Ferienkurs Mathematik für Physiker I
Musterlösung für Übungsblatt 1
(27.3.2017)

Aufgabe 1: Eigenschaften von Gruppen

Wir betrachten eine Gruppe $(G, \circ)$.

(a) Listen Sie die von G erfüllten Gruppenaxiome auf. Welches zusätzliche Axiom ist für abelsche Gruppen erfüllt?

Lösung: Die Gruppenaxiome sind

(i) $\forall a, b \in G : a \circ b \in G$

(ii) $\exists e \in G \forall a \in G : a \circ e = e \circ a = a$

(iii) $\forall a \in G \exists a^{-1} \in G : a^{-1} \circ a = e$

(iv) $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$

(b) Zeigen Sie unter Benutzung der Gruppenaxiome aus a) folgende allgemeine Eigenschaften von Gruppen:

(i) Eindeutigkeit des inversen Elements für jedes $a \in G$

(ii) Eindeutigkeit des neutralen Elements e

(iii) $\forall a, b, c \in G \, : \, a \circ b = a \circ c \Rightarrow b = c$

Lösung:

(i) Seien a^{-1} und $\tilde{a}^{-1}$ zwei inverse Elemente für a. Es gilt

$$a^{-1} = a^{-1} \circ a \circ \tilde{a}^{-1} = \tilde{a}^{-1}$$

(ii) Seien e und $\tilde{e}$ zwei neutrale Elemente. Es gilt

$$e = e \circ \tilde{e} = \tilde{e}$$

(iii) Es gilt

$$a \circ b = a \circ c \Leftrightarrow a^{-1} \circ a \circ b = a^{-1} \circ a \circ c \Leftrightarrow b = c$$

(c) Warum gilt Eigenschaft (iii) nicht für die Multiplikation in $\mathbb{R}$ oder einem anderen Körper?

Lösung: In einem Körper gilt $a \cdot 0 = 0$ für alle $a \in G$, sodass die Eigenschaft (iii) nur erfüllt ist für $a \neq 0$.

Aufgabe 2: Untergruppen und Linksnebenklassen

Sei G eine Menge und $\circ : G \times G \to G$ eine zweistellige Verknüpfung, sodass $(G, \circ)$ eine Gruppe bildet. Im folgenden betrachten wir Tupel $(H, \circ)$, wobei H jeweils eine Teilmenge von G ist.

(a) Welche Axiome müssen erfüllt sein, damit es sich bei $(H, \circ)$ um eine Untergruppe von $(G, \circ)$ handelt?

Lösung: $(H, \circ)$ muss die Gruppenaxiome erfüllen. Da $(G, \circ)$ bereits eine Gruppe ist, ist Assoziativität von $\circ$ bereits automatisch erfüllt und das neutrale Element $e \in G$ existiert. An nicht-trivialen Eigenschaften verbleiben

(i) $a \in H \Rightarrow a^{-1} \in H$

(ii) $e \in H$

(iii) $a, b \in H \Rightarrow a \circ b \in H$

(b) Zeigen Sie, dass $(H, \circ)$ genau dann eine Untergruppe von $(G, \circ)$ ist, wenn

$$\forall a, b \in H : a \circ b^{-1} \in H. \tag{1}$$

Lösung:

„$\Rightarrow$“: H ist eine Untergruppe. Seien nun $a, b \in H$. Wegen (i) ist b^{-1} in H und damit wegen (iii) auch $a \circ b^{-1}$.

„$\Leftarrow$“: Für alle $a, b \in H$. ist $a \circ b^{-1}$ in H. Insbesondere ist also $e = a \circ a^{-1}$ in H und damit auch $a^{-1} = e \circ a^{-1}$. (i) und (ii) sind also erfüllt und $b^{-1} \in H$. Damit ist schließlich auch $a \circ b = a \circ \left(b^{-1}\right)^{-1}$ in H.

(c) Sei $a \in G$ ein Element von G. Wenn H eine Untergruppe ist, so heißt die Menge $aH := \{a \circ h | h \in H\}$ „Linksnebenklasse“ von a. Zeigen Sie folgende Eigenschaften von Linksnebenklassen:

(i) $eH = H$, wobei e das neutrale Element in G ist.

(ii) $a \in H \Leftrightarrow aH = H$

(iii) $aH = bH \Leftrightarrow b^{-1} \circ a \in H$

Lösung:

(i) Es gilt $eH = \{e \circ h | h \in H\} = \{h | h \in H\} = H$.

(ii) Es sei $g \in aH$. Da $a \in H$ gilt auch $g \in H$, woraus folgt dass $aH \subseteq H$. Andererseits ist aber auch $H \subseteq aH$, da $h = a \circ \left(a^{-1} \circ h\right)$ mit $a^{-1} \circ h \in H$. Folglich gilt $H = aH$.

(iii) „$\Rightarrow$“: $aH = bH$ impliziert, dass für ein $h \in H$ die Identität $a = b \circ h$ bzw. $b^{-1} \circ a = h \in H$ gilt.
„$\Leftarrow$“: Aus $b^{-1} \circ a \in H$ folgt direkt $a \in bH$, und damit $aH \subseteq bH$. Andererseits gilt auch $a^{-1} \circ b \in H$, da H eine Gruppe ist, und damit auf analoge Weise $bH \subseteq aH$. Folglich ist $aH = bH$.

(d) **Bonusfrage:** Zeigen Sie, dass es sich bei der Relation $a \sim b \Leftrightarrow b^{-1} \circ a \in H$ genau dann um eine Äquivalenzrelation handelt, wenn H eine Untergruppe von G ist.

Lösung:

„$\Rightarrow$“: Wenn H keine Untergruppe von G ist, existieren $a, b \in H$, sodass $a \circ b^{-1} \notin H$. Damit kann $\sim$ keine Äquivalenzrelation sein, da $a \sim e \sim b$ aber nicht $a \sim b$ gilt und $\sim$ also nicht transitiv ist.

„$\Leftarrow$“: Es sei H eine Untergruppe von G. Dann ist $\sim$ reflexiv, da $a^{-1} \circ a = e \in H$. $\sim$ ist weiterhin symmetrisch und transitiv, da $b^{-1} \sim a \in H \Leftrightarrow a^{-1} \circ b \in H$ und ausserdem für $c^{-1} \circ b \in H$ und $b^{-1} \circ a \in H$ auch $c^{-1} \circ b \circ b^{-1} \circ a = c^{-1} \circ a \in H$ gilt.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

TABELLE 1: Additionstabelle für Aufgabe 3

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

TABELLE 2: Multiplikationstabelle für Aufgabe 3

Aufgabe 3: Polynome über allgemeinen Körpern

Die Menge $G = \{0, 1, a, b\}$ bildet zusammen in der in den Tabellen 1 und 2 gezeigten Addition $+$ und Multiplikation $\cdot$ einen Körper. Es lässt sich über $(G, +, \cdot)$ also insbesondere auch mit Polynomen rechnen.

(a) Sei $x \in G$ eine Unbekannte. Finden Sie die Nullstellen der folgenden Gleichungen :

(i) $0 = x + b$

(ii) $1 = x^3$

(iii) $0 = x^2 + bx + a$

(iv) $1 = x^6 + bx^4 - a$

Lösung:

(i) Aus der Additionstabelle ist ersichtlich, dass $x = -b = b$.

(ii) Aus der Multiplikationstabelle kann man ablesen, dass $1^3 = a^3 = b^3 = 1$, also erhält man als Lösungen $x_1 = 1$, $x_2 = a$, und $x_3 = b$.

(iii) Aus der Mutliplikationstabelle ist ersichtlich, dass $ab = 1$ und $a^2 = a + 1 = b$. Durch Ausprobieren erhält man damit die beiden Lösungen $x_1 = 1$ und $x_2 = a$.

(iv) Aufgrund von $x^3 = 1$ für alle $x \neq 0$ ist die Gleichung equivalent zu $1 = 1 + bx - a$ bzw. $a = bx$. Aus der Multiplikationstabelle ließt man als also die Lösung $x = a$ ab.

(b) Zeigen Sie, dass für alle $x, y \in G$ die Identität $(x + y)^2 = x^2 + y^2$ gilt. *Hinweis:* Benutzen Sie, dass die Hauptdiagonale der Additionstabelle nur aus Nullen besteht.

Lösung: Aus der Hauptdiagonalen der Additionstabelle kann man ablesen, dass $\forall x \in G : x = -x$. Damit erhält man $(x + y)^2 = x^2 + y^2 + yx + xy = x^2 + y^2$.

Aufgabe 4: Restklassenringe

In der Vorlesung wurde die Menge der ganzen Zahlen $\mathbb{Z}$ zusammen mit der Standart-Addition als Beispiel für eine Gruppe genannt. Hier betrachten wir anstatt von $\mathbb{Z}$ die Menge $\mathbb{Z}_p$ der natürlichen Zahlen kleiner p für ein gegebenes $p \in \mathbb{N}$.

(a) Zeigen Sie, dass $\mathbb{Z}_p$ zusammen mit der Addition $+$ modulo p eine Gruppe bildet. Welche Eigenschaften müssen Sie hierfür überprüfen?

Lösung: Es müssen die Gruppenaxiome überprüft werden. $\mathbb{Z}_p$ ist abgeschlossen bezüglich der Addition modulo p, da der Rest bei division durch p kleine p sein muss, und assoziativ da die Standartaddition assoziativ ist. Die Null ist das neutrale Element, da für alle $n \in \mathbb{N} : n \equiv n + 0 \bmod p$. Das inverse Element für $n \in \mathbb{N}$ ist $p - n$, da $n + p - n \equiv 0 \bmod p$.

(b) Warum kann $\mathbb{Z}_p$ zusammen mit der Multiplikation $\cdot$ modulo p keine Gruppe bilden? Zeigen Sie, dass $\cdot$ auf $\mathbb{Z}_p$ assoziativ ist und ein neutrales Element besitzt!

Lösung: Die Multiplikation modulo p ist assoziativ, da die Standartmultiplikation assoziativ ist. Das neutrale Element ist 1, da für alle $n \in \mathbb{N} : n \equiv 1 \cdot n \bmod p$. Da aber die Null bezüglich der Multiplikation kein inverses Element besitzt, kann $(\mathbb{Z}_p, \cdot)$ keine Gruppe bilden.

(c) Man definiert $\mathbb{Z}_p^*$ als die Menge der *positiven* Zahlen kleiner p. Bilden die Mengen $\mathbb{Z}_3^*$, $\mathbb{Z}_4^*$, und $\mathbb{Z}_6^*$ mit der Multiplikation modulo p jeweils eine Gruppe? Begründen Sie!

Lösung: Aus dem vorherigen Aufgabenteil ist bekannt, dass die Multiplikation modulo p assoziativ ist und alle drei Mengen ein neutrales Element besitzen. Es verbleibt zu überprüfen, ob die Mengen abgeschlossen sind und jeweils alle Elemente ein Inverses besitzen.
Für $\mathbb{Z}_4^*$ gilt $2 \cdot 2 \equiv 0 \bmod 4$ und für $\mathbb{Z}_6^*$ gilt $2 \cdot 3 \equiv 0 \bmod 6$, beide Mengen sind also nicht abgeschlossen und damit keine Gruppen.
Für $\mathbb{Z}_3^*$ ist aus der vorherigen Aufgabe bekannt, dass 1 das neutrale Element ist. Da weiterhin $2 \cdot 2 \equiv 1 \bmod 3$ ist die Menge abgeschlossen und jedes Element besitzt ein Inverses. $\mathbb{Z}_3^*$ ist also eine Gruppe.

(d) **Bonusfrage:** Sei p nun eine Primzahl. In diesem Fall gilt für jedes $a \in N$, dass

$$a^{p-1} \equiv 1 \bmod p. \tag{2}$$

Diese Aussage ist bekannt als der „kleine Satz des Fermat“. Was implizert Gleichung 2 für $\left(\mathbb{Z}_p^*, \cdot\right)$?

Lösung: Der kleine Satz des Fermat ist gleichbedeutend damit, dass jedes a in $\mathbb{Z}_p^*$ ein inverses Element besitzt. Damit ist sichergestellt, dass $\left(\mathbb{Z}_p^*, \cdot\right)$ eine Gruppe bildet.