Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 2

Aufgabe 1 (4 Punkte)
Seien $A_1 = \{1, ..., d\}$ (für $d \in \mathbb{N}$ beliebig, aber fest), $A_2 = \mathbb{Z}$. Beide Mengen werden durch die Verknüpfung $x \bullet y = \min(x, y)$ zu einem Magma.
Zeige, dass A_1 und A_2 sogar Halbgruppen sind. Sind es sogar Monoide? Gib gegebenenfalls das neutrale Element und alle invertierbaren Elemente an.
Bestimme nun für $i = 1, 2$ die Magmen-Automorphismen von A_i.

Lösung:
In beiden A_i gilt: $(x \bullet y) \bullet z = \min(x, y, z) = x \bullet (y \bullet z)$, wie man etwa leicht durch eine Fallunterscheidung (8 Fälle, etwa $x \leq y \leq z$, dann...) einsieht.
In $A_2 = \mathbb{Z}$ gibt es kein neutrales Element, für beliebiges $z \in \mathbb{Z}$ ist zum Beispiel $z \bullet (z + 1) = z \neq z + 1$, also z nicht neutral.
In A_1 ist d neutrales Element, denn $d \bullet x = x \bullet d = \min(d, x) = x$ für alle x. Für $x < d$ gilt aber für alle y: $x \bullet y = \min(x, y) \leq x < d \Rightarrow x \bullet y \neq d$, also ist x nicht invertierbar. Die Einheitengruppe ist trivial.

Schließlich suchen wir alle Magmenautomorphismen, zur Erinnerung, dies sind die bijektiven Homomorphismen. Sowohl in A_1 als auch A_2 gilt für einen Homomorphismus φ:
$x \leq y \overset{x=\min(x,y)}{\Rightarrow} \varphi(x) = \varphi(x \bullet y) = \varphi(x) \bullet \varphi(y) = \min(\varphi(x), \varphi(y)) \Rightarrow \varphi(x) \leq \varphi(y)$.
φ ist also monoton, für einen Automorphismus φ liegt sogar strenge Monotonie vor.
Andersherum ist auch jede monotone Abbildung ein Homomorphismus, wie man leicht einsieht.

Die Automorphismen von sind also (in beiden Fällen) gerade die bijektiven, streng monotonen Abbildungen.

Auf A_1 gibt es offensichtlich nur eine streng monotone Abbildung. Dies ist die Identität, die der einzige Automorphismus von A_1 ist: $\mathrm{Aut}(A_1) = \{\mathrm{id}\}$.

Behauptung: Die bijektiven, streng monotonen Abbildungen auf $\mathbb{Z}$ sind gerade die Translationen, diese bilden dann die Automorphismengruppe.
Beweis der Behauptung: Dass Translationen $x \mapsto x + t$ für ein festes $t \in \mathbb{Z}$ bijektiv und streng monoton, also Automorphismen sind, ist offensichtlich, oder?
Sei nun φ ein Automorphismus von $(\mathbb{Z}, \bullet)$. φ ist eine Translation, wenn $\varphi(x) - x$ für alle x den gleichen Wert liefert, offensichtlich reicht es aus, dies für benachbarte ganze Zahlen zu zeigen.
Sei dazu $x \in \mathbb{Z}$ beliebig mit $\varphi(x) = x + t$ (wobei t einfach als $t := \varphi(x) - x$ berechnet wird). Wegen der Monotonie ist sicher $\varphi(x + 1) \geq x + 1 + t$, wir nehmen an, es sei echt größer.
Wegen der Monotonie gilt dann aber $\varphi(y) \leq x + t$ für alle $y \leq x$ und $\varphi(y) > x + 1 + t$ für alle $y \geq x + 1$, so dass $x + 1 + t$ in diesem Fall nicht im Bild von φ liegen kann, was als surjektiv vorausgesetzt war. WIDERSPRUCH
Also ist $\varphi(x + 1) = x + 1 + t$, womit die Behauptung bewiesen wäre.

Aufgabe 2 (4 Punkte)
Wir betrachten das Magma $M = (\mathbb{Z}, -)$.

a) Zeige, dass M keine Halbgruppe ist. Zeige weiterhin, dass M kein neutrales Element besitzt. Gib gegebenenfalls ein links- bzw. rechtsneutrales Element an und folgere daraus, dass M nicht kommutativ ist.

b) Finde ein Erzeugendensystem von M, so dass es kein Erzeugendensystem mit weniger Elementen gibt. Wieviele solcher Systeme gibt es?

c) Zeige, dass $(\mathrm{End}(M), \circ) \simeq (\mathbb{Z}, \cdot)$ ist.

Lösung Aufgabe 2

a) Es ist $(1-1)-1 = -1 \neq 1 = 1-(1-1)$. Die Verknüpfung ist also nicht assoziativ und somit ist M keine Halbgruppe.

Für ein linksneutrales Element e muss insbesondere gelten $e-1 \overset{(!)}{=} 1$, also verbleibt nur $e = 2$ als Kandidat. Wegen $2-2 = 0 \neq 2$ ist dies nicht linksneutral, es gibt also insbesondere kein neutrales Element.

Wegen der Forderung $1 - e \overset{(!)}{=} 1$ verbleibt nur $e = 0$ als mögliches rechtsneutrales Element und wegen $x - 0 = x$ für alle x ist dies auch tatsächlich rechtsneutral.
Wäre M abelsch, so wäre jedes rechtsneutrale Element auch linksneutral, M kann also nicht abelsch sein. (Das hätten wir natürlich auch direkt durch ein Gegenbeispiel zeigen können.)

b) $\{1\}$ ist ein solches Erzeugendensystem. Wegen $-1 = (1-1)-1$ ist auch -1 in $< 1 >$ enthalten und schließlich für alle $n \in \mathbb{N}$ $n = (1-(-1))-(-1)...$ mit $n-1$ Subtraktionen von -1. Für $z \in \mathbb{Z} \setminus \mathbb{N}$ ist $z = (((1-1)-1)-1...)$ mit $-z-1$ Subtraktionen der 1.
Jedes Element lässt sich also aus der 1 darstellen, dies ist gerade die Anforderung an ein Erzeugendensystem. Ein kleineres System müsste leer sein und kann also nicht erzeugend sein.
$\{-1\}$ ist ein weiteres solches System: Wegen $1 = (-1-(-1))-(-1)$ sind 1 und -1 in $< -1 >$ und dass $< -1 >= \mathbb{Z}$ zeigt man wie im obigen Fall.
Dies sind alle, denn 0 ist offensichtlich kein Erzeuger und alle Elemente aus $< m >$ mit $|m| \geq 2$ sind ganzzahlige Vielfache von m, also insbesondere $1 \notin < m >$. Es gibt somit genau zwei solcher Erzeugendensysteme mit minimaler Mächtigkeit.

c) Definiere $\psi : (\mathbb{Z}, \cdot) \to (\mathrm{End}(M), \circ)$ mit $\psi(x)(a) = xa$. ($\psi(x) : \mathbb{Z} \to \mathbb{Z}$ ist also die Multiplikation mit x.)
Man rechnet für beliebiges $x \in \mathbb{Z}$ nach, dass $\psi(x)(a-b) = x(a-b) = xa - xb = \psi(x)(a) - \psi(x)(b)$ für alle $a, b \in M$ gilt, $\psi(x)$ ist also ein Endomorphismus von M, das heißt, ψ ist wohldefiniert.
Zu zeigen verbleibt, dass ψ ein bijektiver Homomorphismus ist:

Seien $x, y \in \mathbb{Z}$ beliebig, zu zeigen ist $\psi(x \cdot y) \overset{(!)}{=} \psi(x) \circ \psi(y)$. Sei dazu $a \in \mathbb{Z}$ beliebig, dann gilt:
$\psi(x \cdot y)(a) = (x \cdot y) \cdot a = x \cdot (y \cdot a) = \psi(x)(\psi(y)(a)) = (\psi(x) \circ \psi(y))(a)$.

Seien $x, y \in \mathbb{Z}$ mit $\psi(x) = \psi(y)$, dann ist $x = x \cdot 1 = \psi(x)(1) = \psi(y)(1) = y \cdot 1 = y$, also ist ψ injektiv.

Sei schließlich $\varphi \in \mathrm{End}(M)$ beliebig, zu zeigen ist, dass es ein $x \in \mathbb{Z}$ gibt mit $\varphi = \psi(x)$. Dann ist ψ surjektiv. Wegen $\varphi(1) \overset{(!)}{=} \psi(x)(1) = x$ bleibt nur die Möglichkeit $x = \varphi(1)$.
An dieser Stelle sind wir im Grunde schon fertig. φ und $\psi(\varphi(1))$ sind beides Endomorphismen, die auf dem Erzeugendensystem $\{1\}$ übereinstimmen. Da die Angabe auf einem Erzeugendensystem einen Homomorphismus höchstens eindeutig festlegt, müssen sie gleich sein.
Wer das lieber etwas grundlegender haben will, rechnet elementweise nach, dass $\varphi = \psi(\varphi(1))$ ist. Zu zeigen ist dann also, dass für alle $z \in M$ gilt: $\varphi(z) = \varphi(1) \cdot z$.
Für den Fall $z = 1$ stimmt die Aussage, ebenso für $z = 0$ wegen $\varphi(0) = \varphi(1-1) = \varphi(1) - \varphi(1) = 0 = \varphi(1) \cdot 0$.
Diese beiden Fällen dienen als Induktionsanfänge.
Sei nun zunächst $z \geq 2$ gegeben. Sei die Aussage richtig für $z-1$. Dann ist
$\varphi(z) = \varphi((z-1)-(0-1)) = \varphi(z-1) - (\varphi(0) - \varphi(1)) = \varphi(1) \cdot (z-1) - (0 - \varphi(1)) = \varphi(1) \cdot z$.
Ähnlich folgt der Fall für $z \leq -1$. Sei die Aussage richtig für $z+1$. Dann ist $\varphi(z) = \varphi((z+1)-1) = \varphi(z+1) - \varphi(1) = \varphi(1) \cdot (z+1) - \varphi(1) \cdot 1 = \varphi(1) \cdot z$.

Aufgabe 3 (8 Punkte)
Diese Aufgabe bietet ein kleines Sammelsurium an Aufgaben über Gruppen und Co. Die einzelnen Teilaufgaben können problemlos unabhängig voneinander bearbeitet werden.

a) Finde eine Halbgruppe G, die mindestens zwei linksneutrale Elemente, aber kein rechtsneutrales Element besitzt.

b) Zeige, dass es (bis auf Isomorphie) genau zwei Gruppen mit 4 Elementen gibt. (*Hinweis:* Wie sehen die Verknüpfungstafeln dieser Gruppen aus?)

c) G sei ein Monoid mit neutralem Element e. Es gelte $x^2 = e$ für alle $x \in G$. Zeige, dass G eine abelsche Gruppe ist.

d) Sei G ein endliches Monoid mit Linkskürzungsregel, das heißt, für $a, x, y \in G$ gelte $ax = ay \Rightarrow x = y$. Zeige, dass G eine Gruppe ist.
Finde ein Beispiel, das zeigt, dass die Aussage für unendliches G im Allgemeinen falsch ist.

e) Sei G eine Halbgruppe. Es gebe ein linksneutrales Element $e \in G$. Weiterhin gebe es für alle $g \in G$ ein $h \in G$ mit $hg = e$. Zeige, dass G dann bereits eine Gruppe ist.

Lösung Aufgabe 3

a) Wir finden eine ganz allgemeine Lösung, die natürlich einfach konkretisiert werden kann. Wähle M beliebig mit $|M| \geq 2$ und setze $x \cdot y = y$ für alle $x, y \in M$. Dies definiert eine Magmenstruktur, die wegen $x \cdot (y \cdot z) = x \cdot z = z = y \cdot z = (x \cdot y) \cdot z$ für alle $x, y, z \in M$ assoziativ ist.
Offensichtlich ist jedes Element linksneutral nach Definition von $\cdot$, aber keines ist rechtsneutral, denn für $x \in M$ finden wir $y \in M, y \neq x$ und wegen $yx = x \neq y$ ist x nicht rechtsneutral.

b) Ohne Einschränkung heißen die Elemente e, a, b, c wobei e das neutrale Element ist.

Hinweis: Wir verwenden den Satz von Lagrange, den wir erst gelernt haben, nachdem das Übungsblatt herausgegeben war. Der Satz besagt, dass jedes Element eine Ordnung hat, die vier teilt. Die Aufgabe ist auch ohne diesen Satz lösbar, ist dann aber etwas umständlicher aufzuschreiben.

Fall 1: Es gibt ein Element der Ordnung 4, ohne Einschränkung sei dies a. Dann ist $G = \{a, a^2, a^3, e\}$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Es gibt also nur eine Gruppe (bis auf Isomorphie) mit einem Element der Ordnung 4.

Fall 2: a, b, c haben alle Ordnung 2. Wir stellen die Verknüpfungstafel einer solchen Gruppe so weit wie möglich auf:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Jetzt verwenden wir, dass in jeder Zeile jedes Element genau einmal steht, denn:
$xy = xz \Rightarrow y = z$, wie Multiplikation von links mit x^{-1} zeigt, also steht jedes Element in jeder Zeile höchstens einmal; aber für $x, y \in G$ beliebig ist $x(x^{-1}y) = y$, also steht auch jedes Element mindestens einmal in jeder Zeile. Das Argument geht für die Spalten analog.
Damit können wir die Tafel bereits vollständig ausfüllen:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tatsächlich müssen wir noch zeigen, dass die letzte Struktur eine Gruppe ist, zu zeigen wäre die Assoziativität. Wir haben aber in jedem Fall gezeigt, dass es höchstens zwei Gruppen mit 4 Elementen geben kann, aber mit $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (wobei in letzterer kein Element der Ordnung 4 existiert, also keine isomorphen Gruppen vorliegen) haben wir zwei verschiedene Gruppen gefunden. Wir können folgern, dass sie zweite Verknüpfungstafel die Tafel zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sein muss, was man auch schnell rechnerisch einsieht.

c) Jedes Element besitzt ein Inverses, nämlich sich selbst. Damit ist G eine Gruppe.
Für $x, y \in G$ gilt: $(xy)(xy) = e$ und $x(yy)x = xx = e$, also gilt $xyxy = xyyx$, wobei aufgrund der Assoziativität die Klammerung weggelassen werden kann. Da in Gruppen die Kürzungsregel gilt, erhalten wir - durch Multiplikation mit dem Inversen von xy von links - die Gleichung $xy = yx$, die Gruppe ist also abelsch, denn x, y waren beliebig.

d) Sei $g \in G$ beliebig. Die Zuordnung $h \mapsto gh$ ist eine Abbildung von G nach G, die wegen der Linkskürzungsregel injektiv ist: $gh = gh' \Rightarrow h = h'$. Da G endlich ist, muss die Abbildung auch surjektiv sein, insbesondere gibt es also ein Rechtsinverses h mit $gh = e_G$.
Es reicht zu zeigen, dass h auch linksinvers zu g ist, das also auch $hg = e_G$ gilt. Auf jeden Fall gibt es - mit der gleichen Begründung wie oben - ein Rechtsinverses g' zu h. Aber dann gilt $g = g(hg') = (gh)g' = g'$, was zu zeigen war.

Ein bekanntes Gegenbeispiel ist $(\mathbb{Z} \setminus \{0\}, \cdot)$. Das ist keine Gruppe, aber die Kürzungsregeln gelten. Dafür mussten wir auch die 0 ausschließen.

e) Sei g beliebig. Dann besitzt g ein Linksinverses g', das wiederum ein Linksinverses g'' besitzt, aber wir haben $g'' = g''(g'g) = (g''g')g = g$.
Also ist wegen $g'g = e$ und $gg' = g''g' = e$ das Element g' sogar ein (richtiges) Inverses zu g. (Dabei sollten wir mit dem Begriff „invers“ noch ein wenig vorsichtig sein, solange wir kein (richtiges) Neutralelement haben, „invers“ ist selbstverständlich bezüglich des linksneutralen Elements e gemeint.)
Nun sei g beliebig mit Inversem g^{-1}, dann ist $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$, also ist e auch rechtsneutral.
Insgesamt folgt, dass G eine Gruppe ist.

Abgabe der Übungsblätter:
Bitte beachte, dass die Übung am 1.5. wegen Feiertag ausfällt. Bitte wirf deine Lösung zu diesem Übungsblatt bis Mittwoch, 2. Mai, 9:30 Uhr, in den entsprechenden Abgabekasten im 1C-Teil des Allianzgebäudes.
Ein neues Übungsblatt erhältst du ab dem 1.5. auf der Vorlesungswebseite, dort findest du auch eine Musterlösung zu diesem Blatt.