Gruppentheorie

Diskrete Strukturen

Uta Priss
ZeLL, Ostfalia

Sommersemester 2016

Agenda

Lesefrage

Aufgaben

Gruppentheorie

Wiederholung: richtig oder falsch?

$(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$

$(A \Longrightarrow B) \Longleftrightarrow \neg A \vee B$

entweder A oder B $\Longleftrightarrow (A \vee B) \wedge (\neg A \vee \neg B) \Longleftrightarrow (\neg A \Longleftrightarrow B)$

$((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$

Wenn man zeigen will, dass $A \Longleftrightarrow B$ muss man zeigen, dass $(A \Longrightarrow B)$ und dass $(B \Longrightarrow A)$.

$(A \Longleftrightarrow B) \Longleftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

$(A \Longleftrightarrow B) \Longleftrightarrow (\neg A \Longleftrightarrow \neg B)$

Lesefrage

„Ich entschuldige mich dafür, dass ich mich hier direkt geäußert habe.“

Kein Problem. Sie dürfen auch Frustration äußern. Sie bekommen trotzdem Ihre Punkte für die Lesefragen. Es ist mir lieber, Sie antworten ehrlich, als dass Sie etwas schreiben, nur weil Sie denken, ich möchte das so lesen.

„Interessant war für mich, wie sich mit den in diesem Bereich vorgestellten Konzepten die grundlegenden Rechenoperationen abstrahieren und verallgemeinern lassen.“

Genau! Darum geht es.

Ihre Fragen

$12 = 7 \pmod 5$

Ist $7 \bmod 5 = 12$ richtig oder falsch?

Sollte es $7 \bmod 5 \equiv 12$ heißen?

Ist b%n==a in SetIX dasselbe wie „$b \bmod n = a$“ in der Mathematik?

Ihre Fragen

- Wieso muss man (K,+,·) schreiben, wenn K sowieso immer + und · hat?
- Beispiel einer Menge mit den Verknüpfungen + und ·, bei der das Distributivgesetz nicht gilt.

Eine Menge $\mathbb{K}$ mit $+$ und $\cdot$ heißt Körper $(\mathbb{K}, +, \cdot)$, wenn
a) $(\mathbb{K}, +)$ eine kommutative Gruppe mit neutralem Element 0 ist.
b) $(\mathbb{K} \setminus \{0\}, \cdot)$ eine kommutative Gruppe mit neutralem Element 1 ist.
c) Das Distributivgesetz gilt: $\forall_{a,b,c \in \mathbb{K}} : a \cdot b + a \cdot c = a \cdot (b + c)$.

Ist $(\mathbb{R}, \cdot, +)$ ein Körper?

Zur Erinnerung

Eine boolesche Algebra $(\mathbb{B}, 1, 0, \vee, \wedge, \neg)$ ist ...

istBooleanAlgebra({true,false}, true, false, oder, und, nicht);

Die Reihenfolge ist wichtig. Daher ist $(\mathbb{R}, \cdot, +)$ kein Körper (Distributivgesetz prüfen).

Ihre Fragen: Inverse

- Das additive Inverse kommt doch in diesem Beispiel gar nicht vor: x = y - 3 = y + 23 (mod 26).
- Ein multiplikatives Inverses ist doch immer eine Kommazahl oder nicht?
- Wenn man Z5 mit 1/2 die Zahl 3 meint, warum schreibt man dann nicht 3?
- Was ist das Additive Inverse von Unendlich in Z?

Ihre Fragen

- Wieso existiert 1/5 in Z6, 1/2 aber nicht?
- Wieso gibt es überhaupt Lösungen, wenn a und m nicht teilerfremd sind?
- Wieso ist Z der Primzahlen eine Multiplikative Gruppe?
- Was genau ist eine Verknüpfung?

(behandeln wir heute oder morgen)

Ihre Fragen

- Und jeder Körper ist ein kommutativer Ring mit 1 oder?
- Ist jeder Körper eine Gruppe, aber nicht jede Gruppe ein Körper?
- Ist der Unterschied von Körper zu Ring, dass es bei Ringen die kommutative Gruppe mit neutralem Element 0 gibt?
- Sind Gebilde, die die Ringaxiome erfüllen, aber andere Operationen haben als $+$ und $\cdot$ trotzdem Ringe?
- Definition des Ringes gern etwas genauer erläutert bekommen.
- Beispiel zum Ring? (Polynome, nicht klausurrelevant)
- Ideal (nicht klausurrelevant)

Eine Menge $\mathbb{K}$ mit $+$ und $\cdot$ heißt Körper $(\mathbb{K}, +, \cdot)$, wenn
a) $(\mathbb{K}, +)$ eine kommutative Gruppe mit neutralem Element 0 ist.
b) $(\mathbb{K} \setminus \{0\}, \cdot)$ eine kommutative Gruppe mit neutralem Element 1 ist.
c) Die Distributivgesetze gelten: $\forall_{a,b,c \in \mathbb{K}} : a \cdot b + a \cdot c = a \cdot (b + c)$ und $a \cdot c + b \cdot c = (a + b) \cdot c$.

Eine Menge $\mathbb{K}$ mit $+$ und $\cdot$ heißt Ring $(\mathbb{K}, +, \cdot)$, wenn
a) $(\mathbb{K}, +)$ eine kommutative Gruppe mit neutralem Element 0 ist.
b) Das Assoziativgesetz gilt: $\forall_{a,b,c \in \mathbb{K}} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
c) Die Distributivgesetze gelten: $\forall_{a,b,c \in \mathbb{K}} : a \cdot b + a \cdot c = a \cdot (b + c)$ und $a \cdot c + b \cdot c = (a + b) \cdot c$.

Was ist der Unterschied zwischen Körper und Ring?
Was ist die Beziehung zwischen Gruppe, Ring und Körper?

Ihre Fragen

- Und jeder Körper ist ein kommutativer Ring mit 1 oder?
- Ist jeder Körper eine Gruppe, aber nicht jede Gruppe ein Körper?
- Ist der Unterschied von Körper zu Ring, dass es bei Ringen die kommutative Gruppe mit neutralem Element 0 gibt?
- Sind Gebilde, die die Ringaxiome erfüllen, aber andere Operationen haben als $+$ und $\cdot$ trotzdem Ringe?

LON-CAPA Aufgabe: Gruppenaxiome

Definition des neutralen Elements: $n \circ a = a \circ n = a$.

Gibt es ein neutrales Element für die Potenzierung, Division und Subtraktion?

Kann es ein Inverses geben, wenn es kein neutrales Element gibt?

Fehler in den SetIX-Aufgaben

- Syntax Fehler: } zu viel, „else“ fehlt, & statt %, \ statt (
- Ist b%n==a in SetIX dasselbe wie „b mod $n = a$“ in der Mathematik?
- isprime: falscher Algorithmus
- Schreibfehler: ggT statt ggt
- „Mein SetIX startet nicht mehr“

Wenn Sie noch Fragen bezüglich der Aufgaben (LON-CAPA oder SetIX) haben, sprechen Sie mich nach der Vorlesung an oder fragen Sie im Mathe-Cafe donnerstags früh.

Schreiben Sie diesen Satz als Formel

Für $e \neq 0$ in $\mathbb{Z}_m$ gilt: Es gibt (genau) ein multiplikatives Inverses genau dann, wenn e und m teilerfremd sind.

(Für das multiplikative Inverse können Sie e^{-1} schreiben.)

Schreiben Sie diesen Satz als Formel

Für $e \neq 0$ in $\mathbb{Z}_m$ gilt: Es gibt (genau) ein multiplikatives Inverses genau dann, wenn e und m teilerfremd sind.

Lösungen:

$\forall_{e \neq 0, e \in \mathbb{Z}_m} : \exists_{e^{-1}} \iff ggT(e, m) = 1$

$\forall_{e \neq 0, e \in \mathbb{Z}_m} : |\{n \in \mathbb{Z}_m \mid n = e^{-1}\}| = 1 \iff ggT(e, m) = 1$

Erklären Sie dies. Benutzen Sie dabei Beispiele

$a + x = b \bmod m$ ist eindeutig lösbar in $\mathbb{Z}_m$. Man erhält die Lösung so: $x = (-a) + b \bmod m$.

Wenn a und m teilerfremd sind, dann ist $a \cdot x = b \bmod m$ eindeutig lösbar in $\mathbb{Z}_m$ und man erhält die Lösung so: $x = a^{-1} \cdot b \bmod m$.

Wenn $t = ggT(a, m)$, gibt es genau t Lösungen von $a \cdot x = b \bmod m$, falls $ggT(b, t) = t$, ansonsten gibt es keine Lösungen.

Wieso gilt $\mathbb{Z}_p^\star = \mathbb{Z}_p \setminus \{0\}$?

Schreiben Sie die Verknüpfungstafel für $\mathbb{Z}_7^\star$.

Zeigen Sie, dass $\mathbb{Z}_7^\star$ eine Gruppe ist.
Ist es eine kommutative Gruppe?

Abgeschlossenheit

Die erste Eigenschaft einer Gruppe lautet: für $a, b \in G$ gilt $a \circ b \in G$. Diese Eigenschaft heißt Abgeschlossenheit.

Warum braucht man diese Bedingung? Finden Sie Beispiele, die diese Bedingung nicht erfüllen.

Eine Teilmenge $H \subseteq G$ heißt Untergruppe wenn $(H, \circ)$ selbst eine Gruppe ist. Was muss man insbesondere prüfen?

Verknüpfungstafeln: Welches sind Gruppen? Welche Eigenschaften fehlen eventuell?

	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

	c	a	b
a	a	b	c
b	b	c	a
c	c	a	b

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	d	e	c
b	b	1	a	e	c	d
c	c	e	d	1	b	a
d	d	c	e	a	1	b
e	e	d	c	b	a	1

	1	a	b	c
1	1	a	b	c
a	a	b	c	d
b	b	c	d	e
c	c	d	e	f

	1	a	b
1	1	a	b
a	a	1	a
b	b	b	1

Satz: In der Verknüpfungstafel einer Gruppe steht jedes Element jeweils 1-mal in jeder Zeile und Spalte.

Annahme: ein Element steht zweimal in einer Zeile:
$a = b + c$ und $a = b + d \Longrightarrow$
$b + c = b + d \Longrightarrow$
$-b + b + c = -b + b + d \Longrightarrow$
$c = d$

Erklären Sie den Beweis. Was ist das für ein Beweisverfahren?

Wiederholung: Definition von Relationen und Funktionen

Relation $r_{\leq}$

$r_{\leq} \subseteq \mathbb{R} \times \mathbb{R}$
$(a, b) \in r_{\leq} :\Longleftrightarrow a \leq b$

Funktion x^2

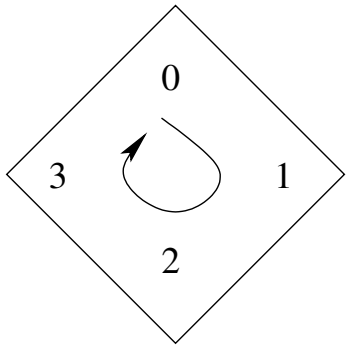
$f : \mathbb{R} \to \mathbb{R}^{\geq 0}$
$x \mapsto x^2$

oder:

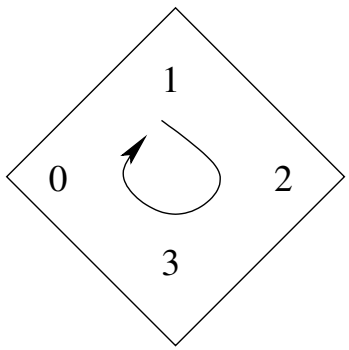
$f : \mathbb{R} \to \mathbb{R}^{\geq 0}$
$f(x) := x^2$

Schreiben Sie eine Verknüpfung (z.B. $+$) als Funktion auf.

Rotation des Quadrats



(0,1,2,3)



(1,2,3,0)

Wie viele Elemente gibt es?
Definieren Sie eine Funktion, die das Quadrat jeweils um 90° dreht.
Schreiben Sie die Verknüpfungstafel auf.
Handelt es sich um eine Gruppe?