, x^k.$$

Addition & Subtraktion von Polynomen III

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = x^3 + 2x^2 - 5x + 3$$
$$b(x) = x^2 + x - 1$$

Hieraus ergibt sich:

$$\begin{aligned} a(x) + b(x) &= x^3 + (2+1)x^2 + (-5+1)x + (3-1) \\ &= x^3 + 3x^2 - 4x + 2 \\ a(x) - b(x) &= x^3 + (2-1)x^2 + (-5-1)x + (3-(-1)) \\ &= x^3 + x^2 - 6x + 4 \end{aligned}$$

Multiplikation von Polynomen I

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Das Produkt dieser beiden Polynome lässt sich auf die folgenden Arten berechnen:

$$a(x) \cdot b(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i \cdot b_j \cdot x^{i+j} \qquad \text{bzw.}$$

$$a(x) \cdot b(x) = \sum_{i=0}^{m+n} \left(x^i \cdot \sum_{k=0}^{i} (a_k \cdot b_{i-k}) \right)$$

Multiplikation von Polynomen II

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = x^3 + 2x^2 - 5x + 3$$
$$b(x) = x^2 + x - 1$$

Hieraus ergibt sich:

$$\begin{aligned} a(x) \cdot b(x) &= x^3 \cdot x^2 + x^3 \cdot x + x^3 \cdot (-1) \\ &\quad + 2x^2 \cdot x^2 + 2x^2 \cdot x + 2x^2 \cdot (-1) \\ &\quad - 5x \cdot x^2 - 5x \cdot x - 5x \cdot (-1) \\ &\quad + 3x^2 + 3x + 3 \cdot (-1) \\ &= x^5 + 3x^4 - 4x^3 - 4x^2 + 8x - 3 \end{aligned}$$

Multiplikation von Polynomen III

Aufgabe 17

Es seien die folgenden beiden Polynome gegeben:

$$a(x) = 2x^3 + 2x^2 + x + 1$$
$$b(x) = x^2 + 2x + 1.$$

Bestimme das Produkt der Polynome $a(x)$ und $b(x)$.

Multiplikation von Polynomen IV

Aufgabe 18

Es seien die folgenden beiden Polynome gegeben:

$$a(x) = x^9 + 2x^7 - 3x^6 + 2x^4 - x^3 + 5x^2 + x - 23$$
$$b(x) = x^{10} - 5x^9 + 2x^6 - 3x^5 - 4x^4 + 2x^3 - x + 42.$$

a) Bestimme den Grad des Polynoms $a(x) \cdot b(x)$.

b) Welchen Koeffizienten besitzt x^{13} im Produkt $a(x) \cdot b(x)$?

Division von Polynomen I

Zu je zwei Polynomen $a(x)$ und $b(x)$ mit $b(x) \neq 0$ gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$ mit $\operatorname{grad}(r(x)) < \operatorname{grad}(b(x))$ oder $r(x) = 0$, so dass

$$a(x) = q(x)b(x) + r(x)$$

gilt. Man nennt dies eine *Zerlegung mit Rest* von $a(x)$ bezüglich $b(x)$.

Division von Polynomen II

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = 2x^4 + x^3 + x + 3$$
$$b(x) = x^2 + x - 1$$

Es folgt:

$$\begin{array}{rllll} & (2x^4 & +x^3 & +x & +3) \quad : (x^2 + x - 1) = 2x^2 - x + 3 \\ - & (2x^4 & +2x^3 & -2x^2) & \\ \hline & & -x^3 & +2x^2 & +x & +3 \\ & - & (-x^3 & -x^2 & +x) & \\ \hline & & & 3x^2 & & +3 \\ & & - & (3x^2 & +3x & -3) \\ \hline & & & & -3x & +6 \end{array}$$

Division von Polynomen III

Als Ergebnis erhält man die folgende Zerlegung mit Rest:

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)}\underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}.$$

Das Ergebnis lässt sich auch wie folgt schreiben:

$$\frac{2x^4 + x^3 + x + 3}{x^2 + x - 1} = 2x^2 - x + 3 + \frac{-3x + 6}{x^2 + x - 1}\ .$$

Division von Polynomen IV

Aufgabe 19

Gegeben seien die beiden folgenden Polynome aus $\mathbb{Q}[x]$:

$$a(x) = 2x^3 + 2x^2 + x + 1$$
$$b(x) = x^2 + 2x + 1.$$

Bestimme den Quotienten $a(x) : b(x)$.

Division von Polynomen V

Aufgabe 20

Gegeben seien die beiden folgenden Polynome aus $\mathbb{Z}_5[x]$:

$$a(x) = 2x^6 + 4x^5 + 3x^4 + 4x^3 + x^2 + 1$$
$$b(x) = 4x^2 + 4.$$

Bestimme den Quotienten $a(x) : b(x)$.

Division von Polynomen VI

Aufgabe 21

Gegeben seien die beiden folgenden Polynome aus $\mathbb{Q}[x]$:

$$a(x) = 2x^3 + 2x^2 + x + 1$$
$$b(x) = x^2 + 2x + 1.$$

Bestimme den normierten größten gemeinsamen Teiler von $a(x)$ und $b(x)$.