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

Einführung in Algebra und Zahlentheorie – Übungsblatt 3 – Musterlösung

Aufgabe 1 (4 Punkte)
Sei $M = \{a, b, c\}$ (mit a, b, c paarweise verschieden) eine Menge mit genau drei Elementen. Gib – falls möglich – eine Verknüpfung $*$ auf M an, so dass

a) M ein Magma, aber keine Halbgruppe ist.

b) M eine Halbgruppe, aber kein Monoid ist.

c) M ein Monoid, aber keine Gruppe ist.

d) M eine Gruppe ist.

Zeige gegebenenfalls, dass eine solche Verknüpfung nicht existiert. Führe Nachweise, dass M die entsprechende algebraische Struktur besitzt, aus, verliere dich dabei aber nicht im Detail. Gib jeweils ein Gegenbeispiel an, dass die Verknüpfung nicht die nächsthöhere Anforderung erfüllt.

Lösung: Es gibt alle geforderten Strukturen. Wir müssen solche angeben und zeigen, dass sie tun, was sie tun sollen.
Dabei können wir – falls bekannt – auf bekannte Strukturen zurückgreifen, dann müssen wir wenig beweisen. Wir können aber auch eine Verknüpfungstafel hinschreiben: Dieser sieht man direkt die Magmenstruktur an (alle Einträge in der Tafel müssen a, b, c sein), die Existenz (oder Nichtexistenz) eines Neutralelements und wenn es ein solches gibt – und wenn wir genau hinschauen – auch, ob es Inverse gibt. Die Assoziativität sehen wir leider nicht so direkt.

a) Als erstes Beispiel schreiben wir eine beliebige Verknüpfungstafel hin, die nicht assoziativ ist. Das schöne ist, dass wir für ein Magma keinerlei Bedingungen an die Tafel stellen.
Zum Beispiel könnte $a * a = b$ und dann $(a * a) * a = b * a = c$ und $a * (a * a) = a * b = a$ sein. Die restlichen Einträge können wir mit beliebigen Einträgen aus a, b, c auffüllen:

$*$	a	b	c
a	b	a	$\cdot$
b	c	$\cdot$	$\cdot$
c	$\cdot$	$\cdot$	$\cdot$

Ein konkretes Beispiel ist $M = (\mathbb{Z}/3\mathbb{Z}, -)$, also $\overline{x} - \overline{y} = \overline{x - y}$. Das ist wegen $(\overline{1} - \overline{1}) - \overline{1} = \overline{2} \neq \overline{1} = \overline{1} - (\overline{1} - \overline{1})$ nicht assoziativ und es ist ein Magma, wenn die Subtraktion wohldefiniert ist – das haben wir aber in der LA indirekt gesehen: Das additiv Inverse ist wohldefiniert, die Addition ist wohldefiniert und Subtraktion ist die Addition des additiv Inversen.
Wir können das aber auch zu Fuß nachrechnen...

b) $*_1$ sei gegeben durch $x *_1 y = a$ für alle $x, y \in M$. Das ist ein Magma (klar), assoziativ (denn $x \cdot y \cdot z = a$, egal, wie wir klammern), aber für alle $x \in M$ gilt $x \cdot b = a \neq b$, also gibt es kein neutrales Element.
$*_2$, gegeben durch $x *_2 y = x$ für alle $x, y \in M$ ist eine weitere Möglichkeit. Das ist ein Magma, assoziativ (denn $x *_2 y *_2 z = x$, egal, wie wir klammern), aber es gibt kein Neutralelement $e \in M$: Sonst wäre $e = e *_2 a = a$ und $e = e *_2 b = b$, also $a = b$.
Die Verknüpfungstafeln wären

$*_1$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

beziehungsweise

$*_2$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

c) Ein Beispiel ist $M = (\mathbb{Z}/3\mathbb{Z}, \cdot)$ gegeben durch $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$. Das ist wohldefiniert (also haben wir ein Magma), was uns wieder die lineare Algebra sagt, denn $\mathbb{Z}/3\mathbb{Z}$ ist doch ein Ring mit vertreterweise + und $\cdot$. Eigentlich wissen wir dann schon alles: Die Multiplikation ist assoziativ und das neutrale Element ist $\overline{1}$, aber da $\overline{0}$ nicht invertierbar ist, liegt keine Gruppe vor.
Wer die lineare Algebra nicht zitieren will, der rechnet die Wohldefiniertheit zu Fuß nach:
Seien $\overline{x_1} = \overline{x_2}$, etwa $x_2 = x_1 + 3l$ für ein $l \in \mathbb{Z}$, und $\overline{y_1} = \overline{y_2}$, etwa $y_2 = x_2 + 3m$ für ein $m \in \mathbb{Z}$, dann ist $x_2 \cdot y_2 = (x_1 + 3l) \cdot (y_1 + 3m) = x_1 \cdot y_1 + 3 \cdot (ly_1 + mx_1 + 3ml)$, also $\overline{x_1 y_1} = \overline{x_2 y_2}$.
Die geforderten Eigenschaften rechnet man dann direkt nach, indem man die entsprechenden Eigenschaften von $(\mathbb{Z}, \cdot)$ benutzt.

d) $(\mathbb{Z}/3\mathbb{Z}, +)$ ist eine solche Gruppe, wobei + wieder vertreterweise definiert ist durch $\overline{x} + \overline{y} = \overline{x + y}$ – die Wohldefiniertheit und die restlichen Gruppenaxiome sind aus der linearen Algebra bekannt oder aus unserer Vorlesung.
Wir lernen bald, dass das (bis auf Isomorphie) sogar die einzige Gruppe ist, die drei Elemente enthält.

Aufgabe 2 (4 Punkte)
Seien G eine Gruppe, $U, V \leq G$ Untergruppen.

a) Zeige, dass $UV := \{uv \mid u \in U, v \in V\}$ genau dann eine Untergruppe ist, wenn $UV = VU$.

b) Zeige, dass $U \cup V$ genau dann eine Untergruppe ist, wenn $U \subseteq V$ oder $V \subseteq U$ gilt.

Lösung:
Elemente der Form u, u', u'', u_1, ... usf. seien stets Elemente aus U, analog seien Elemente aus V bezeichnet.

a) „$\Rightarrow$“: „$\subseteq$:“ Sei $uv \in UV$. Da UV eine Untergruppe ist, besitzt uv ein Inverses $u'v' \in UV$ und damit gilt $uv = (u'v')^{-1} = v'^{-1}u'^{-1} \in VU$.
„$\supseteq$:“ Sei $vu \in VU$. Es ist $vu = (v^{-1})^{-1}(u^{-1})^{-1} = (u^{-1}v^{-1})^{-1} \in UV$, denn $u^{-1}v^{-1} \in UV$ und da UV eine Untergruppe ist, ist auch das Inverse in UV enthalten.
„$\Leftarrow$:“ Wir verwenden das Untergruppenkriterium:
Es ist $e := e_G \in U$ und $e \in V$, also $ee = e \in UV$, also $UV \neq \emptyset$.
Weiterhin müssen wir zeigen, dass für $uv, u'v' \in UV$ das Produkt $(uv)(u'v')^{-1} \overset{(!)}{\in} UV$ liegt. Es ist
$(uv)(u'v')^{-1} = uvv'^{-1}u'^{-1} \overset{vv'^{-1} = v'' \in V}{=} uv''u'^{-1} \overset{v''u'^{-1} \in VU = UV \Rightarrow v''u'^{-1} = u''v'''}{=} uu''v''' \in UV$.

b) „$\Leftarrow$“ ist klar, denn dann ist $U \cup V = U$ oder $U \cup V = V$.
„$\Rightarrow$:“ Sei nun $U \cup V$ eine Untergruppe und $U \not\subseteq V$. Wir zeigen, dass dann $V \overset{(!)}{\subseteq} U$ gilt. Sei dazu $v \in V$ beliebig, also $v \in U \cup V$.
$U \not\subseteq V$, also gibt es ein $u \in U$ (also $u \in U \cup V$), $u \notin V$.
Da $u, v \in U \cup V$ ist, ist auch $uv \in U \cup V$, denn $U \cup V$ ist als Untergruppe abgeschlossen bezüglich der Verknüpfung. Dann aber ist $uv \in U$ oder $uv \in V$.
Wäre $uv \in V$, so wäre $u = (uv) \cdot v^{-1} \in V$, denn V ist eine Untergruppe. WIDERSPRUCH
Also ist $uv \in U$ und damit $v = u^{-1}(uv) \in U$, was zu zeigen war.

Alternativ setzen wir voraus, dass $U \not\subseteq V$ und $V \not\subseteq U$. Dann gibt es $u \in U \setminus V, v \in V \setminus U$, damit sind u und $v \in U \cup V$, aber $uv \notin U, uv \notin V$ (wie oben), also $uv \notin U \cup V$, also ist $U \cup V$ keine Gruppe.

Aufgabe 3 (4 Punkte)
Finden Sie Monoide M, N und einen Monoid-Homomorphismus $\varphi\colon M \to N$ mit der folgenden Eigenschaft:
Es ist $\varphi^{-1}(\{e_N\}) = \{e_M\}$, aber φ ist nicht injektiv.

Lösung:
Setze $M = (\mathbb{Z} \setminus \{-1\}, \cdot)$. Dies ist ein Untermonoid von $(\mathbb{Z}, \cdot)$, wie wir leicht einsehen:
Das neutrale Element ist 1 und die Assoziativität vererbt sich von $(\mathbb{Z}, \cdot)$ – es bleibt zu zeigen, dass $(M, \cdot)$ abgeschlossen ist:
Dafür müssen wir zeigen, dass $ab \neq -1$ für alle $a, b \in M$ gilt.
Das ist richtig für $a = 0$ oder für $b = 0$ und auch für $a = b = 1$. Für $a, b \neq 0$ und $a \neq 1$ ist $|ab| \geq |a| \geq 2$ (da $a \neq -1$), also ebenfalls $ab \neq -1$; analog für $a, b \neq 0, b \neq 1$.

Nun betrachten wir die Abbildung $\varphi\colon M \to \mathbb{Z}$ gegeben durch $x \mapsto x^2$.
Wegen $\varphi(1) = 1$ und $\varphi(xy) = (xy)^2 = xyxy = x^2y^2 = \varphi(x) \cdot \varphi(y)$ für alle $x, y \in M$ ist das ein Monoid-Homomorphismus.
φ ist nicht injektiv, etwa $\varphi(2) = 4 = \varphi(-2)$, aber es ist $\varphi^{-1}(\{1\}) = \{1\}$.

Aufgabe 4 (4 Punkte)
Gegeben seien das Monoid $N = \mathbb{N}_0 \times \mathbb{N}_0$ mit komponentenweiser Addition sowie ein weiteres Monoid M.
Bestimme alle Monoid-Homomorphismen von N nach M.

Lösung:
Schreibweise: Die Verknüpfung in M nennen wir $\cdot$ und $g^k = g \cdot ... \cdot g$ mit k Faktoren g für $k \in \mathbb{N}_0$, $g \in M$.
$\mathbb{N}_0 \times \mathbb{N}_0$ wird (als Monoid) erzeugt von $e_1 = (1, 0)$ und $e_2 = (0, 1)$, denn jedes $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ ist die x-fache Summe von e_1 mit der y-fachen Summe von e_2.
Jeder Monoid-Homomorphismus $\varphi\colon N \to M$ ist eindeutig über die Bilder von e_1, e_2 in M gegeben, aber nicht alle möglichen Bilder sind erlaubt, denn es gilt

$$\varphi(e_1)\varphi(e_2) = \varphi(e_1 + e_2) = \varphi((1, 1)) = \varphi(e_2 + e_1) = \varphi(e_2)\varphi(e_1).$$

Dies bringt uns zu folgender **Behauptung:**
Es gibt eine Bijektion zwischen $\mathrm{Hom}(N, M)$ und der Menge $P = \{(x, y) \in M^2 : xy = yx\}$ aller geordneten Paare aus M, die kommutieren.

Gilt $gh = hg$ in M, so definiert $\varphi(x, y) = g^x h^y$ einen Monoid-Homomorphismus vom N nach M, denn:
$\varphi(e_N) = \varphi(0, 0) = g^0 h^0 = e_M$ und für alle $(x, y), (x', y') \in N$ gilt
$\varphi((x, y) + (x', y')) = \varphi(x + x', y + y') = g^{x+x'} h^{y+y'} = g^x g^{x'} h^y h^{y'} = (*)$ und
$\varphi((x, y)) \cdot \varphi((x', y')) = g^x h^y g^{x'} h^{y'} = (*)$,
da wir g und h beliebig vertauschen dürfen, wenn wir mehrmalig $gh = hg$ anwenden.
Also haben wir eine Abbildung $\alpha\colon P \to \mathrm{Hom}(N, M)$, gegeben durch $\alpha((g, h)) : N \to M, (x, y) \mapsto g^x h^y$.

Andererseits haben wir in der Vorüberlegung schon gesehen, dass für jeden Homomorphismus $\varphi \in \mathrm{Hom}(N, M)$ das Paar $(\varphi(e_1), \varphi(e_2)) \in P$ liegt.
Also haben wir die Abbildung $\beta\colon \mathrm{Hom}(N, M) \to P$, gegeben durch $\beta(\varphi) = (\varphi((1, 0)), \varphi((0, 1)))$.

Es bleibt zu zeigen, dass die Zuordnungen bijektiv zueinander sind:

Sei zunächst $(g, h) \in P$. Zu zeigen ist $\beta(\alpha((g, h))) \overset{(!)}{=} (g, h)$. Es ist
$\beta(\alpha((g, h))) \overset{\mathrm{Def}\,\beta}{=} (\alpha((g, h))(1, 0), \alpha((g, h))(0, 1)) \overset{\mathrm{Def}\,\alpha}{=} (g^1 h^0, g^0 h^1) = (g, h)$.

Sei weiterhin $\varphi \in \mathrm{Hom}(N, M)$ beliebig. Zu zeigen ist $\alpha(\beta(\varphi)) \overset{(!)}{=} \varphi$:
Für $(x, y) \in N$ gilt $\alpha(\beta(\varphi))(x, y) \overset{\mathrm{Def}\,\beta}{=} \alpha(\varphi((1, 0)), \varphi(0, 1))(x, y) \overset{\mathrm{Def}\,\alpha}{=} \varphi((1, 0))^x \varphi((0, 1))^y \overset{\varphi\mathrm{Hom}}{=} \varphi((x, y))$.

Zusatzaufgabe (4 Punkte)
Seit Jahren schon – ach was: seit Jahrhunderten! – wohnten die Zwerge in ihrer gemütlichen Höhle und erfreuten sich des Lebens. Schon so manchen Strauß hatten sie mit den Zauberern gefochten, hatten Riesen invariant gemacht und Schneewittchens Wünsche zu erfüllen versucht und was es noch so an zwergentypischen Aufgaben zu erledigen galt. Und immer hatten sie es verstanden, die richtigen mathematischen Konzepte für ihre Zwecke zu nutzen.[1]

In letzter Zeit jedoch beklagten sich einige unserer Zwerge über eine unangenehme Wärme, die immer stärker aus dem Gestein zu steigen schien. Schon munkelte man über Vulkane, Sühne und Untergang der Zwergengemeinschaft.
Oberschlau waren diese Unkenrufe nicht recht, und so hinterfragte er die düsteren Prognosen der anderen ein ums andere Mal.

Als er Monopel fragte, was das für ein Magma sein solle, das da in den Tiefen schlummert, erhielt er nur zur Antwort: „Kein triviales jedenfalls, soviel sagt mir der Verstand unter meiner Zwergenmütze."

Zwiepel antwortete, nach möglichen Aktionen befragt, dass er nur wisse, was sicher nichts bringt; teilen könne man das Magma nicht, denn es hänge so fest zusammen, dass es von jedem Teil[2] erzeugt werde.

Als Tripel schließlich Auskunft über das Ausmaß des Magmas geben sollte, erfuhr Oberschlau lediglich, dass es sehr tief hinabreiche.

„Ah… so… tia… tief – ABER JA DOCH!!! – Genau das müsste uns helfen. Das Magma, das ihr beschreibt, ist leer!"

Ein erstauntes Raunen ging durch die Menge, und als man den Fels einen kleinen Spalt weit öffnete, fand man nichts. Alle waren erstaunt, wie Oberschlau das nun wieder angestellt hatte. Schließlich verriet er, dass er insbesondere deshalb nicht an das Magma geglaubt hatte, da er – etwas betagt war er ja nun schon – sich den Luxus einer kleinen Heizung erlaubt hatte, und die wäre wahrscheinlich für die ungewöhnliche Wärme zuständig.
Der Rest war eine leichte Übungsaufgabe. Oder?

Lösung: Wir erinnern uns, dass für eine Halbgruppe H das Halbgruppenerzeugnis $\langle T\rangle$ einer Menge $T \subseteq H$ die Menge aller endlichen nichtleeren Produkte von Elementen aus T ist. Insbesondere ist $\langle t\rangle = \{t^n : n \in \mathbb{N}\}$.

Wir haben ein assoziatives (laut Tripel) Magma M, also eine Halbgruppe M. M besitzt nicht genau ein Element (laut Monopel) und es gilt $M = \langle N\rangle$ für jede nichtleere Teilmenge N von M (laut Zwiepel) – insbesondere wird M also von jedem einzelnen Element erzeugt. (Das ist sogar äquivalent zu Zwiepels Aussage, nicht wahr? Das brauchen wir aber gar nicht.)
Zu zeigen ist $M = \emptyset$, also nehmen wir an, es gäbe ein Element $a \in M$, dann wäre (nach Monopel) $\#M \geq 2$. Es ist $a^2 \neq a$, sonst wäre $a^n = a$ für alle $n \in \mathbb{N}$ und damit $\langle a\rangle = \{a\} \neq M$ (im Widerspruch zu Zwiepel).
Auch a^2 erzeugt M, also ist insbesondere $a \in \langle a^2\rangle$, also $a = (a^2)^j = a^{2j}$ für ein $j \in \mathbb{N}$, wobei $j > 1$ wegen $a^2 \neq a$. Insbesondere muss es ein kleinstes $k \in \mathbb{N}_{>1}$ geben, so dass $a^k = a$ gilt.
Für a^{k-1} gilt dann $a^{k-1} \cdot a^{k-1} = a^k \cdot a^{k-2} = a \cdot a^{k-2} = a^{k-1}$, aber dann gilt – wie wir das oben für a gesehen haben – $\langle a^{k-1}\rangle = \{a^{k-1}\} \neq M$. (Widerspruch zu Zwiepel)

Also gibt es dieses a nicht und damit sind wir fertig und die Zwerge gerettet.

[1] Bisher ist das eher für solche Leser interessant, die schon andere Zwergenaufgaben kennen, am besten die, auf die hier angespielt wird. ;-)
[2] Von jedem nichtleeren Teil versteht sich; für solche Haarspaltereien hatten nicht alle Zwerge einen Sinn, vor allem in diesen Schicksalsstunden.