

Musterlösung zur Serie 5

Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

8. Juni 2017

- Aufgabe 1** (5+5 Punkte). 1. Es sei N eine Menge. Zeigen Sie, dass $(\mathfrak{P}(N), \Delta)$ eine abelsche Gruppe ist, wobei die *symmetrische Differenz* Δ für zwei Mengen A und B wie folgt definiert ist: $A \Delta B := (A \cup B) \setminus (A \cap B)$.
2. Wir definieren auf $\mathbb{Z} \times \mathbb{Z}$ die Struktur $\odot$ durch: $(z_1, z_2) \odot (z'_1, z'_2) := (z'_1 z_2 + z_1, z_2 z'_2)$. Zeigen Sie, dass $(\mathbb{Z} \times \mathbb{Z}, \odot)$ ein nicht-abelscher Monoid ist. Geben Sie für alle Elemente von $\mathbb{Z} \times \mathbb{Z}$, die bezüglich $\odot$ eine Inverse besitzen, sowohl das Element als auch dessen Inverse an.

Lösung:

1. Die symmetrische Differenz Δ ist kommutativ, da $\cup$ und $\cap$ kommutativ sind, und $\emptyset$ ist ein neutrales Element bzgl. Δ . Des Weiteren ist jedes Element von $\mathfrak{P}(N)$ zu sich selbst invers, d.h. $A \Delta A = \emptyset$. Es bleibt also die Assoziativität zu zeigen. Es seien A, B und C Teilmengen von N . Wir zeigen, dass $(A \Delta B) \Delta C$ und $R := (R_1 \setminus R_2) \cup R_3$ übereinstimmen, wobei die R_i wie folgt definiert sind:

$$R_1 := A \cup B \cup C, \quad R_2 := (A \cap B) \cup (A \cap C) \cup (B \cap C), \quad R_3 := A \cap B \cap C.$$

Wir zeigen zuerst " $\subseteq$ ". Es sei x ein Element von $L := (A \Delta B) \Delta C$.

1. Fall: $x \in A \Delta B$. Dann $x \notin C$, da $x \in L$, und $x \in A \cup B$, da $A \Delta B$ eine Teilmenge von $A \cup B$ ist. Es folgt weiter $x \notin A \cap B$ aus $x \in A \Delta B$. Also ist x ein Element von $R_1 \setminus R_2$.

2. Fall: $x \in C$ und $x \notin A \Delta B$. Wenn x ein Element von A ist, dann ist es auch ein Element von B , da $x \notin A \Delta B$. Insbesondere ist dann x ein Element von R_3 . Das gleiche Argument verwendet man im Fall $x \in B$. Wenn x kein Element von $A \cup B$ ist, dann ist es auch kein Element von R_2 und somit ein Element von $C \setminus R_2$, also ein Element von R .

Wir zeigen nun die andere Inklusion " $\supseteq$ ": Erstmal stellen wir fest, dass R_3 eine Teilmenge von L ist, denn jedes Element von R_3 ist ein Element von C aber kein Element von $A \Delta B$.

Fall 1: $x \in R \setminus C$. Dann liegt x nicht in R_3 und muss sich deshalb in $R_1 \setminus R_2$ befinden, und kann somit kein Element von $A \cap B$ sein, d.h. dass x in $(A \Delta B) \setminus C$ liegt. Letztere ist eine Teilmenge von L .

Fall 2: $x \in R \cap C$. Es ist x entweder ein Element von $A \cup B$ und somit ein Element von $R_3 \subseteq L$, da x kein Element von $R_1 \setminus R_2$ sein kann, oder kein Element von $A \cup B$ und somit eines von $C \setminus (A \Delta B)$. In jedem Fall ist x ein Element von L . Damit sind beide Inklusionen gezeigt.

Wir erhalten also die folgende Gleichung:

$$(A \Delta B) \Delta C = R = (B \Delta C) \Delta A = A \Delta (B \Delta C).$$

wobei hier mehrmals die Kommutativität von Schnitt und Vereinigung ausgenutzt wurden.

2. Es gibt eine kanonische Bijektion zur Menge M der Matrizen der Form

$$\begin{pmatrix} z_2 & z_1 \\ 0 & 1 \end{pmatrix}$$

wobei z_1 und z_2 die Menge der ganzen Zahlen passieren. Diese Bijektion ist ein Homomorphismus bzgl. $\odot$ und der Matrizenmultiplikation. Das zeigt automatisch, die Abgeschlossenheit von M bzgl.

der Matrizenmultiplikation, da $\mathbb{Z} \times \mathbb{Z}$ abgeschlossen bezüglich $\odot$ ist. Die Multiplikation von Matrizen ist assoziativ und die Einheitsmatrix liegt in M , und damit ist M ein Monoid. Also folgt aus der obigen Isomorphie, dass $\odot$ eine Monoidstruktur ist. Die Elemente (z_1, z_2) mit den Einträgen $z_2 \in \{1, -1\}$ sind invertierbar, mit der Inversen $(-z_2 z_1, z_2)$ wie eine Rechnung leicht zeigt, und ein invertierbares Element von $\mathbb{Z} \times \mathbb{Z}$ muss automatisch $|z_2| = 1$, erfüllen, da z_2 bezüglich der Multiplikation in $\mathbb{Z}$ eine Inverse haben muss. Die Struktur $\odot$ ist nicht abelsch, wie das folgende Beispiel zeigt.

$$(2, 3) \odot (3, 5) = (11, 15), \quad (3, 5) \odot (2, 3) = (13, 15).$$

Aufgabe 2 (10 Punkte). (Translationen) Es seien $(M, *)$ eine Halbgruppe und g ein Element von M . Die Abbildung $l_g : M \rightarrow M$, definiert durch $l_g(h) := g * h$, heißt g -Linkstranslation von M . Zeigen Sie, dass $(M, *)$ genau dann eine Gruppe ist, wenn alle Linkstranslationen bijektiv sind und für alle $g_1, g_2 \in M$ die Linkstranslationen l_{g_1} und l_{g_2} nur im Fall $g_1 = g_2$ übereinstimmen.

Lösung: In einer Gruppe besitzt nach der Vorlesung (Satz 43) jede Gleichung $ax = b$, $a, b \in M$, genau eine Lösung. Invertieren der beiden Seiten zeigt, dass auch für jede Gleichung $xa = b$, $a, b \in M$, genau eine Lösung existiert. Aus der ersten Aussage folgt, dass alle Linkstranslationen bijektiv sind, und aus der zweiten Aussage, dass aus $l_{a_1} = l_{a_2}$ die Gleichung $a_1 = a_2$ folgt. Wir müssen also nur noch die Rückrichtung zeigen. Wenn alle Linkstranslationen surjektiv sind, dann existiert für jedes Element $g \in G$ ein Element e_g , so dass $ge_g = g$ gilt. Daraus folgt durch die Injektivität von l_g die Gleichung $e_g h = h$, denn es gilt: $ge_g h = gh$. Insbesondere stimmen l_{e_g} und l_{e_a} für jedes Paar g, a von Elementen von G überein. Also gilt nach der Voraussetzung für die Rückrichtung, dass e_g und e_a für alle a und g übereinstimmen. Wir setzen deshalb $e := e_g$ für egal welches g . Nach dem Vorhergehenden ist e ein neutrales Element bezüglich $*$. Aus der Surjektivität der Linkstranslationen folgt, dass jedes Element aus M eine Rechtsinverse besitzt, etwa sei g' eine Rechtsinverse von g , und g'' eine Rechtsinverse von g' . Dann gilt

$$g = ge = gg'g'' = eg'' = g'',$$

und somit ist g' eine Linksinverse von g , da es eine Linksinverse von g'' ist. Das Element g ist also invertierbar.

Aufgabe 3 (7+8 Punkte). (Auswahlaxiom)

1. Gegeben sei eine Abbildung $h : M \rightarrow N$. Beweisen Sie die folgenden drei Aussagen ohne das Auswahlaxiom zu verwenden.
 - (a) Die Abbildung h ist genau dann injektiv, wenn sie eine Linksinverse besitzt.
 - (b) Wenn h eine Rechtsinverse besitzt, dann ist h surjektiv.
 - (c) Die folgenden drei Aussagen sind äquivalent:
 - (i) h ist bijektiv.
 - (ii) h besitzt eine Links- und eine Rechtsinverse.
 - (iii) Zu h existiert eine *Inverse*, d.h. eine Abbildung von N nach M , die sowohl eine Rechts- als auch eine Linksinverse von h ist.

Hinweis: Benutzen Sie die Definition einer Abbildung aus der 1. Übung: Eine *Abbildung von M nach N* ist eine Teilmenge T von $M \times N$, für die gilt, dass für jedes $x \in M$ genau ein Element $y \in N$ existiert, so dass (x, y) ein Element von T ist. Beispiel: $\text{id}_M = \{(x, x) | x \in M\} \subseteq M \times M$.

Bitte wenden.

2. Zeigen Sie, dass das Auswahlaxiom aus dem folgenden Axiom (AER) folgt:

(AER):=„Zu jeder surjektiven Abbildung gibt es eine Rechtsinverse.“

Hinweis: Gegeben sei eine Abbildung $G : I \rightarrow \mathfrak{P}(M) \setminus \{\emptyset\}$. Betrachten Sie auf der Menge $\mathcal{M} := \{(i, x) | i \in I, x \in G(i)\}$ die Äquivalenzrelation:

$$(i, x) \sim (j, y) \Leftrightarrow_{Def} i = j.$$

Wir postulieren von nun an für die Vorlesung, dass das Auswahlaxiom Gültigkeit hat.

Lösung:

1. (a) „ $\Rightarrow$ “: Es sei h injektiv. Als Abbildung ist h eine Teilmenge von $M \times N$. Wir fixieren ein Element m_0 von M . Die folgende Teilmenge

$$f := \{(n, m) \mid (m, n) \in h\} \cup \{(n, m_0) \mid n \in N \setminus \text{im}(h)\}$$

ist eine Abbildung von N nach M , denn aus $(n, m), (n, m') \in f$ folgt für $n \in N \setminus \text{im}(h)$ nach der Definition von f die Gleichheit $m = m' = m_0$ und für $n \in \text{im}(h)$ aus der Gleichung $h(m) = n = h(m')$ die Gleichung $m = m'$ aus der Injektivität von h . Aus der Definition von f folgt $(f \circ h)(m) = m$ für alle Elemente m von M .

„ $\Leftarrow$ “: Es sei f eine Linksinverse von h . Aus $h(m) = h(m')$ folgt

$$m = \text{id}(m) = f(h(m)) = f(h(m')) = \text{id}(m') = m'.$$

- (b) Es seien f eine Rechtsinverse von h und y ein Element von M . Dann gilt:

$$y = \text{id}(y) = h(f(y)) \in \text{im}(h).$$

Da y beliebig gewählt wurde, ist h somit surjektiv.

- (c) Aus (iii) folgt evident (ii) und aus (ii) folgt (i) nach 3.1.(a) und 3.1.(b). Es bleibt (i) $\Rightarrow$ (iii) zu zeigen. Wir definieren:

$$f := \{(n, m) \mid (m, n) \in h\}.$$

Da h surjektiv ist, ist N der Definitionsbereich von f und nach dem Beweis von 3.1.(a)($\Rightarrow$) ist f eine Abbildung. Die Gleichungen $h(f(m)) = m = f(h(m))$ folgen direkt aus der Definition von f .

2. Es seien eine nichtleere Menge M und eine Abbildung $G : I \rightarrow \mathfrak{P}(M) \setminus \{\emptyset\}$ gegeben. Wir übernehmen die Notationen aus dem Hinweis. Die Abbildung: $\pi : \mathcal{M} \rightarrow \mathcal{M}/\sim$ die einem Paar (i, m) deren Äquivalenzklasse zuordnet ist surjektiv und besitzt deshalb nach (AER) eine Rechtsinverse, etwa $\Phi := (\Phi_I, \Phi_M)$ von $\mathcal{M}/\sim$ nach $\mathcal{M}$. Die Abbildung $\Phi_I : \mathcal{M}/\sim \rightarrow \mathcal{I}$ ist injektiv nach der Definition von $\sim$. Wir zeigen, dass Φ_I surjektiv ist. Zu $i \in I$ gibt es ein Element $m \in G(i)$, da letztere Menge nichtleer ist, und es gilt:

$$\pi(\Phi_I(\pi(i, m)), \Phi_M(\pi(i, m))) = \pi(i, m).$$

Das heißt, dass $(\Phi_I(\pi(i, m)), \Phi_M(\pi(i, m)))$ und (i, m) äquivalent sind, also beide Paare die selbe erste Koordinate haben. Damit ist i im Bild von Φ_I und die Surjektivität folgt. Insgesamt ist Φ_I also bijektiv und besitzt nach 3.1.(c) eine Inverse Ψ_I . Die Abbildung

$$g : I \rightarrow M, g := \Phi_M \circ \Psi_I,$$

erfüllt $g(i) \in G(i)$, denn $(i, g(i)) = (\Phi_I(\Psi_I(i)), \Phi_M(\Psi_I(i)))$ ist ein Element von $\mathcal{M}$. Da M und G beliebig gewählt wurden, ist damit das Auswahlaxiom gezeigt.

Aufgabe 4 (5+(5+5) Punkte). (Die volle Automorphismengruppe eines Graphen) Es sei (E, K) ein Graph.

1. Zeigen Sie, dass $\text{Aut}(E, K)$ eine Gruppe ist.
2. Es sei m eine natürliche Zahl größer als 2. Betrachten Sie den Graphen

$$(E', K') := (\mathbb{Z}/\equiv_m, \{\{[z]_m, [z+1]_m\} \mid z \in \mathbb{Z}\}).$$

Eine Abbildung $f : \mathbb{Z}/\equiv_m \rightarrow \mathbb{Z}/\equiv_m$ heißt

- Spiegelung von (E', K') , falls eine ganze Zahl a existiert, so dass für alle $z \in \mathbb{Z}$ die Gleichung $f([z]_m) = [a]_m - [z]_m$ gilt. Wir bezeichnen diese Abbildung mit s_a .
 - Drehung von (E', K') , falls eine ganze Zahl a existiert, so dass für alle $z \in \mathbb{Z}$ die Gleichung $f([z]_m) = [a]_m + [z]_m$ gilt. Wir bezeichnen diese Drehung mit d_a .
- (a) Zeigen Sie, dass zwei Elemente f und g von $\text{Aut}(E', K')$ genau dann übereinstimmen, wenn es eine ganze Zahl z gibt, so dass $f([z]_m) = g([z]_m)$ und $f([z+1]_m) = g([z+1]_m)$ gelten.

(b) Zeigen Sie die folgende Gleichung

$$\text{Aut}(E', K') = \{d_1, \dots, d_m, s_1, \dots, s_m\},$$

und beweisen Sie, dass $\text{Aut}(E', K')$ genau $2m$ Elemente enthält.

Die Gruppe $\text{Aut}(E', K')$ heißt die *Diedergruppe* mit $2m$ Elementen und wird mit D_{2m} bezeichnet.

Lösung:

- Wir wissen bereits aus der Vorlesung, dass $\text{Sym}(E)$ eine Gruppe ist, und wir werden das Untergruppenkriterium verwenden, um für $\text{Aut}(E, K)$ die Gruppeneigenschaft nachzuweisen. Als erstes sei erwähnt, dass $\text{Aut}(E, K)$ nichtleer ist, da sie id_E enthält. Es seien f und g zwei Automorphismen des Graphen (E, K) und e_1, e_2 Elemente von E . Dann gelten

$$\{e_1, e_2\} \in K \Leftrightarrow \{f(e_1), f(e_2)\} \in K \Leftrightarrow \{g(f(e_1)), g(f(e_2))\} \in K$$

und

$$\{g^{-1}(e_1), g^{-1}(e_2)\} \in K \Leftrightarrow \{e_1 = g(g^{-1}(e_1)), e_2 = g(g^{-1}(e_2))\} \in K.$$

Somit sind $f \circ g$ und g^{-1} Elemente von $\text{Aut}(E, K)$. Nach dem Untergruppenkriterium ist $\text{Aut}(E, K)$ eine Untergruppe von $\text{Sym}(E)$.

- (a) Es ist nur die Rückrichtung zu zeigen, denn die andere Richtung ist trivial. Es seien also f und g Automorphismen des gegebenen Graphen, für die eine ganze Zahl z existiert, so dass beide Abbildungen auf $\{[z]_m, [z+1]_m\}$ übereinstimmen. Wir zeigen nun durch vollständige Induktion, dass für alle natürlichen Zahlen l die Abbildungen f und g in $[z+l]_m$ übereinstimmen, womit dann auch die Aussage der Aufgabe bewiesen wäre.

Bew.: (IA) Der Induktionsanfang folgt aus der Voraussetzung an beide Abbildungen. (IS) Es sei $l > 1$, und wir nehmen an, dass beide Abbildungen auf

$$\{[z+i]_m \mid i \in \mathbb{N}_0^{\leq l-1}\}$$

übereinstimmen. Die Ecke $[z+l-1]_m$ hat genau zwei Nachbarn: $[z+l-2]_m$ und $[z+l]_m$, genauso wie auch $f([z+l-1]_m) = g([z+l-1]_m)$ genau zwei Nachbarn hat. $f([z+l-2]_m) = g([z+l-2]_m)$ ist ein Nachbar von $f([z+l-1]_m)$, und da f und g Automorphismen des Graphen, und insbesondere bijektiv, sind, müssen $f([z+l]_m)$ und $g([z+l]_m)$ der andere Nachbar von $f([z+l-1]_m)$ sein. Also stimmen beide Abbildungen in $[z+l]_m$ überein. q.e.d.

- (b) Die Drehungen und Spiegelungen sind Elemente von $\text{Aut}(E', K')$, denn aus der Definition folgt sofort, dass s_a und d_a und deren Inverse s_a und d_{m-a} Kanten auf Kanten abbilden. Wir zeigen zunächst, dass die Elemente $d_1, \dots, d_m, s_1, \dots, s_m$ paarweise verschieden sind. Aus $s_a = s_b$ bzw. $d_a = d_b$ folgt nach Einsetzen von $[0]_m$, dass a und b in der selben Restklasse mod m liegen. Aus der Gleichung $s_a = d_b$ folgt genauso $[a]_m = [b]_m$ und somit

$$[a-1]_m = s_a([1]_m) = d_a([1]_m) = [a+1]_m,$$

also $[0]_m = [2]_m$. Ein Widerspruch dazu, dass m größer als 2 ist. Es bleibt nur noch zu zeigen, dass jedes Element f von $\text{Aut}(E', K')$ eine Spiegelung oder eine Drehung ist. Es gibt ein $v \in \mathbb{Z}$, so dass $f([0]_m) = [v]_m$ gilt. Dann ist $f([1]_m)$ ein Element von $\{[v+1]_m, [v-1]_m\}$, da f ein Automorphismus des gegebenen Graphen ist. Unter Anwendung von 4.2.(a) gilt nun Folgendes. Im Fall $f([1]_m) = [v+1]_m$ stimmt f mit d_v überein, und im Fall $f([1]_m) = [v-1]_m$ mit s_v . Also ist f eine Drehung oder eine Spiegelung.