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

Einführung in Algebra und Zahlentheorie – Übungsblatt 6

Aufgabe 1 (4 Punkte)
Sei M eine Menge und $\mathcal{P}(M)$ ihre Potenzmenge. Für $A, B \in \mathcal{P}(M)$ sei $A \triangle B$ die *symmetrische Differenz*:

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Zeige, dass $\mathcal{P}(M)$ mit den Verknüpfungen $\triangle$ und $\cap$ zu einem kommutativen Ring wird.
Überlege dir zunächst, welche der beiden Verknüpfungen additiv, welche multiplikativ ist, und zeige anschließend die Axiome.

Lösung Aufgabe 1
Dass $\cap$ und $\triangle$ Verknüpfungen auf $\mathcal{P}(M)$ sind, ist offensichtlich. Sie sind kommutativ, wie man schnell einsieht.
Ohne Einschränkung nehmen wir an, dass $M \neq \emptyset$, ansonsten ist $\mathcal{P}(M)$ der Nullring.

M selbst ist neutral bezüglich $\cap$, denn für alle $A \in \mathcal{P}(M)$ ist $A \cap M = A$. Es gibt aber kein Inverses von $\emptyset$ bezüglich Schnitt, denn $\emptyset \cap A = \emptyset \neq M$ für alle $A \in \mathcal{P}(M)$. Wir folgern, dass $\cap$ die multiplikative Verknüpfung sein muss.

Seien ab sofort stets $A, B, C \in \mathcal{P}(M)$ beliebig.
Schritt 1: Zeige, dass $\mathcal{P}(M)$ bezüglich $\triangle$ eine abelsche Gruppe bildet.

- Das neutrale Element ist $\emptyset$, denn für alle $A \in \mathcal{P}(M)$ ist $A \triangle \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$.
- Jedes $A \in \mathcal{P}(M)$ ist selbstinvers, denn $A \triangle A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$.
- Schließlich müssen wir noch die Assoziativität zeigen, was etwas Arbeit bedeutet. Dabei nutzen wir aus, dass ein x aus M genau dann in der symmetrischen Differenz zweier Mengen liegt, wenn es genau in einer der Mengen liegt. $(*)$
  Wir zeigen, dass x genau dann in $(A \triangle B) \triangle C$ liegt, wenn x in allen drei Mengen oder in genau einer Menge liegt, was auch äquivalent zu $x \in A \triangle (B \triangle C)$ ist.
  Für $x \in M$ gibt es genau 8 Möglichkeiten, wie x in A, B, C enthalten ist oder nicht. Wir können den Beweis zum Beispiel mit einer Wahrheitstafel mit diesen 8 Fällen führen.
  Etwa für $x \in A, x \in B, x \in C$ ist $x \notin A \triangle B, x \in C \Rightarrow x \in (A \triangle B) \triangle C$ nach $(*)$. Ebenso ist dann $x \notin B \triangle C, x \in A$, also in $A \triangle (B \triangle C)$.
  Für $x \in A, x \in B, x \notin C$ ist $x \notin A \triangle B, x \notin C \Rightarrow x \notin (A \triangle B) \triangle C$ und $x \in B \triangle C, x \in A \Rightarrow x \notin A \triangle (B \triangle C)$.
  (... 6 weitere Fälle, die jeder selbst hinbekommt; Alternativ können die Aussagen auch direkt umgeformt werden, dies wird nur etwas wüst zum aufschreiben, ist aber auch nicht schwer!)

Schritt 2: Zeige, dass $\mathcal{P}(M)$ bezüglich $\cap$ ein Monoid ist. Dies ist relativ offensichtlich, das neutrale M haben wir oben bereits gefunden, die Assoziativität von $\cap$ ist klar, denn $x \in A \cap B \cap C \Leftrightarrow x \in A, x \in B, x \in C$, egal, wie wir auf der linken Seite klammern.

Schritt 3: Es verbleibt das Distributivgesetz $A \cap (B \triangle C) \overset{(!)}{=} (A \cap B) \triangle (A \cap C)$ zu zeigen. Dies kann wieder mit einer Wahrheitstafel gemacht werden oder wir zeigen es diesmal direkt:
Nach $(*)$ ist $x \in A \cap (B \triangle C) \Leftrightarrow x \in A, x \in B \triangle C \Leftrightarrow x \in A, x \in B, x \notin C$ oder $x \in A, x \notin B, x \in C$ $(**)$, wobei sich die letzten beiden Möglichkeiten ausschließen, also sogar ein entweder-oder vorliegt.
Andersherum ist $x \in A \cap B \triangle A \cap C \Leftrightarrow$ entweder $x \in A \cap B$ oder $x \in A \cap C \Leftrightarrow$ entweder $x \in A, x \in B, x \notin C$ oder $x \in A, x \notin B, x \in C$ was genau $(**)$ entspricht.

Wir sind fertig und es verbleibt, eine elegante **Alternativlösung** zu zeigen. Da wir diese in der Übung vielleicht etwas zu schnell durchgerechnet haben, werde ich das Ganze etwas genauer ausführen. Die Lösung wirkt dadurch nicht viel kürzer als die erste Lösung, aber wir erinnern uns, dass wir dort nicht alles ausgeführt haben, außerdem schreiben wir hier etwas mehr als nötig, damit die Lösung gut verstanden werden kann.

Betrachte die algebraische Struktur $R = \mathrm{Abb}(M, \mathbb{Z}/2\mathbb{Z})$ mit elementweiser Addition und Multiplikation - d.h.$(\varphi_1 + \varphi_2)(m) = \varphi_1(m) + \varphi_2(m), (\varphi_1 \cdot \varphi_2)(m) = \varphi_1(m) \cdot \varphi_2(m)$ für alle $\varphi_1, \varphi_2 \in R, m \in M$. Dies ist ein Ring, wie aus der linearen Algebra bekannt ist.

Wir finden nun eine Bijektion zwischen R und $\mathcal{P}(M)$, die mit den Verknüpfungen verträglich ist, das heißt, $\cap$ auf der einen Seite entspricht $\cdot$ auf der anderen, $\triangle$ entspricht $+$, alles vermöge der Bijektion versteht sich.
Dann folgt sofort, dass $\mathcal{P}(M)$ mit den gegebenen Verknüpfungen auch ein Ring ist, die beiden algebraischen Strukturen sind dann ja die gleichen bis auf Umbenennung - unsere Bijektion war also ein Isomorphismus von Ringen, wobei $1 \mapsto 1$ gleich mitgeschenkt wird. (Wieso?)

Wir ordnen jeder Menge $A \subseteq M$ ihre Indikatorfunktion I_A mit $I_A(m) = \begin{cases} 1 & \text{falls } m \in A \\ 0 & \text{falls } m \notin A \end{cases}$ zu.
Da eine Teilmenge A von M gerade dadurch charakterisiert ist, dass für jedes $m \in M$ entschieden wird, ob m in A liegt oder nicht, liefert die obige Zuordnung eine Bijektion. (Man kann Injektivität und Surjektivität auch schnell nachrechnen, wenn man das bislang noch nicht glaubt.)

Nun identifizieren wir $A \leftrightarrow I_A$ und zeigen, dass sich die Verknüpfungen wie oben gesehen entsprechen. Für beliebige $A, B \subseteq M$ zeigen wir also folgende Aussagen:
$A \cap B \leftrightarrow I_A \cdot I_B$ und $A \triangle B \leftrightarrow I_A + I_B$.

Für die erste Aussage müssen wir zeigen, dass $I_{A\cap B} \overset{(!)}{=} I_A \cdot I_B$ ist.
Für $x \in M$ ist $I_{A\cap B}(x) = 1 \Leftrightarrow x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \Leftrightarrow I_A(x) = 1 \wedge I_B(x) = 1 \Leftrightarrow I_A(x) \cdot I_B(x) = 1 \Leftrightarrow (I_A \cdot I_B)(x) = 1$, wobei wir nutzen, dass in $\mathbb{Z}/2\mathbb{Z}$ das Produkt zweier Zahlen genau dann 1 ist, wenn beide 1 sind.

Für die zweite Aussage müssen wir zeigen, dass $I_{A\triangle B} \overset{(!)}{=} I_A + I_B$ ist.
Für $x \in M$ ist $I_{A\triangle B}(x) = 1 \Leftrightarrow x \in A \backslash B \vee x \in B \backslash A \Leftrightarrow (I_A(x) = 1, I_B(x) = 0) \vee (I_A(x) = 0, I_B(x) = 1) \Leftrightarrow I_A(x) + I_B(x) = 1 \Leftrightarrow (I_A + I_B)(x) = 1$, wobei wir nutzen, dass in $\mathbb{Z}/2\mathbb{Z}$ nur 0 und 1 als Summe 1 ergeben.

Das war alles!

Aufgabe 2 (5 Punkte)
Sei $d \in \mathbb{Z}$ kein Quadrat einer rationalen Zahl und $w \in \mathbb{C}$ eine Wurzel von d. Sei R der kleinste Ring, der $\mathbb{Z}$ und w umfasst. Zeigen Sie:

a) Jedes Element aus R kann eindeutig als $a + bw,\ a, b \in \mathbb{Z}$ geschrieben werden.

b) Die Abbildung $\psi : R \to R, a + bw \mapsto a - bw$ ist ein Ring-Automorphismus von R.

c) Die Abbildung $\mathcal{N} : R \to \mathbb{C}, r \mapsto r \cdot \psi(r)$ ist ein Monoid-Homomorphismus von $(R, \cdot)$ nach $(\mathbb{Z}, \cdot)$.

d) Es ist $R^\times = \{r \in R : \mathcal{N}(r) \in \{\pm 1\}\}$.

e) Berechnen Sie mit Hilfe von d) für alle $d < 0$ die Einheitengruppe.

Lösung Aufgabe 2

a) Da d keine Quadratzahl ist, ist $w \notin \mathbb{Q}$ und damit sind 1 und w über $\mathbb{Q}$ linear unabhängig. Für jede Zahl der Form $a + bw,\ a, b \in \mathbb{Z}$, sind daher die Koeffizienten eindeutig bestimmt.
(Wem das nicht gefällt, der nehme an, $a + bw = a' + b'w$. Für $b = b'$ ist $a = a'$, die Darstellungen also gleich, aber $b \neq b'$ ist gar nicht möglich, sonst wäre $w = \frac{a-a'}{b'-b} \in \mathbb{Q}$.)

Wegen der Abgeschlossenheit liegen sicher alle Elemente der Form $a + bw,\ \ a, b \in \mathbb{Z}$, in R und es muss nur noch gezeigt werden, dass jedes Element aus R von der gewünschten Gestalt ist. Dies folgt wegen der Minimalität von R daraus, dass

$$\tilde{R} := \{a + bw \mid a, b \in \mathbb{Z}\}$$

ein Teilring von $\mathbb{C}$ ist.

Dies wiederum ist klar, denn $\tilde{R}$ ist offensichtlich eine Gruppe bezüglich der Addition, $1 \in \tilde{R}$, und

$$\forall a, b, r, s \in \mathbb{Z} : (a + bw) \cdot (r + sw) = (ar + bsd) + (as + br)w \in \tilde{R}.$$

b) Es ist

$$\psi(1) = \psi(1 + 0w) = 1 - 0w = 1,$$

und außerdem gilt für alle $a, b, r, s \in \mathbb{Z}$:

$$\begin{aligned}\psi((a + bw) + (r + sw)) &= \psi((a + r) + (b + s)w) = (a + r) - (b + s)w \\ &= (a - bw) + (r - sw) = \psi(a + bw) + \psi(r + sw)\end{aligned}$$

sowie

$$\begin{aligned}\psi((a + bw) \cdot (r + sw)) &= \psi((ar + bsd) + (as + br)w) = (ar + bsd) - (as + br)w \\ &= (a - bw) \cdot (r - sw) = \psi(a + bw) \cdot \psi(r + sw).\end{aligned}$$

Damit sind alle Eigenschaften eines Ring-Homomorphismus nachgewiesen.

Offensichtlich ist ψ selbstinvers, also insbesondere bijektiv, also sogar ein Ring-Automorphismus.

c) Es ist

$$\mathcal{N}(a + bw) = (a + bw) \cdot \psi(a + bw) = (a + bw) \cdot (a - bw) = a^2 - b^2 d \in \mathbb{Z},$$

also ist $\mathcal{N}$ eine Abbildung von R nach $\mathbb{Z}$. Da ψ ein Ringhomomorphismus und R kommutativ ist, gilt tatsächlich $\mathcal{N}(1) = 1$ und

$$\mathcal{N}(x \cdot y) = xy\psi(xy) = xy\psi(x)\psi(y) = x\psi(x) \cdot y\psi(y) = \mathcal{N}(x) \cdot \mathcal{N}(y).$$

d) Wenn $x \in R$ eine Einheit ist, dann gilt

$$\mathcal{N}(x) \cdot \mathcal{N}(x^{-1}) = \mathcal{N}(1) = 1.$$

Da aber sowohl $\mathcal{N}(x)$ als auch $\mathcal{N}(x^{-1})$ in $\mathbb{Z}$ liegen, müssen beide ± 1 sein. Es folgt $\mathcal{N}(x) = \pm 1$.

Wenn umgekehrt $\mathcal{N}(x) = \pm 1$ gilt, so folgt $x\psi(x) = \pm 1$, und damit $x \cdot (\pm\psi(x)) = 1$, also ist $\pm\psi(x) = x^{-1}$ und x ist eine Einheit.

e) Nun sei $d < 0$. Dann gilt für $a, b \in \mathbb{Z}$:

$$\mathcal{N}(a + bw) = a^2 + b^2|d|.$$

Aus der Bedingung $a^2 + b^2|d| = 1$ folgt für $d \leq -2$ (d.h. $|d| \geq 2$) sofort $b = 0$ und anschließend $a = \pm 1$, wir haben also die Einheiten ± 1.
Für $d = -1$ gilt schwächer $|b| \leq 1$ und wir finden die vier Einheiten $1, -1, w, -w$, dies sind offensichtlich alle.

Aufgabe 3 (3 Punkte)
Zeige, dass es keinen Ring mit genau 5 Einheiten geben kann.
(*Hinweis:* Was ist die Charakteristik eines solchen Ringes? Untersuche für eine Einheit a der Ordnung 5 das Element $1 + a^2 + a^3$!)

Lösung Aufgabe 3
Nach dem Satz von Lagrange hat jede Einheit $\neq 1$ (multiplikative) Ordnung 1 oder 5. Wegen $(-1)^2 = 1$ (Das ist eine gute Übungsaufgabe, die eventuell schon im Tutorium behandelt wurde.) ist die Ordnung von -1 also ≤ 2, also insgesamt folgt $\operatorname{ord}(-1) = 1$, was $-1 = 1$ impliziert. Der Ring hat Charakteristik 2.

Für die nachfolgende Rechnung nutzen wir $x + x = 0$ für alle $x \in R$ und dass $1, a, a^2, a^3, a^4$ paarweise verschieden sind sowie $a^5 = 1$. Dann gilt für $1 + a^2 + a^3$:

$(1 + a^2 + a^3)^2 = 1 + a^2 + a^3 + a^2 + a^4 + a^5 + a^3 + a^5 + a^6 = 1 + a + a^4$
$(1 + a^2 + a^3)^3 = (1 + a + a^4) \cdot (1 + a^2 + a^3) = 1 + a^2 + a^3 + a + a^3 + a^4 + a^4 + a^6 + a^7 = 1.$
Dies ist ein Widerspruch, denn wegen $a^2 \neq a^3$ ist $1 + a^2 + a^3 \neq 1$, hat aber Ordnung < 5.

Märchen 4 (4 Punkte)
Was war das für ein Trubel in der Höhle der Zwerge. Schneewittchen hatte wieder einmal angekündigt, ihren Prinzen heiraten zu wollen, und obwohl jedem der Zwerge insgeheim klar war, dass die Hochzeit wieder einmal daran scheitern würde, einen Termin zu finden, an dem alle Gäste Zeit finden – dies erzählen wir in einer anderen Geschichte – waren alle Zwerge mit den Vorbereitungen beschäftigt.
Oberschlau hatte bei Hochzeit natürlich gleich wieder an die Algebra gedacht, „Ohne Ringe kann man nicht heiraten!“ gerufen und einen Vortrag über Ringtheorie gehalten, der allen im Kopf rumspukte, spätestens seit der Prinz erschreckt festgestellt hatte, dass er die Ringe ganz vergessen hatte.
„Die Kuh motzt schon wieder“, rief Rumpel, der gerade verzweifelt versuchte, die Kuh zu melken, die heftig dagegen protestierte, aber sie brauchten doch dringend Milch für die Hochzeitstorte.
„Die Kuh motzet?“, sinnierte Kumpel. Gleich kam ihm eine Idee und flugs schrieb er dem verblüfften Prinzen $\mathbb{Q}/\mathbb{Z}$ auf einen Zettel und verkündete lautstark, dass er hier eine additive Gruppe gefunden habe, die der Prinz nur noch mit einer passenden Multiplikation versehen müsse, um Schneewittchen doch einen Ring überreichen zu können. Gerade wollte Oberschlau protestieren, doch zu ihrer aller Verblüffung rief schon der Prinz spontan aus, dass er wohl noch einen Zauberer benötigen würde, um hier eine Multiplikation zu finden. „Richtig, das geht nämlich gar nicht“, ergänzte Oberschlau, ein wenig verärgert, dass der Prinz die passende Antwort gegeben hatte. $(*)$
„Aua...“, das war wieder Rumpel, der sich sein Schienbein rieb, gegen das er gerade getreten worden war, „Brauchen wir die Milch denn wirklich?“
„Da steht: 'ein Liter Milch'.“ antwortete Hampel, der das Kochbuch noch einmal genau studierte. „Wenn wir keine Milch hätten...“ „Ein Liter gleich null Liter...“ warf Oberschlau ein, „Das geht wohl genau dann, wenn die Mengenangaben des Kochbuchs aus dem Nullring stammen“. $(*)$
Hatte er das wirklich gesagt? Dass der Prinz ihm die Möglichkeit genommen hatte, Kumpel zu verbessern, hatte ihn dermaßen geärgert, dass er jetzt schon solche Trivialitäten von sich gab. „Den Nullring sollte Schneewittchen aber besser nicht kriegen“, hielt Hampel dagegen, der immer noch das Kochbuch las. „Hier, wir können notfalls Phi-Kringel backen, dazu brauchen wir keine Milch.“
„Wir kriegen aber Milch und wenn ich das blöde Vieh....... Er... Es... Sie hat mich schon wieder getreten!“, beschwerte sich Rumpel. „Vieh, Er, Es?“, wiederholte Pümpel nachdenklich von der Seite. „Da konnte ich vorhin schon bei Oberschlaus Vortrag nicht folgen. Der hatte doch auch immer sowas...“ „Schneewittchen ist ja auch nicht homomorph“, wandte der freche Hampel von der Seite ein und erntete ein paar böse Blicke. „Früher sah sie mehr wie eine 1 aus.... Wenn wir sie jetzt auch noch mit Hochzeitstorte füttern...“
„Das wiederum würde für Phi-Kringel sprechen“, rief Oberschlau dazwischen, „schließlich wissen wir, was mit Einsen passiert, zumindest, wenn Phi ein Ring-Homomorphismus ist.“ „Wieso muss man das eigentlich fordern?“ fragte Pümpel, der sich langsam wieder an Details aus Oberschlaus Vortrag erinnerte. „Ich meine, heute fordert Schneewittchen doch schon genug von uns...“
Oberschlau war in seinem Element und da der Prinz gerade dabei war, seine Leibgarde zu begutachten, konnte er in aller Ruhe Pümpel mit einem Beispiel überzeugen, dass er in seinen Definitionen nicht zu viel hingeschrieben hatte. $(*)$
„Verdammt...“, hörten sie den Prinzen aus der Ferne fluchen. „Meine Leibgarde sollte hochzeitlich aussehen, aber in ihren Rüstungen sehen sie aus wie Einheiten, die aufs Schlachtfeld, nicht an einen Altar

gehören.“ „Auch hier werden Phi-Kringel nicht helfen“, lachte Oberschlau. „Denn was unter einem Ringhomomorphismus Phi mit Einheiten passiert, sollte bekannt sein...“ $(*)$

An dieser Stelle wollen wir unsere Zwerge verlassen, die weitere Geschichte ist kurz erzählt: Es gab ein großes Chaos, Rumpel wurde von der Kuh getreten, die Phi-Kringel sind verbrannt, aber das war gar nicht schlimm, weil die Hochzeit eh ausfallen muste... Gerade Schneewittchens wichtiger Freund aus China hatte es zu dem Termin nicht geschafft...
Und wenn sie nicht gestorben sind, dann reden sie auch heute noch durcheinander. Du hingegen solltest dir die Stellen mit den Sternchen noch einmal genauer anschauen und etwas Mathematik betreiben. Worüber haben die Zwerge an diesen Stellen gesprochen?

Weitere offene Fragen, die dich interessieren könnten:
Wird Schneewittchen jemals heiraten? Wird der chinesische Restsatz ihr dabei helfen können, endlich ihr Glück zu finden? Wenn ja: Wird Dornröschen die Trauung verschlafen? Welcher der Zwerge sollte Trauzeuge des Prinzen sein?
Achja, wieviel Mehl braucht man noch mal für ein Dutzend Phi-Kringel?

ENDE

Lösung Märchen 4

- Sei R zunächst ein beliebiger Ring mit 1 und endlicher Charakteristik n. Für alle x ist dann $x + ... + x = 1x + ... + 1x = (1 + ... + 1)x = 0$, wenn wir n Summanden x addieren. Die additive Ordnung jedes Elementes ist also kleinergleich der Charakteristik - es ist sogar ein Teiler davon, wie wir früher gesehen haben.

  In $(\mathbb{Q}/\mathbb{Z}, +)$ besitzt jedes Element endliche additive Ordnung, denn die Elemente sind von der Form $[\frac{a}{b}]$ und b-fache Addition liefert $[\frac{a}{b}] + ... + [\frac{a}{b}] = [a] = [0]$.
  Gäbe es eine passende Multiplikation, so hätte er endliche Charakteristik n, aber die additive Ordnung von $[\frac{1}{n+1}]$ ist $n + 1$, was der Vorüberlegung widerspricht.

- Die einfache Behauptung ist $0 = 1 \Leftrightarrow R = \{0\}$, wobei „$\Leftarrow$“ sicher stimmt.
  Gilt aber $0 = 1$, so ist für alle $x \in R$ $x = 1x = 0x = 0$, also R der Nullring.

- Wieso fordern wir $\varphi(1_R) = 1_S$, aber nicht $\varphi(0_R) = 0_S$? Letzteres gilt bei jedem Gruppenhomomorphismus, aber wir erinnern uns, dass wir bei Monoidmorphismen vorsichtig sein mussten.[1]
  Ein konkretes Beispiel wäre die Nullabbildung von $\mathbb{Z}$ auf sich selbst, die die Addition und Multiplikation erhält, aber kein Ringhomomorphismus ist, weil die 1 nicht auf die 1 abgebildet wird.[2]

- Das haben wir doch sogar in der Vorlesung schon gesehen. Einheiten werden auf Einheiten abgebildet unter Ringhomomorphismen.
  Ist $r \in R^\times$, etwa $rs = sr = 1_R$, so ist $\varphi(r) \cdot \varphi(s) = \varphi(rs) = \varphi(1_R) = 1_S$ und analog $\varphi(s)\varphi(r) = 1_S$, also $\varphi(r) \in S^\times$.
  (Stärker wissen wir sogar sofort, wie wir das Inverse des Bildes bestimmen: als Bild des Inversen. Genau so wollen wir es doch auch haben, da die Struktur erhalten bleiben soll...)

[1] Dies wäre ein guter Zeitpunkt, sich noch einmal anzuschauen, wie man das bei Gruppenhomomorphismen direkt zeigen konnte, wenn man nur fordert, dass die Verknüpfung respektiert wird. Da muss man eben aufpassen. Scheinbar wird laut Definition nur ein kleiner Teil der Struktur respektiert, der Rest (etwa, was mit dem Neutralelement geschieht) kann aber eben daraus abgeleitet werden und gehört wohl zur Strukturerhaltung!

[2] Damit wird die multiplikative Struktur eben doch nicht erhalten. Denn das Neutralelement gehört eben zur Struktur dazu!